



RIVISTA ITALIANA DI INFORMATICA E DIRITTO

Periodico internazionale di diritto, giustizia e tecnologie

1 • 2026

SEZIONE MONOGRAFICA

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

a cura di
Gaetana Morgante e Gaia Fiorinelli

diretta da **Sebastiano Faro • Marina Pietrangelo**

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

anno VIII • periodicità semestrale • ISSN 2704-7318

www.rivistaitalianadiinformaticaediritto.it



Consiglio Nazionale
delle Ricerche

Organi

DIREZIONE

SEBASTIANO FARO IGSG-CNR
MARINA PIETRANGELO IGSG-CNR

COMITATO DI DIREZIONE

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

COMITATO SCIENTIFICO

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

MONICA PALMIRANI Università di Bologna
UGO PAGALLO Università di Torino
GIOVANNI PASCUZZI Consiglio di Stato
PAOLO PASSAGLIA Università di Pisa
ORESTE POLLICINO Università di Milano-Bocconi
BENEDETTO PONTI Università di Perugia
GIOVANNI SARTOR Università di Bologna
ANDREA SIMONCINI Università di Firenze
CARLO SORRENTINO Università di Firenze
GIANCARLO TADDEI ELMI già IGSG-CNR
LARA TRUCCO Università di Genova
ALESSANDRA VALASTRO Università di Perugia
FRANCO VALLOCCHIA Università Roma-Sapienza
GIOVANNI ZICCARDI Università di Milano

ESPERTI PER LA VALUTAZIONE

[Elenco degli esperti](#) è reperibile sul sito della Rivista

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. MacIntosh, P. Maharg, J. Mayor, L.T. McCarty, F. Novak, A. Paliwala, A.E. Perez-Luño, R. Petrauskas, L. Philipps, Y. Poulet, 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

ELABORAZIONE TESTI E GRAFICA Teresa Balsamo

RESPONSABILE DEL SITO WEB Elisabetta Marinai

DIREZIONE E REDAZIONE IGSG/CNR • Via dei Barucci, 20 • 50127 Firenze • Tel. +39 055 43995

rivistariid.igsg@cnr.it • www.rivistaitalianadiinformaticaediritto.it

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

Indice

Sezione monografica

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

a cura di Gaetana Morgante e Gaia Fiorinelli

Prove digitali e ruolo delle piattaforme alla luce del pacchetto Europeo <i>e-Evidence</i> [MATILDE BELLINGERI]	9
La <i>data retention</i> : alcune riflessioni nella prospettiva del diritto privato della protezione dei dati personali [SILVIA BONETTI]	27
Il sequestro di dispositivi e informazioni digitali? [DENISE BORIERO]	43
Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA [FEDERICA DELAINI]	57
Il concetto di criminalità grave e la sfida della proporzionalità nelle indagini digitali [ROBERTO FLOR, BEATRICE PANATTONI]	83
La lunga storia delle intercettazioni nel processo penale: dal confidente al captatore informatico [PIETRO SCHIRÒ]	99
Ricadute sostanziali delle prescrizioni e dei divieti del regolamento europeo sull'intelligenza artificiale [ROSA MARIA VADALÀ]	119

Studi e ricerche

Ridurre la complessità, ricostruire la fiducia: dalla retorica della semplificazione alla teoria della chiarezza [UMBERTO NIZZA]	143
Gemelli digitali e diritto pubblico: tra questioni ricorrenti e nuove sfide [STEFANO TORREGIANI]	167
Causa ed effetto dell'intelligenza artificiale: sulla natura giuridica dell'output dell'IA e il suo impatto sul regime di responsabilità [VINCENZO CALDERONIO]	187
Privacy e protezione dei dati mentali [MAURIZIO DI MASI]	207
Technology-based decentralization and the structural limits of legal attribution: Why adapting the law requires rethinking its foundations [FILIPPO ZATTI]	223
Between the theory and practice of human oversight: Towards specialized AI regulatory sandboxes [DAVIDE BALDINI]	243
Il tool ACOI per lo screening del conflitto d'interessi e il <i>gap</i> italiano da colmare nei sistemi AI di prevenzione della corruzione [BENEDETTO PONTI]	265

Sistemi e applicazioni

Oltre la Conformità: dalle scelte strategiche ISO e NIST 2.0 alla gestione proattiva del rischio [GIOVANNI COMANDÈ, CHIARA NASI]	299

Note e discussioni

I poteri privati digitali nell'era dell'IA: profili di concorrenza, protezione dei dati e tutela dei consumatori [ARIANNA FIORENZA]	<u>325</u>
Cybersecurity e sovranità digitale: un modello normativo integrato [ELISA SORRENTINO, ANNA FEDERICA SPAGNUOLO]	<u>341</u>
La natura relativa e contestuale della nozione di dato personale alla luce della sentenza <i>Deloitte</i> [LAURA LA CORTE]	<u>357</u>
Measures for the metering of telephone calls and the interception of telecommunications in criminal proceedings: Legal aspects and implications for human rights and public safety – The case of Kosovo [VILARD BYTYQI]	<u>371</u>

Sezione monografica

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

a cura di

Gaetana Morgante e Gaia Fiorinelli



MATILDE BELLINGERI

Prove digitali e ruolo delle piattaforme alla luce del pacchetto Europeo *e-Evidence*

Le informazioni rilevanti per il processo penale sono frequentemente generate, conservate e rese accessibili da parte dei prestatori di servizi digitali secondo logiche infrastrutturali che rendono incerta la localizzazione fisica del dato. In questo contesto le categorie tradizionali della cooperazione giudiziaria, costruite intorno alla territorialità della prova e alla relazione tra autorità statali, meritano di essere ripensate secondo un modello di accesso alla prova elettronica uniforme e diretto. Il presente contributo, dopo aver analizzato il contenuto del pacchetto *e-Evidence*, composto dal Regolamento (UE) 2023/1543 e dalla Direttiva (UE) 2023/1544, delinea la struttura degli ordini europei di produzione e conservazione, concentrandosi sulla tassonomia dei dati, sulla graduazione delle garanzie, oltretutto sui rapporti tra Stato di emissione, Stato di esecuzione e prestatori di servizi. Per finire, si propone di verificare se la cooperazione diretta tra lo Stato di emissione e i prestatori di servizi riesca a coniugare efficienza investigativa e tutela dei diritti fondamentali, senza tradursi in una riduzione del controllo giurisdizionale.

Prova elettronica – Piattaforme digitali – e-Evidence – Cooperazione giudiziaria europea – Prestatori di servizi

Digital evidence and the role of platforms under the European e-Evidence package

In the current digital environment, information relevant to criminal proceedings is frequently generated, stored, and made accessible by digital service providers that make the physical location of data uncertain. In this context, the traditional categories of judicial cooperation, built around the territoriality of evidence and the relationship between state authorities, deserve to be rethought according to a uniform and direct model of access to electronic evidence. This paper, after analyzing the content of the e-Evidence package, consisting of Regulation (EU) 2023/1543 and Directive (EU) 2023/1544, outlines the structure of the European production and preservation orders, focusing on data taxonomy, the levels of guarantees, as well as the relationships between issuing and executing states, and service providers. Finally, the aim is to examine whether direct cooperation between the issuing State and service providers currently succeeds in combining investigative efficiency and the protection of fundamental rights, without reducing judicial review.

Electronic evidence – Digital platforms – e-Evidence – European judicial cooperation – Internet service providers

L'Autrice è dottoranda nel corso di Dottorato in Scienze giuridiche europee e internazionali dell'Università di Verona. Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli.

SOMMARIO: 1. Introduzione. – 2. Genesi, struttura e finalità del pacchetto europeo *e-Evidence*. – 3. Le prove elettroniche oggetto di acquisizione: categorie di dati e diversi livelli di intrusività. – 4. Le piattaforme digitali nel nuovo ecosistema investigativo europeo. – 5. Garanzie processuali e diritti fondamentali nella cooperazione diretta con le piattaforme. – 6. Considerazioni conclusive.

1. Introduzione

La progressiva digitalizzazione delle relazioni sociali, economiche e comunicative ha inciso profondamente sulla fisionomia della prova nel processo penale. Una quota crescente delle informazioni rilevanti ai fini investigativi non si manifesta più attraverso supporti materiali o fonti dichiarative tradizionali, ma mediante dati informatici generati, trasmessi, archiviati o elaborati all'interno di ecosistemi digitali complessi: comunicazioni elettroniche, metadati di accesso, cronologie di navigazione, contenuti conservati in cloud, dati di geolocalizzazione, transazioni su piattaforme online, account personali e professionali¹. La prova penale contemporanea tende così a smaterializzarsi, assumendo carattere dinamico, diffuso e strutturalmente transnazionale². A questa evoluzione si accompagna la necessità di governare in modo rigoroso tale patrimonio informativo, il quale, per la sua intrinseca modificabilità, per la velocità con cui circola e per il rischio di dispersione cui è

esposto, richiede presidi adeguati nelle fasi di conservazione, acquisizione e analisi³.

La rivoluzione digitale ha messo in crisi uno dei presupposti impliciti del processo penale: la possibilità di ricondurre l'elemento probatorio a una determinata collocazione spaziale, così da individuare l'autorità competente alla sua acquisizione. Oggi, infatti, i dati rilevanti per l'accertamento penale sono spesso generati, conservati o elaborati in ambienti digitali gestiti da prestatori di servizi privati, i quali detengono la disponibilità tecnica delle informazioni e ne governano, in concreto, le condizioni di accesso. Ne deriva una centralità crescente di tali soggetti nella filiera acquisitiva della prova elettronica: in molti casi la loro cooperazione è indispensabile; in altri, pur essendo astrattamente praticabili canali alternativi, questi risultano più invasivi, più onerosi o incompatibili con le esigenze di segretezza dell'attività investigativa⁴.

In questo contesto si colloca il c.d. pacchetto europeo *e-Evidence*⁵, composto dal Regolamento (UE) 2023/1543, relativo agli ordini europei di produzione e di conservazione delle prove elettroniche

1. SVANTESSON–OSULA 2025, p. 52 ss.; SIRACUSANO 2017, p. 181.

2. DASKAL 2015, p. 365 ss.

3. CUTRIGNELLI 2023.

4. FRANSSEN–TOSZA 2025, p. 2.

5. Il pacchetto europeo *e-Evidence* – composto dal Regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali [da ora in avanti “Regolamento” o “Reg.”] e dalla Direttiva (UE) 2023/1544 recante norme armonizzate sulla designazione degli stabilimenti e sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove elettroniche [da ora in avanti “Direttiva” o “Dir.”] – è entrato in vigore il 18 agosto 2023. Ai sensi dell'art. 35 del Regolamento, esso troverà applicazione soltanto a decorrere dal 18 agosto 2026, mentre il termine per il recepimento della Direttiva è fissato al 18 febbraio 2026. Deve pertanto ritenersi che la piena operatività del sistema europeo *e-Evidence* decorrerà dal 18 agosto 2026.

e dalla Direttiva (UE) 2023/1544, concernente la designazione di stabilimenti designati e la nomina di rappresentanti legali dei prestatori di servizi ai fini dell'acquisizione di tali prove⁶.

Il nuovo assetto normativo muove dall'intento di rendere più rapido ed effettivo l'accesso transfrontaliero ai dati digitali, riducendo i tempi e gli oneri della cooperazione tradizionale, senza rinunciare, almeno nelle intenzioni del legislatore unionale, a una cornice di garanzie coerente con i principi di necessità, proporzionalità e tutela dei diritti fondamentali. La portata del pacchetto eccede, tuttavia, il piano meramente tecnico-procedurale; non solo introduce nuovi strumenti di acquisizione probatoria, ma incide direttamente sulla geografia dei poteri nel processo penale, ridefinendo il rapporto tra autorità pubbliche e operatori privati. E proprio in questa transizione – dalla piattaforma come spazio tecnico alla piattaforma come snodo regolato della cooperazione giudiziaria – si coglie una delle linee evolutive più significative del diritto processuale penale europeo nell'era delle prove digitali⁷.

2. Genesi, struttura e finalità del pacchetto europeo *e-Evidence*

Le coordinate elaborate dalla giurisprudenza della Corte di giustizia hanno costituito il presupposto sistematico dell'intervento normativo dell'Unione europea, volto a tradurre, sul piano del diritto positivo, le esigenze emerse nel contesto

digitale, di effettività investigativa e di tutela dei diritti fondamentali⁸.

In questa prospettiva, il pacchetto *e-Evidence* si presenta quale risposta a una duplice crisi: quella inerente alla territorialità e quella dell'adeguatezza degli strumenti tradizionali di cooperazione, strutturati secondo un criterio di circolazione della prova mediato dal rapporto tra autorità statali.

Sebbene la progressiva evoluzione verso modelli di riconoscimento reciproco e di interazione tra autorità giudiziarie non sia nuova al diritto unionale (come dimostrano il mandato di arresto europeo⁹, l'ordine europeo di indagine¹⁰ e il sistema di riconoscimento reciproco dei provvedimenti di sequestro e confisca¹¹), l'acquisizione delle prove elettroniche, pur collocandosi entro tale processo di trasformazione, presenta caratteri assai peculiari, legati alla natura immateriale dei dati, alla loro frequente dispersione transnazionale e al ruolo centrale assunto da soggetti privati estranei al circuito giurisdizionale, quali sono i prestatori di servizi¹².

Sotto tale profilo, l'elemento qualificante del nuovo assetto risiede nel superamento di una logica esclusivamente interstatale di cooperazione probatoria e nell'affermazione di un modello di interlocuzione diretta con i prestatori di servizi, funzionale a fronteggiare la rapidità di circolazione del dato digitale e la frequente irrilevanza della sua localizzazione fisica¹³. Da qui, l'introduzione di due strumenti specifici – l'ordine europeo di produzione e l'ordine europeo di conservazione – i quali non

6. GAUDIERI 2023, pp. 1234-1235; FORLANI 2023, p. 174 ss.

7. AGUINALDO-DE HERT 2025, p. 200 ss.

8. CAIANIELLO 2022, p. 165; ALLEGREZZA 2020, p. 1123 ss.

9. Decisione quadro 2002/584/GAI, attuata nell'ordinamento interno con la legge n. 69/2005.

10. Direttiva 2014/41/UE, attuata con il d.lgs. n. 108/2017. In argomento si veda: CALAVITA 2025; ERTOLA 2025; RAUCCI 2025, p. 1 ss.; NASCIMBENI 2022, p. 410 ss.

11. Regolamento (UE), 2018/1805, attuato con il d.lgs. 7 agosto 2020, n. 137. Sul tema, si vedano: GRANDI 2021; MAUGERI 2019.

12. Commissione Europea, *Impact Assessment*, SWD (2018) 118, § 2.1 e § 2.2, che evidenziano come la maggior parte delle prove elettroniche sia detenuta da prestatori di servizi privati e come l'accesso ai dati nelle indagini penali richieda forme strutturate di cooperazione diretta tra autorità pubbliche e prestatori di servizi.

13. Il considerando n. 12 del regolamento chiarisce, non a caso, che il meccanismo degli ordini europei di produzione e conservazione consente alle autorità nazionali competenti di inviare tali ordini direttamente ai prestatori di servizi. È in questo passaggio che si coglie il mutamento di paradigma: l'efficienza acquisitiva non viene più affidata soltanto all'intermediazione di un'altra autorità statale, ma si fonda sulla possibilità di raggiungere immediatamente il soggetto privato che detiene o governa il dato.

eliminano il ricorso all'ordine europeo di indagine, ma ne ridimensionano la centralità nei casi in cui l'oggetto dell'acquisizione sia costituito da dati elettronici già esistenti, detenuti da prestatori di servizi rientranti nell'ambito applicativo del Regolamento.

L'obiettivo perseguito dal legislatore unionale è duplice: da un lato, predisporre strumenti capaci di assicurare un accesso tempestivo alle prove elettroniche in contesti transfrontalieri; dall'altro, sottoporre tale accesso a una cornice uniforme di garanzie, coerente con i principi di necessità e proporzionalità e con la tutela dei diritti fondamentali, in particolare del giusto processo, della protezione dei dati personali e della riservatezza delle comunicazioni. Il Regolamento (UE) 2023/1543, costituisce il nucleo sostanziale e procedurale della disciplina: introduce gli ordini europei di produzione e di conservazione delle prove elettroniche, ne definisce i presupposti, le categorie di dati, le garanzie applicabili e il meccanismo di trasmissione diretta ai prestatori di servizi¹⁴, al fine di assicurare un elevato grado di armonizzazione ed evitare soluzioni nazionali eterogenee¹⁵. La Direttiva (UE) 2023/1544, assolve una funzione complementare di carattere organizzativo. Essa mira ad armonizzare la designazione di stabilimenti designati e la nomina di rappresentanti legali¹⁶, così da assicurare, all'interno dell'Unione, un referente certo per la ricezione, l'ottemperanza e l'esecuzione degli ordini¹⁷.

Non si tratta, dunque, di due atti contigui, ma di segmenti normativi reciprocamente integrati: il Regolamento appronta il titolo europeo di acquisizione o conservazione; la Direttiva ne garantisce

l'effettività operativa mediante la costruzione di un punto di contatto giuridico con il soggetto privato che detiene, conserva o gestisce il dato.

Il sistema delineato dal Regolamento non ha carattere esclusivo; gli strumenti tradizionali di cooperazione giudiziaria continuano a trovare applicazione nei rapporti con Stati terzi e nelle ipotesi che non rientrano nell'ambito oggettivo o soggettivo del pacchetto¹⁸.

Su questa architettura si innesta la disciplina nazionale chiamata a regolare gli aspetti organizzativi e procedurali rimessi agli Stati membri. Nell'ordinamento interno, i d.lgs. 30 dicembre 2025, n. 215 e n. 216 confermano la logica bipartita del pacchetto: il primo adegua il sistema interno al Regolamento, sul piano delle competenze e delle procedure; il secondo dà attuazione alla Direttiva, rendendo operativa la figura dello stabilimento designato e del rappresentante legale.

3. Le prove elettroniche oggetto di acquisizione: categorie di dati e diversi livelli di intrusività

La nozione di prova elettronica assunta dal Regolamento riguarda dati elettronici già esistenti, detenuti da prestatori di servizi rientranti nell'ambito applicativo della disciplina europea e suscettibili di essere prodotti o conservati a fini probatori. A tale riguardo, l'art. 3 del Regolamento individua i dati relativi agli abbonati, i dati di accesso, i dati di traffico e i dati relativi al contenuto delle comunicazioni¹⁹. Questa delimitazione oggettiva condiziona l'intera architettura del sistema, individuando il

14. Cfr. artt. 1, 3, 4-11 Reg.

15. Cfr. considerando 7, 8 e 9 Reg., dai quali emerge l'esigenza di superare la frammentazione degli strumenti nazionali, assicurare un quadro comune per l'acquisizione transfrontaliera di prove elettroniche e rafforzare certezza giuridica, efficacia e rapidità della cooperazione con i prestatori di servizi.

16. Cfr. artt. 1-3 Dir.

17. Cfr. art. 3 Dir., relativo alla designazione di stabilimenti designati e alla nomina di rappresentanti legali. Si veda anche art. 4, sulle notifiche e sulle lingue, e art. 6, sulle autorità centrali. La direttiva precisa che stabilimenti designati e rappresentanti legali fungono da destinatari delle decisioni e degli ordini finalizzati all'acquisizione di prove elettroniche nei procedimenti penali.

18. Il pacchetto opera entro il perimetro unionale e riguarda i prestatori che offrono servizi nell'Unione, anche se stabiliti in Paesi terzi, i quali sono tenuti a designare uno stabilimento o a nominare un rappresentante legale nell'Unione ai fini della ricezione e dell'esecuzione degli ordini europei.

19. Cfr. art. 3, nn. 8-13, Reg., il quale definisce la nozione di "prova elettronica" e distingue le categorie di dati rilevanti: dati relativi agli abbonati, dati richiesti al solo scopo di identificare l'utente, dati relativi al traffico e dati relativi al contenuto. Si veda altresì, art. 2, sull'ambito di applicazione, e art. 3, n. 3 e n. 7, sulla nozione di prestatore di servizi e di stabilimento.

perimetro applicativo degli ordini europei di produzione e conservazione, nonché il grado di interferenza che l'atto acquisitivo è idoneo a produrre sui diritti fondamentali. La classificazione dei dati non assolve una funzione meramente definitoria: essa costituisce il presupposto della graduazione delle garanzie, poiché consente di distinguere tra dati funzionali all'identificazione dell'utente, dati capaci di ricostruire le modalità esteriori delle comunicazioni e dati che investono direttamente il contenuto informativo delle stesse.

La prima categoria è costituita dai dati relativi agli abbonati. Si tratta delle informazioni concernenti l'identità dell'utente, la sottoscrizione o l'attivazione del servizio, gli elementi di contatto e, più in generale, i dati idonei a collegare una determinata utenza digitale a una persona fisica o giuridica²⁰. La loro minore intrusività, rispetto ai dati di traffico e di contenuto, non deve tuttavia essere intesa in termini assoluti. Anche il dato apparentemente identificativo può assumere una rilevanza investigativa decisiva, nella misura in cui consente di trasformare un identificativo tecnico (ad esempio, un account, un indirizzo IP, un numero telefonico, un codice cliente) in un riferimento soggettivo utilizzabile nel procedimento penale. Proprio per questa ragione il Regolamento individua una categoria ulteriore di dati, ossia quelli richiesti al solo fine di identificare l'utente.

Tale scelta assume particolare interesse sistemico: essa comporta la sottrazione di una parte dei dati tecnici alla disciplina più rigorosa prevista per i dati di traffico valorizzando non soltanto la natura del dato ma la funzione della richiesta. Tale categoria di dati comprende, in particolare, gli indirizzi IP e, ove necessario, le porte di origine e la marcatura temporale, nonché equivalenti tecnici di tali identificativi, quando siano richiesti esclusivamente per individuare l'utente in una specifica

indagine penale²¹. Il medesimo dato può quindi assumere un diverso grado di intrusività a seconda che sia utilizzato per una mera identificazione oppure per ricostruire sequenze comunicative, relazioni, accessi o condotte digitali.

Più problematico risulta essere il trattamento dei dati relativi al traffico; essi non rivelano il contenuto della comunicazione, ma ne descrivono gli elementi esteriori, quali origine, destinazione, tempo, durata, percorso, servizio utilizzato e altri parametri tecnici dell'interazione digitale. La distinzione tra contenuto e dati esterni della comunicazione, pur conservando rilievo dogmatico, non è sufficiente a fondare una rigida gerarchia di tutela. La giurisprudenza della Corte di giustizia ha progressivamente chiarito che i dati relativi al traffico e all'ubicazione, specie se considerati nel loro insieme, possono consentire inferenze estremamente precise sulla vita privata dell'interessato, sulle sue abitudini, sui suoi spostamenti e sulle sue relazioni personali²². Il metadato, in altri termini, non è un dato neutro: la sua capacità rivelatrice cresce in funzione della quantità, della durata temporale dell'acquisizione e delle possibilità di aggregazione.

La categoria più invasiva resta quella dei dati relativi al contenuto. Essa comprende il contenuto sostanziale delle comunicazioni o delle informazioni conservate mediante il servizio digitale: messaggi, testi, immagini, video, file, documenti, registrazioni o altri materiali caricati, trasmessi o archiviati. In questo caso, l'interferenza con la sfera privata è diretta, poiché l'autorità procedente accede non soltanto agli indici esteriori della comunicazione, ma al suo contenuto semantico. Per tale ragione, l'acquisizione dei dati di contenuto impone un controllo particolarmente rigoroso di legalità, necessità e proporzionalità, oltre a una più attenta verifica dei presupposti di emissione dell'ordine.

20. Cfr. art. 3, n. 9, Reg., relativo alla definizione di "subscriber data", sul rilievo pratico dei dati di abbonamento nell'identificazione dell'utente.

21. Cfr. art. 3, n. 10, Reg. Sul punto si veda anche WAHL 2023, p. 165 ss., che segnala l'introduzione, accanto alle categorie tradizionali dei dati di abbonamento, traffico e contenuto, di una quarta categoria relativa ai dati richiesti esclusivamente per identificare l'utente.

22. Cfr. Corte giust., Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*; Corte giust., Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Watson*; Corte giust., Grande Sezione, 2 marzo 2021, causa C-746/18, *Prokuratuur*. In quest'ultima decisione la Corte ha escluso che il pubblico ministero, quando dirige le indagini e sostiene l'accusa, possa essere considerato autorità indipendente idonea ad autorizzare l'accesso ai dati relativi al traffico e all'ubicazione ai fini dell'indagine penale.

Al riguardo, il Regolamento conferma questa impostazione graduata, sicché l'ordine europeo di produzione avente ad oggetto dati relativi agli abbonati o dati richiesti al solo fine di identificare l'utente può essere emesso per tutti i reati; al contrario, l'ordine relativo a dati di traffico o di contenuto è ammesso, in linea generale, solo per reati punibili nello Stato di emissione con pena detentiva pari, nel massimo, ad almeno tre anni, salve alcune ipotesi specificamente individuate²³.

Tale graduazione incide anche sul profilo soggettivo dell'autorità competente. Il Regolamento consente infatti al pubblico ministero di emettere ordini europei di produzione per dati relativi agli abbonati e per dati richiesti al solo fine di identificare l'utente, nonché ordini europei di conservazione; viceversa, quando l'ordine di produzione abbia ad oggetto dati di traffico o dati di contenuto, l'intervento del pubblico ministero richiede la convalida da parte di un giudice, di un organo giurisdizionale o di un giudice istruttore²⁴.

Tale differenziazione non elimina, tuttavia, ogni margine problematico. Il rischio è che la classificazione normativa venga intesa come automatismo, secondo una logica per cui i dati diversi dal contenuto sarebbero, per ciò solo, scarsamente lesivi. L'esperienza della prova digitale mostra, al contrario, che la capacità conoscitiva del dato dipende, non soltanto dalla sua appartenenza formale a una categoria, ma anche dal modo in cui esso viene combinato con altri dati, dalla durata dell'osservazione, dalla posizione del soggetto interessato e dal contesto investigativo. La proporzionalità dell'acquisizione non può quindi essere esaurita nella qualificazione astratta del dato, ma richiede una valutazione concreta della sua incidenza.

In questa prospettiva, la classificazione prevista dal Regolamento deve essere letta come primo presidio di garanzia, non come criterio autosufficiente di legittimazione. Essa serve ad orientare l'autorità procedente nella scelta dello strumento, nella delimitazione dell'oggetto dell'ordine e nella

motivazione della richiesta. Al tempo stesso, vincola il prestatore di servizi destinatario dell'ordine a svolgere una verifica circa la natura dei dati domandati e del regime applicabile.

Proprio questo sembra essere il punto di intersezione tra la dimensione probatoria e quella organizzativa del pacchetto *e-Evidence*: la prova elettronica, nel modello europeo, non è soltanto un'informazione da acquisire, ma un dato collocato presso un soggetto privato che diviene snodo necessario della cooperazione penale transfrontaliera. La delimitazione dell'oggetto dell'acquisizione rileva nel rapporto con gli altri strumenti di cooperazione giudiziaria. Il Regolamento 2023/1543 non disciplina ogni forma di evidenza elettronica e non esclude, in via generale, il ricorso ad altri strumenti dell'Unione o internazionali²⁵.

Ne discende che la corretta qualificazione della categoria di dati richiesta costituisce il primo momento di una più ampia verifica di legalità probatoria. Prima ancora di individuare lo strumento da attivare, l'autorità procedente è chiamata a precisare quale dato intenda acquisire, quale grado di intrusività lo caratterizzi e quale regime di garanzie debba accompagnarne la circolazione transfrontaliera.

4. Le piattaforme digitali nel nuovo ecosistema investigativo europeo

Né il Regolamento (UE) 2023/1543 né la Direttiva (UE) 2023/1544 assumono la "piattaforma" quale categoria normativa autonoma. Entrambi gli atti operano, piuttosto, attraverso la nozione più ampia e funzionale di prestatore di servizi. Tale scelta non è priva di rilievo sistematico, poiché consente di ricomprendere entro un'unica cornice regolatoria una pluralità di soggetti eterogenei – prestatori di servizi di comunicazione elettronica, fornitori di hosting, cloud providers, piattaforme di messaggistica, social network, marketplace e altri intermediari digitali – accomunati dalla posizione infrastrutturale che occupano rispetto alla

23. Cfr. art. 5, parr. 3 e 4, Reg.

24. Cfr. art. 4 Reg., sul diverso ruolo del pubblico ministero a seconda della categoria di dati richiesta.

25. Art. 32, par. 1, Reg. Sul carattere non esclusivo dello strumento, si veda ESPINA RAMOS 2025, secondo il quale l'autorità di emissione conserva la possibilità di ricorrere, a seconda del caso concreto, agli ordini europei di produzione o conservazione oppure ad altri strumenti dell'Unione o internazionali.

generazione, conservazione e accessibilità dei dati rilevanti per l'accertamento penale²⁶.

Da questo punto di vista, la piattaforma rileva anzitutto come infrastruttura probatoria. Essa non costituisce solo uno spazio digitale nel quale gli utenti comunicano, acquistano beni, condividono contenuti o conservano informazioni, ma rappresenta l'ambiente tecnico-organizzativo in cui si formano elementi suscettibili di assumere valore investigativo: dati di registrazione, identificativi tecnici, log di accesso, metadati, cronologie di interazione, contenuti archiviati, informazioni relative a dispositivi, sessioni, indirizzi IP, localizzazioni e modalità di utilizzo del servizio.

La prova elettronica, dunque, non è semplicemente collocata presso il prestatore di servizi: la sua individuazione, estrazione e verificabilità dipendono dalle modalità con cui la piattaforma organizza le informazioni, ne disciplina la conservazione e la cancellazione e ne rende possibile l'estrazione secondo procedure tecniche interne²⁷. L'accesso al dato presuppone, pertanto, non solo un titolo giuridico legittimante, ma anche la cooperazione tecnica e organizzativa del soggetto che governa l'infrastruttura digitale entro cui quel dato è generato, conservato o reso accessibile.

Il Regolamento prende atto di tale trasformazione e costruisce un modello nel quale il prestatore di servizi diviene destinatario diretto dell'ordine europeo. La novità non consiste soltanto nella riduzione dei tempi di acquisizione, ma investe la struttura stessa del rapporto cooperativo: rispetto agli strumenti tradizionali, fondati sull'intermediazione dello Stato di esecuzione, l'autorità

competente dello Stato di emissione può rivolgersi direttamente al soggetto privato che detiene, conserva o controlla i dati richiesti.

Il confronto con l'ordine europeo di indagine (OEI) consente di precisare la portata di questo mutamento. L'OEI conserva la funzione di strumento generale per l'acquisizione transnazionale della prova e mantiene rilievo per gli atti che richiedano l'intervento dell'autorità dello Stato di esecuzione o che non rientrino nell'ambito applicativo del Regolamento. L'*e-Evidence* opera, invece, secondo una logica di specialità funzionale: quando l'acquisizione riguarda dati elettronici già esistenti e detenuti da un prestatore di servizi rientrante nell'ambito soggettivo della disciplina europea, l'ordine europeo di produzione o di conservazione diviene il canale tipico di accesso alla prova. In questo schema, la piattaforma non è più un terzo occasionalmente coinvolto nel circuito acquisitivo, ma il punto di raccordo tra l'autorità giudiziaria e l'ambiente tecnico nel quale il dato è generato, conservato, organizzato e reso disponibile²⁸.

In questo contesto la Direttiva completa il modello sotto il profilo organizzativo, mirando a garantire che tale titolo abbia un destinatario certo, stabile e giuridicamente responsabile all'interno dell'Unione. L'obbligo di designare uno stabilimento o nominare un rappresentante legale non costituisce un adempimento meramente formale, ma il presupposto operativo dell'intero sistema. Senza un punto di contatto giuridicamente individuabile, l'ordine europeo rischierebbe di restare ineffettivo, soprattutto nei confronti di prestatori

26. Sul ricorso a una nozione funzionale, e non tipologica, di prestatore di servizi, si veda l'art. 3, n. 3, Reg.; nonché gli artt. 1 e 2 Direttiva (UE) 2023/1544, quanto all'ambito soggettivo degli obblighi di designazione dello stabilimento o di nomina del rappresentante legale. Si veda inoltre il considerando n. 16 Reg., ove sono richiamati, a titolo esemplificativo, mercati online, servizi di hosting, cloud computing, piattaforme di gioco online e piattaforme di gioco d'azzardo online.

27. Per una lettura della prova digitale come evidenza la cui formazione, conservazione e intelligibilità dipendono dall'ambiente tecnico nel quale il dato è generato e gestito, si veda: Corte suprema di Cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, *Relazione su novità normativa n. 25/2026*, 7 aprile 2026, Parte I, § 1, secondo cui il passaggio da fonti probatorie materialmente localizzate a informazioni digitali, la cui esistenza, conservazione e intelligibilità dipendono da infrastrutture tecnologiche, determina una trasformazione epistemologica della prova penale.

28. *Ibidem*; cfr. considerando n. 12 e artt. 5-7, 9-11 Reg., relativi alle condizioni di emissione degli ordini europei di produzione e conservazione, ai destinatari, ai certificati degli ordini e alla loro esecuzione.

non stabiliti nello Stato di emissione o strutturati secondo modelli societari transnazionali²⁹.

L'effetto complessivo sembra essere quello di una responsabilizzazione organizzativa delle piattaforme, chiamate a predisporre canali di ricezione, procedure di verifica, sistemi di identificazione delle richieste, meccanismi di conservazione selettiva e modalità di trasmissione dei dati compatibili con i termini e le garanzie previsti dal Regolamento. Il prestatore di servizi deve essere in grado di distinguere tra dati relativi agli abbonati, dati richiesti al solo fine di identificare l'utente, dati di traffico e dati di contenuto; deve conservare o produrre soltanto quanto richiesto; deve rispettare i termini ordinari o emergenziali; deve eventualmente far valere i motivi di impossibilità, opposizione o conflitto normativo previsti dalla disciplina europea. In questo contesto, la tassonomia dei dati esaminata nel paragrafo precedente non rileva soltanto per l'autorità che emette l'ordine, ma anche per il destinatario privato, il quale è chiamato a tradurre la richiesta giuridica in operazione tecnica selettiva³⁰.

Tale responsabilizzazione non equivale, tuttavia, all'attribuzione di una funzione pubblica in senso proprio, né determina una privatizzazione dell'attività investigativa; la decisione sull'acquisizione resta ancorata a un titolo emesso dall'autorità competente, soggetto ai controlli previsti dal Regolamento. Ciò che muta è la dipendenza funzionale dell'accertamento pubblico dall'infrastruttura privata: l'effettività dell'ordine europeo

presuppone la cooperazione tecnica, organizzativa e documentale del prestatore³¹. In questa prospettiva, la formula della collaborazione para-giurisdizionale dei prestatori di servizi può essere accolta solo in senso descrittivo, per indicare una funzione procedimentale intermedia nella quale obblighi di cooperazione, capacità tecnica e organizzazione interna concorrono a rendere possibile – o, al contrario, a ostacolare – l'accesso alla prova elettronica. La posizione delle piattaforme sembra dunque collocarsi in una zona intermedia tra soggezione all'ordine pubblico e autonomia organizzativa privata. Da un lato, esse sono destinatarie di obblighi giuridici tipizzati e possono essere esposte a conseguenze sanzionatorie in caso di inottemperanza; dall'altro, l'esecuzione concreta dell'ordine dipende da sistemi tecnici e procedure interne che restano in larga misura nella disponibilità del prestatore. Il controllo di legalità, pertanto, non può arrestarsi al provvedimento emesso dall'autorità giudiziaria, ma deve estendersi alla verificabilità della filiera acquisitiva, comprensiva della fase esecutiva svolta presso il soggetto privato³².

Il punto assume particolare rilievo con riferimento all'ordine europeo di conservazione, la cui funzione non è quella di acquisire immediatamente il dato, ma di impedirne la cancellazione, l'alterazione o la dispersione in vista di una successiva produzione.

La piattaforma diviene il soggetto presso il quale si realizza una forma di tutela anticipata della

29. Sulla funzione organizzativa della direttiva, cfr. artt. 1 e 3 Dir.: la disciplina mira a garantire che i prestatori di servizi che offrono servizi nell'Unione dispongano di uno stabilimento designato o di un rappresentante legale incaricato della ricezione, dell'ottemperanza e dell'esecuzione degli ordini e delle decisioni diretti all'acquisizione di prove elettroniche nei procedimenti penali. Cfr., altresì, artt. 4 e 5 Dir., in tema di notifiche e sanzioni. Per l'attuazione nell'ordinamento italiano, si veda d.lgs. 30 dicembre 2025, n. 216.

30. Sulla tassonomia dei dati quale presupposto non solo dell'emissione, ma anche dell'esecuzione selettiva dell'ordine si veda, *supra*, § 3, nonché art. 3, nn. 9-12, Reg. Gli obblighi del prestatore si ricavano, in particolare, dagli artt. 10 e 11 Reg., relativi all'esecuzione dell'ordine europeo di produzione e dell'ordine europeo di conservazione, e dall'art. 12, che disciplina l'impossibilità di esecuzione, i motivi di rifiuto e i meccanismi di riesame. Cfr. altresì artt. 7 e 9 Reg., sui destinatari degli ordini e sui certificati degli ordini, dai quali emerge la necessaria traduzione della richiesta giuridica in un'operazione tecnica di individuazione, selezione e trasmissione del dato.

31. DE MAIO 2026.

32. La posizione intermedia del prestatore emerge dal combinato disposto degli artt. 7, 9-12 e 15 Reg. Sul versante organizzativo, si vedano gli artt. 1, 3 e 5 Dir., dai quali risulta che lo stabilimento designato o il rappresentante legale deve disporre dei poteri e delle risorse necessari per ricevere, ottemperare ed eseguire gli ordini e le decisioni rivolti al prestatore. In tale quadro, la fase esecutiva svolta presso il soggetto privato diviene parte essenziale della filiera acquisitiva, con conseguente rilievo della verificabilità delle operazioni tecniche di individuazione, conservazione, selezione e trasmissione del dato.

fonte digitale: non vi è ancora accesso conoscitivo da parte dell'autorità, ma vi è già un vincolo giuridico sulla gestione privata del dato. Questo profilo mostra con chiarezza come, nell'ambiente digitale, la conservazione della prova sia distinta dalla sua acquisizione e possa costituire una fase autonoma e strategica dell'attività investigativa³³.

La centralità del prestatore produce, infine, inevitabili tensioni con la dimensione transnazionale dell'economia digitale. Molte piattaforme operano attraverso gruppi societari globali, infrastrutture distribuite e centri decisionali collocati anche al di fuori dell'Unione. Ne discende il rischio di conflitti tra l'obbligo di ottemperare all'ordine europeo e vincoli derivanti da ordinamenti di Paesi terzi, specie quando la produzione del dato possa violare divieti, procedure autorizzative o discipline straniere in materia di protezione dei dati, segreto, sicurezza nazionale o comunicazioni elettroniche. Il Regolamento prende in considerazione tale eventualità, prevedendo meccanismi di obiezione e riesame; nondimeno, il problema resta strutturale, poiché il prestatore globale è chiamato a muoversi entro una pluralità di regimi normativi potenzialmente incompatibili³⁴.

In definitiva, le piattaforme non diventano titolari del potere di decidere se e come procedere all'accertamento penale, ma governano le condizioni tecniche e organizzative di accesso a una parte crescente delle evidenze rilevanti per il processo. Per tale ragione, la loro funzione non può essere ridotta a quella di meri archivi privati, né sovrapposta a quella delle autorità giudiziarie; esse rappresentano, piuttosto, uno snodo regolato del nuovo ecosistema investigativo europeo, nel quale

l'effettività della cooperazione penale transfrontaliera dipende dall'interazione tra titolo giudiziario, infrastruttura digitale, compliance privata e garanzie processuali. Questa interdipendenza costituisce uno dei tratti più innovativi e, al tempo stesso, più problematici del pacchetto *e-Evidence*.

5. Garanzie processuali e diritti fondamentali nella cooperazione diretta con le piattaforme

Il ruolo infrastrutturale delle piattaforme, descritto nel paragrafo precedente, assume rilievo soprattutto sul piano delle garanzie. La maggiore efficienza nell'acquisizione transfrontaliera delle prove elettroniche, perseguita attraverso gli ordini europei di produzione e di conservazione, impone di verificare la tenuta del modello di cooperazione diretta con i prestatori di servizi. La questione non si esaurisce nella tutela della riservatezza e della protezione dei dati personali, ma investe, in maniera più ampia, l'equilibrio tra rapidità dell'azione investigativa, controllo giurisdizionale, diritti della difesa ed effettività dei rimedi. Proprio perché l'ordine europeo può essere indirizzato direttamente al soggetto privato che detiene, conserva o controlla il dato, con un coinvolgimento solo eventuale o ridimensionato dell'autorità dello Stato di esecuzione, il profilo decisivo diviene la distribuzione dei controlli lungo l'intera filiera acquisitiva³⁵.

Il punto critico non risiede nell'assenza di garanzie, bensì nella loro diversa collocazione procedimentale. Il Regolamento delinea un sistema nel quale la verifica dei presupposti dell'ordine è affidata principalmente all'autorità dello Stato di emissione; l'autorità dello Stato di esecuzione

33. Sulla natura preservativa, e non immediatamente acquisitiva, del Certificato europeo di ordine di conservazione, si vedano gli artt. 6 e 11 Reg., relativi, rispettivamente, alle condizioni di emissione e all'esecuzione dell'ordine europeo di conservazione; cfr. altresì considerando n. 31 e n. 33 del medesimo regolamento, che valorizzano la funzione di impedire la cancellazione, alterazione o dispersione dei dati in vista di una successiva produzione. Nello stesso senso, Corte suprema di Cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, *Relazione su novità normativa* n. 25/2026, 7 aprile 2026, § 5.4, sulla conservazione quale fase autonoma e anticipata di tutela della fonte digitale.

34. Il problema è espressamente considerato dall'art. 17 Reg., che disciplina il riesame dell'ordine europeo di produzione in caso di conflitto con obblighi derivanti dal diritto di un Paese terzo, consentendo al destinatario del Certificato europeo dell'ordine di produzione di formulare un'obiezione motivata ove l'esecuzione dell'ordine possa comportare la violazione di tali obblighi.

35. Cfr. artt. 5 e 6 Reg., sui requisiti di necessità, proporzionalità e ammissibilità della misura in un caso interno comparabile; artt. 8, 10-12 e 16 Reg., sul coinvolgimento dell'autorità di esecuzione, sull'esecuzione degli ordini e sui motivi di rifiuto; artt. 13 e 18 Reg., rispettivamente in tema di informazione dell'interessato e ricorsi effettivi.

interviene solo in ipotesi determinate, mentre la prima presa in carico dell'ordine si realizza presso il prestatore di servizi destinatario della richiesta. Ne deriva un assetto nel quale l'effettività della tutela dipende, non soltanto dalla qualità del titolo emesso dall'autorità procedente, ma anche dalla possibilità che l'interessato sia tempestivamente informato, che l'autorità di esecuzione possa intervenire nei casi necessari e che il prestatore sia in grado di riconoscere e segnalare eventuali profili ostativi all'esecuzione dell'ordine³⁶.

In questa architettura, i requisiti di necessità e proporzionalità costituiscono il primo argine all'ingiustificata espansione dello strumento. Tanto l'ordine europeo di conservazione quanto l'ordine europeo di produzione possono essere emessi solo se necessari e proporzionati rispetto alle finalità del procedimento penale e nel rispetto dei diritti della persona sottoposta alle indagini o imputata. Nel primo caso, il giudizio è calibrato sull'esigenza di impedire la cancellazione, la rimozione o la modifica dei dati; nel secondo, sull'acquisizione conoscitiva dell'informazione a fini probatori. In entrambi, il Regolamento introduce una clausola di equivalenza interna, richiedendo che una misura analoga sia ammissibile in un caso interno comparabile³⁷. Tale clausola impedisce che lo strumento europeo sia impiegato come via più agevole per eludere le garanzie previste dall'ordinamento nazionale. La proporzionalità, pertanto, non può ridursi a una formula motivazionale di stile, ma deve tradursi in

una verifica concreta della pertinenza, selettività e indispensabilità dei dati richiesti, specie quando l'ordine sia rivolto a piattaforme digitali capaci di concentrare una quantità elevatissima di informazioni relative non solo all'indagato, ma anche a terzi estranei al procedimento.

La graduazione delle garanzie si innesta sulla tassonomia dei dati elettronici prevista dal Regolamento. Gli ordini aventi a oggetto dati identificativi³⁸ o relativi agli abbonati³⁹ sono assoggettati a un regime più flessibile; quelli relativi a dati di traffico non richiesti al solo scopo di identificare l'utente o a dati di contenuto sono invece sottoposti a presupposti più rigorosi, in ragione della maggiore capacità intrusiva di tali informazioni. Per gli ordini europei di produzione relativi a dati di traffico o di contenuto, il Regolamento rafforza il controllo sull'emissione e collega l'accesso, salvo eccezioni specificamente individuate, alla gravità del reato, richiedendo che esso sia punito nello Stato di emissione con pena detentiva pari, nel massimo, ad almeno tre anni. La classificazione dei dati opera così come tecnica di regolazione dell'intrusività: quanto più l'informazione richiesta consente di ricostruire comunicazioni, relazioni, spostamenti, abitudini o contenuti della vita privata, tanto più il sistema pretende un controllo qualificato sull'accesso⁴⁰.

L'art. 1, par. 2, del Regolamento riconosce alla persona sottoposta alle indagini o imputata, nonché al suo difensore, la possibilità di richiedere

36. Cfr. art. 13 Reg., sull'informazione alla persona i cui dati sono richiesti; artt. 8 e 12 Reg., sul coinvolgimento dell'autorità di esecuzione e sui motivi di rifiuto; artt. 10, parr. 5-8, e 11, parr. 4-7, Reg., sulle interlocuzioni tra destinatario dell'ordine e autorità di emissione in caso di impossibilità o criticità esecutive; art. 17 Reg., sull'obiezione motivata per conflitto con obblighi derivanti dal diritto di un Paese terzo.

37. Le menzionate regole sull'adozione degli ordini sono contenute nell'art. 5 Reg. per l'OEP e nel successivo art. 6 per l'OEC.

38. I dati richiesti al solo scopo di identificare l'utente appaiono individuati secondo un criterio teleologico. Pensiamo agli indirizzi IP, dai quali si possono trarre informazioni anche con riguardo al sito visitato dall'utente, ma che rientrano nella categoria *de qua* se richiesti al solo scopo di identificazione. Per la definizione completa, si veda l'art. 3, n. 10, Reg.

39. I dati relativi agli abbonati sono, per esempio, quelli inerenti all'indirizzo e-mail fornito dall'utente o alla durata del servizio al quale si è abbonato; tra i "dati sul traffico", a titolo di esempio, rientrano quelli relativi alla fonte ed al destinatario di un messaggio e quelli sull'ubicazione, mentre sono "relativi al contenuto" i dati come il testo, la voce, i video, le immagini o il suono. Per le definizioni complete, si veda: art. 3, nn. 9, 11 e 12 Reg.

40. Cfr. art. 5, paragrafo 4, Reg. Al riguardo, la soglia editale è ritenuta essere troppo bassa da CORHAY 2021, pp. 448-449; stigmatizza invece l'assenza di un vaglio circa la sussistenza di un compendio indiziario minimo in ordine al fatto per cui si procede, GERACI 2019, p. 1360.

all'autorità competente l'emissione di un ordine europeo di produzione o di conservazione. Si tratta di una previsione significativa, perché sottrae gli strumenti *e-Evidence* a una lettura esclusivamente accusatoria e ne consente, almeno in astratto, l'impiego anche nella ricerca di elementi favorevoli all'indagato o all'imputato.

Questa apertura non elimina, tuttavia, le criticità connesse alla conoscibilità dell'acquisizione. Per l'ordine europeo di conservazione non è previsto un obbligo generale di informazione dell'utente, i cui dati siano oggetto di preservazione; l'interessato può dunque restare ignaro della misura anche dopo la sua esecuzione. Diversamente, per l'ordine europeo di produzione, il Regolamento impone all'autorità di emissione di informare senza indebito ritardo la persona i cui dati sono richiesti, pur consentendo che tale comunicazione sia ritardata o omessa quando ciò risulti necessario per non compromettere le indagini. La valutazione è rimessa alla stessa autorità procedente e si fonda su presupposti ampi, potenzialmente idonei a comprimere l'effettività del diritto all'informazione.

Ne deriva una tensione evidente tra segretezza investigativa e accesso ai rimedi. L'informazione all'interessato costituisce, infatti, il presupposto pratico per contestare la legittimità dell'acquisizione. Sebbene il Regolamento riconosca alla persona i cui dati siano stati prodotti mediante un ordine europeo di produzione, il diritto a un mezzo di impugnazione effettivo dinanzi a un organo giurisdizionale dello Stato di emissione, l'effettività di tale rimedio dipende dalla conoscenza dell'avvenuta acquisizione. Ancora più problematica appare

la posizione dell'interessato rispetto all'ordine di conservazione, poiché non è previsto né un rimedio specifico avverso gli effetti della misura, né un obbligo generale di informazione che consenta di contestarne tempestivamente la legittimità⁴¹.

Il profilo più delicato resta il ridimensionamento del ruolo dell'autorità di esecuzione.

Nel modello ordinario dell'*e-Evidence*, il rapporto primario intercorre tra autorità di emissione e prestatore di servizi. Per l'ordine europeo di conservazione e per l'ordine europeo di produzione avente a oggetto dati relativi agli abbonati o dati richiesti al solo scopo di identificare l'utente, il prestatore provvede senza il necessario coinvolgimento dell'autorità dello Stato in cui è stabilito il rappresentante o lo stabilimento designato: nel primo caso, preservando i dati; nel secondo, trasmettendoli all'autorità di emissione entro il termine previsto⁴².

Qualora emergessero difficoltà di esecuzione dell'ordine, il primo interlocutore del destinatario rimane l'autorità di emissione. Il prestatore di servizi deve indicare le ragioni per le quali l'ordine non può essere eseguito, o non può esserlo nei termini, instaurando un dialogo diretto con l'autorità procedente, la quale può modificare o ritirare l'ordine. L'autorità di esecuzione viene coinvolta solo in ipotesi specifiche, ad esempio quando l'adempimento possa interferire con immunità o privilegi, con norme sulla libertà di stampa o di espressione oppure, con riferimento all'ordine europeo di produzione, quando possa determinare la violazione di obblighi derivanti dal diritto di un Paese terzo⁴³.

41. Cfr. artt. 13 Reg., il quale disciplina l'informazione alla persona i cui dati sono richiesti, consentendone tuttavia il ritardo o la limitazione nei casi previsti; 18 Reg., il quale riconosce alla persona i cui dati siano stati richiesti mediante ordine europeo di produzione il diritto a un ricorso effettivo dinanzi a un organo giurisdizionale dello Stato di emissione. Quanto all'ordine europeo di conservazione, si veda l'art. 11 Reg., il quale disciplina l'esecuzione senza prevedere un autonomo rimedio dell'interessato avverso la misura conservativa.

42. Cfr. artt. 11, par. 1, Reg., secondo il quale il destinatario dell'ordine europeo di conservazione deve conservare i dati richiesti senza indebito ritardo per il periodo previsto; 10, parr. 1 e 3, Reg., il quale disciplina l'esecuzione dell'ordine europeo di produzione, imponendo al destinatario di trasmettere i dati richiesti direttamente all'autorità di emissione o alle autorità di contrasto indicate nel certificato europeo dell'ordine di produzione, entro i termini stabiliti.

43. Cfr. art. 11, par. 4, Reg., per l'ordine europeo di conservazione, e art. 10, par. 5, Reg., per l'ordine europeo di produzione, i quali disciplinano le ipotesi in cui il destinatario dell'ordine non possa ottemperarvi, o non possa farlo entro il termine stabilito, prevedendo l'interlocuzione con l'autorità di emissione e, nei casi indicati, il coinvolgimento dell'autorità di esecuzione. Quanto al conflitto con obblighi derivanti dal diritto di un Paese terzo, si veda l'art. 17 Reg., il quale introduce una procedura di riesame dell'ordine europeo di produzione.

Lo Stato di esecuzione riacquista una posizione più incisiva solo in una fase successiva, qualora il prestatore non adempia e l'autorità di emissione richieda l'attivazione di meccanismi coercitivi. In tale ipotesi, l'autorità di esecuzione può ingiungere formalmente al destinatario di ottemperare, salva la possibilità di far valere motivi di rifiuto nei termini previsti dal Regolamento. L'inottemperanza successiva può esporre il prestatore a sanzioni particolarmente elevate, fino alla soglia massima individuata dal diritto unionale⁴⁴.

Un regime più garantito sembra essere previsto per gli ordini europei di produzione relativi a dati di traffico o di contenuto, quando non ricorrano determinate circostanze che riconducono il caso allo Stato di emissione. In tali ipotesi opera il c.d. regime con notifica: l'autorità di emissione deve notificare l'ordine anche all'autorità di esecuzione, la quale dispone di un termine per far valere eventuali motivi di rifiuto. Il coinvolgimento anticipato dello Stato di esecuzione consente, almeno in tali casi, un controllo ulteriore, soprattutto quando vengano in rilievo immunità, privilegi, libertà di stampa o libertà di espressione⁴⁵. La portata di tale garanzia resta, tuttavia, circoscritta. Il regime con notifica non opera quando vi sia fondato motivo di ritenere che il reato sia stato commesso, sia in atto o possa essere commesso nello Stato di emissione, oppure quando la persona i cui dati sono

richiesti risieda in tale Stato⁴⁶. Considerato che, in molti procedimenti, l'unico elemento transfrontaliero consiste nella localizzazione del prestatore, del rappresentante legale o dello stabilimento designato in un altro Stato membro, è plausibile che la vicenda resti integralmente riconducibile allo Stato di emissione, con conseguente esclusione del regime notificatorio. Inoltre, la verifica delle condizioni che escludono la notifica è rimessa alla stessa autorità di emissione, con il rischio di una lettura restrittiva del coinvolgimento dello Stato di esecuzione.

Anche in questo caso il confronto con l'OEI permette di cogliere la portata del pacchetto. Nell'OEI l'autorità di esecuzione conserva un ruolo strutturale: interloquisce con quella di emissione, partecipa al riconoscimento e all'esecuzione dell'atto e può verificare, tra l'altro, la compatibilità della misura richiesta con i diritti fondamentali. Nel sistema *e-Evidence*, invece, una parte della funzione di filtro che nell'OEI appartiene all'autorità di esecuzione risulta essere anticipata sul prestatore di servizi. Nonostante il testo definitivo del Regolamento abbia corretto alcune criticità rispetto alla proposta originaria, introducendo il regime con notifica per taluni ordini relativi a dati di traffico o di contenuto⁴⁷, riconoscendo all'autorità di esecuzione la possibilità di far valere il motivo di rifiuto fondato sulla violazione dei diritti fondamentali⁴⁸, al di

44. Cfr. art. 16 Reg., il quale disciplina la procedura di esecuzione forzata degli ordini europei di produzione e conservazione in caso di mancata ottemperanza da parte del destinatario, attribuendo all'autorità di esecuzione il compito di ingiungere formalmente l'adempimento e di valutare gli eventuali motivi di rifiuto; si veda altresì l'art. 15 Reg., il quale impone agli Stati membri di prevedere sanzioni effettive, proporzionate e dissuasive, le quali possono arrivare sino al 2% del fatturato mondiale totale annuo del prestatore di servizi nell'esercizio precedente.

45. Cfr. art. 8 Reg., che disciplina la notifica all'autorità di esecuzione dell'ordine europeo di produzione relativo a dati di traffico, diversi da quelli richiesti al solo scopo di identificare l'utente, o a dati relativi al contenuto, salvo che il reato sia stato commesso, sia in corso o possa essere commesso nello Stato di emissione, oppure che la persona i cui dati sono richiesti risieda in tale Stato; art. 12 Reg., sui motivi di rifiuto opponibili dall'autorità di esecuzione, tra cui le ipotesi relative a immunità, privilegi, libertà di stampa e libertà di espressione in altri mezzi di comunicazione.

46. Cfr. art. 8, par. 2, Reg.

47. Cfr. art. 8 Reg.

48. Cfr. art. 12 Reg. Particolarmente significativa è, inoltre, la formulazione del motivo di rifiuto fondato sulla violazione dei diritti fondamentali. Gli artt. 12 e 16 del Regolamento lo ammettono soltanto in situazioni eccezionali, quando vi siano validi motivi per ritenere, sulla base di elementi concreti e oggettivi, che l'esecuzione o l'applicazione dell'ordine comporterebbe una violazione manifesta di un diritto fondamentale sancito dall'art. 6 TUE e dalla Carta. La Direttiva OEI, invece, consente il rifiuto quando vi siano seri motivi per ritenere che l'esecuzione dell'atto richiesto sia incompatibile con gli obblighi dello Stato di esecuzione ai sensi dell'art. 6 TUE e

fuori delle ipotesi di notifica, l'intervento dell'autorità pubblica dello Stato di esecuzione resta eventuale e successivo, mentre il primo filtro operativo è rimesso al destinatario privato⁴⁹. E proprio sotto questo punto di vista, il ruolo centrale attribuito alle piattaforme, si mostra nella sua problematicità. Il prestatore può segnalare difficoltà di esecuzione, interferenze con immunità, privilegi o libertà fondamentali, nonché conflitti con obblighi derivanti da ordinamenti di Paesi terzi. Tuttavia, esso non è un'autorità indipendente di garanzia, non è collocato in posizione di neutralità istituzionale e non dispone necessariamente delle competenze giuridiche richieste per valutare compiutamente l'incidenza dell'ordine sui diritti fondamentali. A ciò si aggiunge che il prestatore opera sotto la pressione di un possibile apparato sanzionatorio, circostanza che può incentivare l'adempimento anche nei casi in cui un controllo pubblico più approfondito sarebbe opportuno⁵⁰.

Il ridimensionamento del ruolo dello Stato di esecuzione emerge, poi, anche sul piano temporale. Esso, quando viene coinvolto, dispone di termini assai brevi (10 giorni) per far valere eventuali motivi di rifiuto⁵¹. Inoltre, il Regolamento non contiene una disposizione analoga a quella dell'OEI che impone, ove in un caso interno comparabile sia necessaria l'autorizzazione di un organo giurisdizionale nello Stato di esecuzione, il ricorso alla medesima autorizzazione, con il risultato che il controllo dello Stato di esecuzione sia meno intenso e strutturato⁵².

Anche il regime dei rimedi sembra confermare questa impostazione. La persona i cui dati siano stati prodotti mediante un ordine europeo di produzione ha diritto a un ricorso effettivo dinanzi a un organo giurisdizionale dello Stato di emissione. La scelta è coerente con la giurisprudenza della Corte di giustizia in materia di ordine europeo di indagine, che ha valorizzato la necessità di rimedi effettivi nello Stato emittente⁵³; tuttavia, il Regolamento non contempla espressamente la possibilità di impugnare l'ordine anche nello Stato di esecuzione. La clausola secondo cui restano salve le garanzie dei diritti fondamentali nello Stato di esecuzione presenta, sotto questo profilo, un contenuto ambiguo: non è chiaro se essa possa fondare un controllo effettivo sulle garanzie previste dall'ordinamento dello Stato di esecuzione, né se il giudice dello Stato di emissione sia sempre il soggetto più idoneo a svolgere tale verifica. In molti casi, lo Stato di esecuzione non viene neppure informato circa l'esecuzione di un ordine rivolto a un prestatore stabilito o rappresentato nel proprio territorio. La ragione di una simile scelta risiede nella peculiarità del nuovo modello: lo Stato di esecuzione è spesso tale soltanto perché in esso si trova il rappresentante legale o lo stabilimento designato del prestatore di servizi, mentre il procedimento, il reato e la persona interessata possono non presentare alcun legame effettivo con quell'ordinamento⁵⁴.

Questa spiegazione, tuttavia, non esaurisce il problema. Il Regolamento non sembra considerare

della Carta. La differenza lessicale non è neutra: nel Regolamento *e-Evidence* la tutela dei diritti fondamentali appare costruita come eccezione qualificata alla regola dell'esecuzione, mentre nell'OEI essa opera come limite generale alla cooperazione.

49. Cfr. Commissione europea, doc. COM(2018) 225, 17 aprile 2018.

50. TOSZA 2021, p. 8 ss.

51. Cfr. art. 12 Reg.

52. Segnatamente, come detto, dieci giorni dalla notifica, ove prevista (art. 12, paragrafo 1, Reg.); cinque giorni lavorativi dalla ricezione della documentazione proveniente dall'autorità di emissione a seguito dell'inadempimento del privato, in linea generale (art. 16, paragrafo 2, Reg.).

53. Cfr. Corte giust., 11 novembre 2021, C-852/19, *Gavanozov II*, sul diritto a un ricorso effettivo nello Stato di emissione dell'ordine europeo di indagine; con riferimento all'art. 18 Reg. e ai profili problematici del rimedio nello Stato di emissione, si veda KIEJNICH-KRUK 2024, p. 135.

54. Cfr. art. 8 Reg., sulla notifica all'autorità di esecuzione e sulle ipotesi in cui essa non è richiesta; art. 7 Reg., sull'individuazione del destinatario dell'ordine nello stabilimento designato o nel rappresentante legale; art. 3, nn. 13-16, Reg., sulle nozioni di Stato di emissione e Stato di esecuzione, sul carattere in parte artificiale del collegamento con lo Stato di esecuzione, quando esso dipenda dalla sola localizzazione del rappresentante o dello stabilimento designato del prestatore.

adeguatamente l'ipotesi in cui la persona interessata risieda in uno Stato membro diverso sia da quello di emissione sia da quello in cui è stabilito il rappresentante del prestatore. In tale situazione, l'autorità più prossima alla tutela delle prerogative individuali potrebbe non coincidere né con quella di emissione né con quella di esecuzione, bensì con quella dello Stato di residenza dell'interessato. La mancata previsione di un coinvolgimento di tale Stato è stata letta come una occasione mancata per costruire un sistema di garanzie più aderente alla natura realmente transnazionale della prova elettronica⁵⁵.

Alla luce di questi elementi, il pacchetto *e-Evidence* si colloca in una posizione ambivalente. Da un lato, positivizza condizioni, categorie di dati, requisiti di proporzionalità, limiti oggettivi e rimedi, superando la frammentarietà delle prassi precedenti e offrendo una base uniforme all'acquisizione transfrontaliera delle prove elettroniche. Dall'altro, il modello di cooperazione diretta, il ridimensionamento dello Stato di esecuzione, la centralità del prestatore di servizi e la debolezza di alcuni obblighi informativi fanno emergere il rischio di una riduzione del livello di tutela rispetto agli standard maturati nell'ambito dell'OEI e della giurisprudenza della Corte di giustizia.

Il punto, naturalmente, non è negare l'esigenza di strumenti più rapidi ed efficaci. La volatilità dei dati, la loro frequente delocalizzazione e la centralità tecnica dei prestatori rendono spesso inadeguati i canali cooperativi tradizionali. Tuttavia, l'efficienza investigativa non può tradursi in una riduzione strutturale delle garanzie. Se la cooperazione diretta costituisce la via più funzionale per raggiungere i dati detenuti dalle piattaforme, essa deve essere accompagnata da controlli capaci di compensare la disintermediazione dello Stato di esecuzione e il coinvolgimento di soggetti privati nella fase esecutiva⁵⁶.

In conclusione, il sistema delineato dal Regolamento non appare privo di garanzie, ma presenta un equilibrio ancora instabile. La sua tenuta dipenderà dalla capacità delle autorità nazionali e della giurisprudenza europea di interpretare i requisiti di necessità e proporzionalità in modo sostanziale, di assicurare un controllo effettivo sugli ordini più invasivi, di valorizzare il diritto all'informazione e al ricorso e di evitare che il prestatore di servizi divenga il principale filtro di tutela dei diritti individuali.

La questione decisiva non sembra dunque consistere nella necessità di stabilire se la cooperazione diretta con i prestatori di servizi sia, in astratto, compatibile con la tutela dei diritti fondamentali, quanto piuttosto nell'individuare quali siano le condizioni in cui essa possa esserlo, senza che la rapidità nell'accesso alla prova elettronica si traduca in una riduzione strutturale del controllo giurisdizionale, dell'informazione dell'interessato e dell'effettività dei rimedi.

6. Considerazioni conclusive.

Complessivamente, il pacchetto *e-Evidence* sembra costituire una prima effettiva risposta alla trasformazione digitale dell'accertamento penale, attraverso l'introduzione di un modello di accesso più diretto, uniforme e calibrato sulle caratteristiche dell'ambiente digitale⁵⁷.

Le novità non si esauriscono nella creazione di nuovi strumenti acquisitivi ma investono l'intero processo penale. L'autorità giudiziaria non si rivolge più, solo, ad un'altra autorità statale, secondo il paradigma classico della cooperazione penale, bensì direttamente al prestatore di servizi digitali determinando, parallelamente, una parziale disintermediazione dello Stato di esecuzione ed una crescente responsabilizzazione dei soggetti privati che detengono, organizzano e/o rendono accessibili le informazioni digitali⁵⁸.

55. Cfr. CHRISTAKIS 2025, p. 198.

56. SACHOULIDOU 2024, p. 267 ss.; TOSZA 2024, p. 147 ss., pp. 152-153; CALAVITA 2021, p. 204; ROSANÒ 2020, pp. 16-17.

57. Cfr.: considerando nn. 7-9 e 12 Regolamento (UE) 2023/1543; Commissione europea, Impact Assessment, SWD (2018) 118 final, §§ 2.1-2.2; Corte suprema di cassazione, Ufficio del Massimario e del Ruolo, Servizio penale, Rel. n. 25/2026, 7 aprile 2026, Parte I, § 1.

58. Sulla cooperazione diretta con i prestatori di servizi quale elemento qualificante del nuovo modello e sul conseguente ridimensionamento dello schema interstatale tradizionale, si veda il considerando 12 Regolamento (UE) 2023/1543; gli artt. 7, 9-11 Regolamento (UE) 2023/1543.

In questo scenario i prestatori di servizi possono essere definiti come *gatekeepers* della cooperazione penale digitale⁵⁹: non titolari della funzione giurisdizionale, né del potere di decidere sull' *an* dell'acquisizione probatoria, bensì detentori delle condizioni tecniche e organizzative di accesso alla prova. Del resto, in assenza di un loro diretto coinvolgimento, l'effettività dell'acquisizione probatoria rischierebbe di risultare compromessa.

Come analizzato, il pacchetto tenta di governare questa interdipendenza attraverso una duplice strategia: da un lato, tipizza gli ordini europei, le categorie di dati, i presupposti di emissione, i termini di risposta e i rimedi; dall'altro, attraverso la Direttiva (UE) 2023/1544, costruisce l'interfaccia organizzativa necessaria affinché l'ordine possa raggiungere operatori spesso transnazionali, imponendo la designazione di uno stabilimento o la nomina di un rappresentante legale. Il legislatore europeo ha dunque predisposto le condizioni affinché il potere di richiedere la cooperazione diretta all'infrastruttura privata che governa il dato possa essere effettivamente esercitato.

L'equilibrio resta, tuttavia, instabile.

La maggiore efficienza dell'acquisizione transfrontaliera si ottiene attraverso un modello che concentra molte garanzie nello Stato di emissione, riduce il ruolo ordinario dello Stato di esecuzione e attribuisce al prestatore la funzione di primo filtro operativo. Se, da un certo punto di vista, ciò produce benefici evidenti in termini di tempestività, specialmente di fronte a dati esposti a cancellazione, sovrascrittura o dispersione; d'altro canto,

solleva interrogativi circa l'effettività della tutela rivolta alla persona interessata⁶⁰.

Sebbene il pacchetto nasca con l'intento di rispondere all'esigenza di acquisire prove elettroniche nel corso di procedimenti penali nei quali l'elemento transfrontaliero generalmente dipende dalla localizzazione del prestatore di servizi, la logica che esso inaugura (accesso diretto al soggetto privato che detiene la prova, riduzione dell'intermediazione statale, centralità della compliance privata), potrebbe incidere in modo più ampio sul futuro della cooperazione penale europea.

La sfida sembra essere duplice. Sul piano dell'effettività occorrerà in primo luogo verificare se i prestatori di servizi riusciranno a rispondere agli ordini europei nei tempi e con il livello di precisione stabiliti; in secondo luogo, se gli uffici giudiziari sapranno dotarsi di competenze tecniche e organizzative adeguate. Sul piano delle garanzie sarà necessario evitare che la rapidità dell'accesso alla prova elettronica si traduca in una riduzione strutturale del controllo giurisdizionale, del diritto all'informazione e dell'effettività dei rimedi.

In un simile contesto il compito del diritto processuale penale europeo sembra essere quello di governare la (necessaria) relazione tra autorità statali e prestatori di servizi digitali, assicurando che l'efficienza della cooperazione diretta non comporti l'esternalizzazione delle garanzie e che i prestatori di servizi, quali snodo indispensabile per l'acquisizione probatoria, non si trasformino in quel luogo in cui il controllo pubblico sulla formazione della prova si attenui.

Riferimenti bibliografici

- A. AGUINALDO, P. DE HERT (2025), *Moving in the Right Direction for Transborder Access to Digital Evidence in Criminal Matters? The Council of Europe and the Second Additional Protocol Introducing Direct Cooperation Mechanisms*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025

59. In senso affine, sul rischio di una privatizzazione della fiducia reciproca e sul ruolo dei prestatori di servizi quali snodi centrali della cooperazione penale digitale, si veda MITSILEGAS 2018, pp. 264-265; TOSZA 2024, p. 143 ss., p. 159 ss., ove i prestatori di servizi sono descritti come *gatekeepers* dei dati e, nel nuovo modello di cooperazione diretta, come primo filtro delle richieste provenienti dalle autorità di law enforcement, con conseguente spostamento su soggetti privati di valutazioni potenzialmente incidenti anche sulla tutela dei diritti fondamentali.

60. In senso critico sul modello di cooperazione diretta, con particolare riferimento alla concentrazione delle garanzie nello Stato di emissione, al ridimensionamento dell'autorità di esecuzione e al ruolo del prestatore di servizi quale primo filtro operativo dell'ordine, si veda SACHOULIDOU 2024, p. 267 ss.

- S. ALLEGREZZA (2020), *L'acquisizione delle prove elettroniche nel processo penale*, in "Rivista italiana di diritto e procedura penale", 2020
- M. CAIANIELLO (2022), *Il procedimento penale europeo*, Giappichelli, 2022
- O. CALAVITA (2025), *L'ordine europeo di indagine penale. Presente e futuro della cooperazione probatoria nell'Unione europea*, CEDAM, 2025
- O. CALAVITA (2021), *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in "La legislazione penale", 2021
- T. CHRISTAKIS (2025), *From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025
- M. CORHAY (2021), *Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal*, in "European Papers", 2021, n. 1
- S. CUTRIGNELLI (2023), *La prova informatica nella pratica investigativa*, in "disCrimen", 2023, n. 2
- V. DASKAL (2015), *The Un-Territoriality of Data*, in "Yale Law Journal", 2015, n. 2
- A. DE MAIO (2026), *L'acquisizione delle prove elettroniche nello spazio di libertà, sicurezza e giustizia: prime applicazioni dell'e-Evidence package*, in "RLF Express", 2026, n. 9
- F. ERTOLA (2025), *L'ordine europeo di indagine penale*, in G. Ubertis, G.P. Voena (a cura di), "Trattato di procedura penale", Giuffrè, 2025
- J.A. ESPINA RAMOS (2025), *European Preservation and Production Orders: A Non-Exclusive Approach to E-Evidence within the EU*, in "EuCrim", 2025
- G. FORLANI (2023), *The E-Evidence Package. The Happy Ending of a Long Negotiation Saga*, in "EuCrim", 2023, n. 2
- V. FRANSSEN, S. TOSZA (2025), *Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025
- A. GAUDIERI (2023), *Novità in tema di cooperazione giudiziaria: i nuovi ordini europei di conservazione e produzione delle prove elettroniche*, in "Diritto penale e processo", 2023
- R.M. GERACI (2019), *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-Evidence*, in "Cassazione penale", 2019, n. 3
- C. GRANDI (2021), *Il mutuo riconoscimento dei provvedimenti di confisca alla luce del Regolamento (UE) 2018/1805*, in "La legislazione penale", 31 maggio 2021
- A. KIEJNICH-KRUK (2024), *Quo vadis Europa? Balancing between efficiency and guarantees in criminal proceedings using the example of EU production and preservation orders*, in "New Journal of European Criminal Law", 2024, n. 2
- A.M. MAUGERI (2019), *Il regolamento (UE) 2018/1805 per il reciproco riconoscimento dei provvedimenti di congelamento e di confisca: una pietra angolare per la cooperazione e l'efficienza*, in "Diritto penale contemporaneo", 16 gennaio 2019
- V. MITSILEGAS (2018), *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-Evidence*, in "Maastricht Journal", 2018, n. 3
- A. NASCIMBENI (2022), *Ordine europeo di indagine penale e diritti fondamentali*, in "Rivista italiana di diritto e procedura penale", 2022

- P. RAUCCI (2025), *L'ordine europeo di indagine e prove digitali: tra presunzione di legittimità degli atti compiuti all'estero e diritti fondamentali*, in "Giurisprudenza penale", 2025
- A. ROSANÒ (2020), *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, in "La legislazione penale", 16 ottobre 2020
- A. SACHOULIDOU (2024), *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of "judicial" cooperation*, in "New Journal of European Criminal Law", 2024, n. 3
- F. SIRACUSANO (2017), *La prova informatica transnazionale: un difficile "connubio" tra innovazione e tradizione*, in "Processo penale e giustizia", 2017
- D. SVANTESSON, A.M. OSULA (2025), *Unresolved Jurisdictional Issues in Law Enforcement Access to Data*, in V. Franssen, S. Tosza (Eds.), "The Cambridge Handbook of Digital Evidence in Criminal Investigations", Cambridge University Press, 2025
- S. TOSZA (2024), *Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, in "Common Market Law Review", 2024, n. 1
- S. TOSZA (2021), *Internet service providers as law enforcers and adjudicators. A public role of private actors*, in "Computer Law & Security Review", vol. 43, 2021
- T. WAHL (2023), *E-Evidence Regulation and Directive Published*, in "Eucrim", 2023



SILVIA BONETTI

La *data retention*: alcune riflessioni nella prospettiva del diritto privato della protezione dei dati personali

Il presente contributo prende in esame, in una prospettiva di diritto privato, il ruolo dei fornitori di servizi di comunicazione elettronica nell'ambito delle investigazioni digitali, con particolare riferimento all'impiego dello strumento della *data retention*. In tale contesto, emerge chiaramente come il perseguimento di finalità pubblicistiche di lotta alla criminalità richieda necessariamente la cooperazione di operatori privati, i quali, in qualità di titolari del trattamento, assumono un ruolo centrale e altamente responsabilizzato nel garantire l'adozione di misure tecniche e organizzative adeguate a far fronte ai rischi per la sicurezza e l'integrità delle informazioni degli utenti interessati.

*Data retention – Conservazione di dati personali – Acquisizione di dati personali
Principi applicabili al trattamento – Accountability*

Data retention: some private law remarks in the light of the protection of personal data

This article analyses, from a private law perspective, the role of electronic communications service providers in the context of digital investigations, with reference to data retention. Within this framework, it clearly emerges that the pursuit of public interests in combating crime necessarily entails the cooperation of private operators, who, in their capacity as data controllers, play a central and highly responsible role in ensuring the adoption of appropriate technical and organizational measures to address risks to the security and integrity of information relating to the users concerned.

*Data retention – Storage of personal data – Access to personal data
Principles relating to processing of personal data – Accountability*

L'Autrice è assegnista di ricerca in Diritto privato presso il Dipartimento di Scienze Giuridiche dell'Università di Verona

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli

SOMMARIO: 1. Introduzione: la rilevanza della *data retention* per il diritto privato della protezione dei dati personali. – 2. Lo statuto eurounitario della *data retention* nella elaborazione della Corte di giustizia UE: dalla sentenza *Digital Rights*... – 3. (Segue)... alla rinnovata disciplina nel diritto italiano: l'art. 132 del Codice in materia di protezione dei dati personali. – 4. Il ruolo del diritto della protezione dei dati personali nella conservazione e acquisizione di informazioni per finalità di contrasto alla criminalità: profili di criticità. – 5. Qualche osservazione conclusiva.

1. Introduzione: la rilevanza della *data retention* per il diritto privato della protezione dei dati personali

La *data retention*, anche se tema pressoché sconosciuto al civilista e, per contro, oggetto di ampie riflessioni nell'ambito del diritto penale e processuale penale e, precisamente, nel contesto delle investigazioni digitali¹, indubbiamente richiede di essere letta e analizzata anche nell'angolo visuale del diritto privato della protezione dei dati personali.

Lo strumento investigativo concretamente si sostanzia nell'obbligo, per i fornitori di servizi di comunicazione elettronica, di conservare per un prolungato periodo di tempo i dati (anche di natura personale) generati dall'uso di tali servizi, a cui consegue la possibilità, per l'autorità giudiziaria, di acquisirli per finalità di prevenzione, indagine, accertamento e perseguimento di reati, nonché per l'esecuzione di sanzioni penali. La sua attuazione impone, dunque, un necessario bilanciamento con i diritti fondamentali del rispetto della vita privata e della vita familiare e della protezione delle informazioni di natura personale².

Nella relativa disciplina trovano, però, riferimento i soli dati cc.dd. esterni del traffico delle

comunicazioni elettroniche, con la conseguenza che dal suo ambito di applicazione devono ritenersi esclusi obblighi di conservazione e poteri di acquisizione che abbiano ad oggetto dati relativi al contenuto delle comunicazioni stesse, ciò che comporterebbe una eccessiva intrusione nella sfera personale dei singoli utenti.

Tale esclusione, tuttavia, non ridimensiona la portata dirompente dell'impatto di una simile disciplina nella sfera giuridica dei soggetti interessati coinvolti, poiché la conservazione e la successiva condivisione di dati – quali quelli necessari ad individuare la fonte di una comunicazione, la sua destinazione, la data, l'ora e la durata della stessa, così come la posizione geografica dei soggetti coinvolti nella conversazione –, sebbene funzionali a fare fronte a generali esigenze di pubblica sicurezza, evidentemente realizzano una significativa ingerenza nei diritti fondamentali degli individui. È pertanto inevitabile che il funzionamento della *data retention* e le garanzie che ad essa si accompagnano a tutela degli utenti delle comunicazioni elettroniche vengano inquadrati anche nella prospettiva dei principi che governano il diritto della protezione dei dati di natura personale³.

1. In argomento, nella precisa prospettiva del penalista e del processual penalista, che pure è necessario comprendere per poter proporre qualche considerazione sul versante del diritto privato della protezione dei dati personali, v. almeno FLOR-PANATTONI 2023; FLOR-MARCOLINI 2022; FLOR 2015.

2. Ci si riferisce, in particolare, ai diritti enunciati agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

3. Ma v. anche FLOR-PANATTONI 2023, pp. 492-494, i quali, in ragione della natura particolarmente intrusiva degli strumenti investigativi digitali (con riguardo specificamente al *lawful hacking*), individuano soprattutto nella

2. Lo statuto eurounitario della *data retention* nella elaborazione della Corte di giustizia UE: dalla sentenza *Digital Rights*...

Al fine di sviluppare il tema nella prospettiva annunciata, si rende in via preliminare necessario comprendere, sia pure per tratti essenziali, l'evoluzione storica – normativa e giurisprudenziale – della *data retention*.

Sospinto dalla introduzione, in numerosi ordinamenti nazionali, di discipline specifiche che individuavano, per i fornitori di servizi di comunicazione, precisi obblighi di conservazione dei dati relativi al traffico e all'ubicazione, al fine di consentire alle autorità competenti, ove necessario, di impiegarli per esigenze di pubblica sicurezza, il legislatore (allora) comunitario ha ritenuto opportuno intervenire con l'adozione di una disciplina di armonizzazione: la direttiva 2006/24/CE⁴. Tale strumento normativo si distingueva, per specialità, dalla di poco precedente direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, la quale, a sua volta, traduceva e adattava allo specifico settore di riferimento i principi generali dell'allora vigente direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati.

Sebbene le normative nazionali in materia di *data retention* avessero sicuramente il pregio di cogliere l'importanza dell'acquisizione di questi dati nelle azioni di contrasto alla criminalità, esse rivelavano, al contempo, un punto di debolezza

nel loro carattere frammentario e disomogeneo, sul piano tanto della regolamentazione giuridica quanto della attuazione tecnica, e ciò in un settore, quello delle comunicazioni elettroniche, idoneo ad assumere una dimensione anche transnazionale, che avrebbe dovuto, perciò, trovare uniforme regolamentazione all'interno della allora Comunità (oggi Unione) europea⁵.

La direttiva sulla *data retention* del 2006, che per anni è stato primo e principale strumento normativo per consentire la conservazione e la successiva acquisizione di dati nel contesto delle investigazioni digitali, diviene ben presto oggetto di uno scrutinio di legittimità da parte della Corte di giustizia, complice pure lo sviluppo di una maggiore sensibilità, anche giuridica, per la tutela delle informazioni personali a fronte della introduzione di tecnologie digitali sempre più innovative.

Nel 2014, con la pronuncia *Digital Rights*⁶, la direttiva sulla *data retention* viene dichiarata invalida. Essa difetta – nella visione della Corte – di un coerente bilanciamento tra gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, da un lato, e l'interesse generale alla lotta e alla repressione della criminalità (anche organizzata e terroristica) dall'altro. Poiché si discorre di due esigenze di protezione contrapposte, ma entrambe di rango fondamentale, le previsioni della direttiva avrebbero dovuto essere ideate di modo da far sì che la regressione di una in favore dell'altra fosse ispirata al principio eurounitario di proporzionalità, così come enunciato nell'art. 52 della Carta dei diritti fondamentali dell'Unione

cybersecurity, e non solo nella privacy e nella protezione dei dati personali, un autonomo interesse di tutela da porre in compensazione con le esigenze di pubblica sicurezza.

4. Si tratta della Direttiva riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (nota anche come direttiva sulla *data retention* o direttiva Frattini).
5. Cfr. considerando n. 6 della direttiva 2006/24/CE, ove si osserva che le differenze tra le normative dei singoli Stati Membri "costituiscono un ostacolo al mercato interno delle comunicazioni elettroniche". Lo strumento di indagine dell'accesso ai dati conservati dai fornitori dei servizi di comunicazioni elettroniche rappresenta inoltre efficace strumento per la lotta alle forme di criminalità anche internazionale, sicché solo una disciplina armonizzata sarebbe stata in grado di massimizzare il livello di cooperazione giudiziaria in materia penale nello spazio (allora) comunitario. Per tale ultimo rilievo v. soprattutto FLOR-MARCOLINI 2022, p. 7.
6. Cfr. Corte giust. Ue, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights*, e i commenti di CASCIONE 2014 e TRUCCO 2014. V. pure il commento di FLOR 2014.

europea⁷, e che la regolamentazione del rapporto fra queste seguisse regole chiare e precise, in grado di assicurare la minima interferenza nella situazione giuridica che viene compressa per estendere lo spazio di operatività all'altra.

Diversi sono i passaggi della direttiva, che, così come emerge dalle argomentazioni della Corte, si pongono irrimediabilmente in contrasto con il principio di proporzionalità. Viene anzitutto in rilievo l'osservazione per cui l'obbligo di conservazione colpisce indistintamente tutti i dati relativi alle comunicazioni elettroniche, senza che operi alcun tipo di esclusione che, per esempio, circoscriva tale trattamento ad un determinato arco temporale, ovvero restringa la raccolta dei dati ad una precisamente individuata area geografica. Altrettanto indeterminata risulta poi la nozione di "reati gravi", con riferimento ai quali è possibile avere accesso ai dati conservati dai fornitori, la cui specificazione è demandata ai singoli ordinamenti nazionali. Non adeguatamente individuate sono, ancora, le categorie di soggetti abilitati all'accesso, quest'ultimo, peraltro, nemmeno sottoposto a precise limitazioni o subordinato all'autorizzazione di un giudice o di una autorità amministrativa indipendente. Indefiniti risultano altresì i criteri oggettivi sulla base dei quali individuare la durata esatta dell'obbligo. Da ultimo, le contestazioni della Corte sottolineano la mancanza di specifiche regole volte a garantire la sicurezza e la protezione dei dati conservati per periodi di tempo anche prolungati⁸.

Al di là del mancato bilanciamento tra situazioni giuridiche tra loro in conflitto, il testo

normativo risulta insoddisfacente anche – come in dottrina è stato osservato – per i numerosi rinvii ai singoli ordinamenti nazionali per la specificazione di alcuni aspetti – tutt'altro che marginali – della disciplina. Per quanto lo strumento stesso della direttiva presupponga, per sua natura, un intervento di recepimento da parte dei singoli Stati membri, l'insistito ricorso alla tecnica del rinvio con riguardo alla determinazione di profili decisivi per il concreto funzionamento della *data retention*, pare, invero, tradire il generale obiettivo di armonizzazione delle specifiche previsioni già in vigore negli ordinamenti nazionali, così vanificando la reale portata applicativa della direttiva⁹.

A partire dalla pronuncia *Digital Rights*, cruciali in questa materia diventano i numerosi interventi della Corte di giustizia, che, anche con numerose pronunce successive, ha contribuito a delineare un vero e proprio statuto eurounitario sul tema della *data retention*; da questi nemmeno la presente riflessione può prescindere, e perciò se ne propongono a seguire gli snodi più rilevanti.

Quale conseguenza della invalidità della direttiva 2006/24/CE la disciplina di riferimento torna ad essere quella, più generale, di cui alla precedente direttiva 2002/58/CE (c.d. direttiva *e-privacy*), che la direttiva sulla *data retention* aveva meglio dettagliato e adeguato al contesto delle investigazioni digitali. In questo senso, confermando la collocazione della materia nell'ambito del diritto eurounitario (allora comunitario), si esprime la Corte di giustizia con la pronuncia del 21 dicembre 2016 (c.d. pronuncia *Tele2*)¹⁰. Principio ispiratore del legislatore della

7. A più riprese la Corte di giustizia richiama nelle proprie riflessioni in materia di *data retention* il principio di proporzionalità, come si vedrà anche in seguito in Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*, e Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*.

8. Più nel dettaglio sui singoli profili di incompatibilità della direttiva con il principio eurounitario di proporzionalità si soffermano FLOR-MARCOLINI 2022, pp. 8-11.

9. V., in argomento, FLOR-MARCOLINI 2022, p. 11, che, per tale ragione, si esprimono in termini di vuoto contenutistico della direttiva 2006/24/CE.

10. Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*. In aggiunta rispetto a quanto già affermato nella pronuncia *Digital Rights*, la Corte di giustizia individua qui, con maggiore precisione, tre distinti momenti, in relazione a ciascuno dei quali apposite tutele devono essere implementate affinché ogni singola disciplina nazionale possa dirsi conforme al concetto eurounitario di proporzionalità: la conservazione, l'accesso e la sicurezza nella fase di conservazione. Anzitutto, con riguardo alla fase della conservazione dei dati, si mette in luce la necessità di introdurre negli ordinamenti nazionali norme chiare, idonee a identificare con precisione *ex ante* le condizioni al sussistere delle quali sorge per i fornitori dei servizi di comunicazioni un obbligo di tale sorta. La successiva acquisizione di dati dovrà essere limitata alle sole ipotesi in cui si riveli essenziale per una adeguata lotta alla criminalità grave, concetto questo che dovrà essere adeguatamente specificato

direttiva *e-privacy* – osservano i giudici di Lussemburgo – è senza dubbio quello della riservatezza dei dati, sicché la *data retention*, che – come detto – prende la forma di obblighi di conservazione e comunicazione, è da collocarsi nell’ambito delle limitazioni a tale principio, precisamente individuate, nel testo della direttiva, all’art. 15. Segnatamente, si prevede che la regola relativa alla riservatezza delle comunicazioni, l’obbligo di cancellazione o anonimizzazione dei dati del traffico una volta venuta meno la finalità di trasmissione della comunicazione, così come l’anonimizzazione dei dati relativi all’ubicazione (diversi dai dati del traffico), possano essere oggetto di limitazione, da parte di una normativa nazionale, quando tale limitazione sia da considerarsi misura necessaria, opportuna e proporzionata nei settori della “sicurezza nazionale [...], della difesa, della sicurezza pubblica”, ovvero “per la prevenzione, ricerca, accertamento e perseguimento dei reati”¹¹.

Lo stato più avanzato delle elaborazioni europee in materia di *data retention* lo si raggiunge soltanto il 6 ottobre 2020, con la sentenza *Quadrature*¹². Ribadite le affermazioni già enunciate nelle precedenti pronunce *Digital Rights* e *Tele2*, i giudici di Lussemburgo sviluppano l’operatività del principio di proporzionalità intorno a tre distinti fattori: la variabile intensità della interferenza nei diritti fondamentali dell’individuo; la gravità del fenomeno criminoso che si intende combattere; la qualità e la quantità delle garanzie che il legislatore nazionale adotta.

All’esito della valutazione di proporzionalità, che tiene conto di tali tre elementi, può risultare una interferenza di minima entità nel bene riservatezza, la quale è perciò da dirsi compatibile con la lotta contro ogni forma di criminalità, non necessariamente grave¹³; per converso, solo l’esigenza pubblica di perseguire crimini di più elevata gravità giustifica una maggiore intrusione nella sfera privata degli individui. Una regola (l’art. 15 della direttiva 2002/58/CE), che si pone come eccezionale rispetto alla tutela dei diritti fondamentali e che potenzialmente coinvolge il trattamento di un numero significativo di dati, non potrà, infatti, prescindere da criteri rigorosi che ne regolano il bilanciamento con la riservatezza e la protezione delle informazioni. Di conseguenza, non sarà sufficiente a legittimare la conservazione e l’acquisizione di dati (anche) personali la generica finalità di prevenzione e contrasto alla criminalità; piuttosto, soltanto la repressione di forme di criminalità che possano definirsi gravi potrà giustificare una più ampia compressione dei diritti dell’individuo. E, in ogni caso, tale compressione andrà accompagnata da garanzie procedurali che possano mitigare gli effetti negativi che in ipotesi si potranno riversare sugli utenti.

Fondamentale garanzia, di cui i giudici di Lussemburgo promuovono l’implementazione, è quella del modello di conservazione mirata dei dati delle comunicazioni (o *targeted retention*)¹⁴. Prevedere un obbligo di conservazione generalizzata e indifferenziata dei dati di tutti coloro che

per il tramite del preciso riferimento alle singole fattispecie di reato che siano a questo riconducibili. L’accesso dovrà inoltre essere subordinato al preventivo controllo da parte di una autorità giudiziaria o amministrativa indipendente. La sicurezza dei dati conservati, infine, andrà realizzata mediante l’introduzione dell’obbligo per i fornitori di adottare, durante il periodo di conservazione, degli standard di protezione elevati, che impongano loro, allo scadere del periodo di tempo di riferimento, la cancellazione irreversibile delle informazioni raccolte.

11. Cfr. art. 15, par. 1, della direttiva 2002/58/CE.

12. Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*.

13. Conclusione, questa, già raggiunta dalla Corte con la sentenza *Ministerio Fiscal*. Cfr. Corte giust. Ue, 2 ottobre 2018, causa C-207/16.

14. Sulla conservazione targhetizzata v., in particolare, Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner*, ove si ribadisce nuovamente il rapporto tra regola ed eccezione in materia di *data retention*, lì dove la regola si identifica nella cancellazione o anonimizzazione delle informazioni per le quali le finalità del trattamento possono dirsi raggiunte ed esaurite ed è, invece, eccezionale la loro ultra-conservazione. Si critica dunque, anche in questa successiva pronuncia, l’impostazione che fa discendere dalla disciplina della *data retention*, quale strumento investigativo di contrasto alla criminalità grave, obblighi di conservazione generali e indifferenziati. Per contro, se la conservazione generalizzata è da considerarsi inaccettabile in una società democratica, i modelli di

utilizzano mezzi di comunicazione elettronica significherebbe, nella sostanza, estendere nel tempo il loro trattamento, o comunque realizzarne uno nuovo, senza limitazione alcuna, in deroga al rapporto regola-eccezione, così come individuato nella direttiva *e-privacy*, e in contrasto pure con l'esigenza, di segno opposto, di contenere entro i limiti della ragionevolezza la regressione di un diritto fondamentale a fronte dell'interesse generale alla sicurezza pubblica.

Fra i criteri idonei a limitare la conservazione che la Corte espressamente suggerisce vi sono il criterio geografico, che circoscrive la raccolta dei soli dati che sono localizzabili in una determinata area ad alto rischio di criminalità; il criterio personale, che consente di identificare quelle categorie di soggetti o quei singoli soggetti che rivelino una stretta connessione con forme di criminalità grave o che, in prima persona, costituiscono una minaccia per la sicurezza; e il criterio temporale, che limita la conservazione ad un determinato periodo di tempo, allo scadere del quale la regola generale,

ossia quella della cancellazione o anonimizzazione dei dati, nuovamente si riespande¹⁵.

Si delineano così, modellati dal formante giurisprudenziale, i principi che devono permeare ogni disciplina, anche nazionale, in materia di *data retention*.

3. (Segue)... alla rinnovata disciplina nel diritto italiano: l'art. 132 del Codice in materia di protezione dei dati personali

Esaminati, per sommi capi, i principi fissati dal diritto eurounitario, occorre ora assumere una prospettiva di diritto interno e analizzare la disciplina in materia di *data retention* che il legislatore italiano, in forza della riserva concessagli dall'art 15 della direttiva *e-privacy*¹⁶, ha introdotto.

La fonte principale che, nell'ordinamento interno, regola gli obblighi in capo agli *internet service provider* di conservare i dati (ma non il contenuto) del traffico telefonico e telematico, nonché le modalità di acquisizione di tali dati da parte delle autorità di pubblica sicurezza, è

conservazione mirata (basata, per esempio, su persone o luoghi) e rapida (o *quick freeze*), si rivelano funzionali alle esigenze di indagine senza tradursi in una eccessiva compressione del diritto alla riservatezza. È dunque, in sintesi, vietata, per finalità di lotta alla criminalità grave e di prevenzione a minacce gravi per la sicurezza pubblica, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Se posta in essere per le medesime finalità, non è invece in contrasto con il diritto eurounitario una disciplina nazionale che preveda la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, purché essa sia limitata nel tempo e allo stretto necessario; parimenti ammessa è la conservazione generalizzata e indifferenziata dei dati relativi all'identità degli utenti delle comunicazioni elettroniche. Sulla selezione dei dati oggetto di conservazione riflettono anche Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*; Corte giust. Ue, 30 gennaio 2024, causa C-118/22, *Direktor* commentata da GRILLO 2024, p. 832 ss., nonché Corte giust. Ue, 28 novembre 2024, causa C-80/2023, *Ministerstvo na vatreshnite raboti*.

15. Richiama tali criteri Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*. Anche quando oggetto di conservazione siano categorie particolari di dati personali (nella specie, dati genetici e biometrici), il relativo trattamento – sempreché sia posto in essere alle condizioni enucleate dalla giurisprudenza eurounitaria – non perde di liceità, poiché si riconosce che tali dati possano rivelarsi utili per ulteriori fini di pubblica sicurezza. Ciò che invece è da scongiurare è una raccolta sistematica e indiscriminata di tali informazioni, poiché in contrasto anche con il principio di minimizzazione, il cui rispetto, con riferimento alla conservazione di particolari categorie di dati, è da sottoporre ad un controllo ancor più rigoroso. In argomento v. Corte giust. Ue, 30 gennaio 2024, causa C-118/22, *Direktor*.
16. Restrizioni del diritto della protezione dei dati personali del medesimo tenore di quelle introdotte con la direttiva del 2002 sono oggi previste anche all'interno del GDPR, ove – all'art. 23 – si prevede che possa essere circonscritta, mediante apposita misura legislativa, la portata degli obblighi e dei diritti del Regolamento, così come dei principi generali in materia di trattamento dallo stesso individuati “qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare [...] la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica”.

l'art. 132 del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

La norma, pur presente già nel testo originario del Codice del 2003, prende atto delle elaborazioni della giurisprudenza eurounitaria soltanto nel 2021¹⁷, a seguito della pronuncia *Prokuratuur*¹⁸, con un mirato intervento legislativo che ha voluto adeguare – sebbene con qualche ritardo – la disciplina interna sulla *data retention* ai principi formulati dalla Corte di giustizia¹⁹.

Nonostante tale intervento abbia sicuramente il merito di avere attenuato i profili di contrasto con il diritto eurounitario, esso non pare del tutto sciogliere alcune criticità che – per quel che in questa sede più rileva – si riflettono anche sul diritto privato della protezione dei dati personali.

La disciplina interna, nella sua formulazione attuale, chiarisce anzitutto i tempi di conservazione dei dati, distinguendo tra dati di traffico telefonico e dati di traffico telematico. Quale regola generale, così come individuata al comma 1, i primi sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati. I secondi (con la precisazione che non sono, fra questi, inclusi i dati relativi al contenuto delle comunicazioni) sono, per le medesime finalità, conservati dal fornitore per dodici mesi dalla data della comunicazione²⁰. La

norma precisa poi, al comma 1-*bis*, che i dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori, che siano accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.

Tale disciplina deve essere, però, letta unitamente a quella di cui alla l. 20 novembre 2017, n. 167²¹, che, all'art. 24, prevede, per la finalità di “garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di lotta contro il terrorismo”, un termine di conservazione ben più elevato, pari a settantadue mesi, dei dati del traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta. Quale esito del coordinamento di tali due previsioni normative, in ragione della considerazione per cui non è possibile per il fornitore conoscere con anticipo, al momento della conservazione, quale sarà la fattispecie di rilevanza penale in funzione della quale l'autorità domanderà l'accesso, il termine di settantadue mesi assorbe inevitabilmente le limitazioni temporali più brevi individuate nel Codice in materia di protezione dei dati personali, sicché il *provider* non avrà altra scelta se non quella di conservare generalmente e indistintamente tutti i dati per il periodo più lungo individuato dalla legge del 2017²².

Sul tema dell'individuazione dell'autorità a cui compete impartire l'ordine di acquisizione dei dati è direttamente intervenuta la già ricordata riforma del

17. Le modifiche all'art. 132 del Codice in materia di protezione dei dati personali in commento vengono introdotte mediante il d.l. 30 settembre 2021, n. 132, convertito con modificazioni dalla l. 23 novembre 2021, n. 178.

18. Cfr. Corte just. Ue, 2 marzo 2021, C-746/2018, *Prokuratuur*. V. anche il commento di LANDOLFI 2021, p. 1481 ss.

19. Si tratterà, nelle pagine a seguire, dell'art. 132 del Codice in materia di protezione dei dati personali nella sua attuale formulazione. Per un'analisi del testo della norma nella sua versione precedente all'intervento legislativo del 2021, v. FLOR-MARCOLINI 2022, p. 89 ss., che ne osservano le criticità relative principalmente ai tempi di conservazione, alle modalità di acquisizione (e all'intervento del pubblico ministero), e alle finalità di accertamento e repressione dei reati.

20. In considerazione del ruolo preponderante che le nuove tecnologie della comunicazione stanno oggi assumendo, a discapito della comunicazione telefonica tradizionale, difficilmente si comprende la ragione per cui il termine di conservazione dei dati del traffico telematico sia sensibilmente inferiore a quello previsto per i dati del traffico telefonico. Così anche FLOR-MARCOLINI 2022, p. 91.

21. Il comma 5-*bis* dell'art. 132 fa infatti salva l'applicabilità della l. 20 novembre 2017, n. 167 e, in particolare, del suo art. 24.

22. In senso critico rispetto a tale irragionevole, seppure inevitabile, conclusione si esprimono, tra gli altri, DEMARTIS 2022, p. 303 e FLOR-MARCOLINI 2022, p. 46 s. e 89 ss. Anche una verifica *ex post*, al momento dell'accesso, della correttezza del termine di conservazione comporterebbe problemi pratici non indifferenti, per esempio, nell'ipotesi in cui la trasmissione e l'acquisizione abbiano luogo nonostante sia ormai trascorso il tempo di conservazione previsto per il reato perseguito e siano, di conseguenza, da ritenersi illegittime. Di riflesso, nella prospettiva privatistica, i trattamenti sarebbero da considerarsi illeciti poiché posti in essere in

2021²³. Sino al 2021 i dati venivano acquisiti presso il fornitore con decreto motivato del pubblico ministero, eventualmente anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa o delle altre parti private. Nella versione attuale della norma si prevede, invece, che i dati siano acquisiti soltanto previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa o delle altre parti

private, così garantendo l'imparzialità di colui che impartisce l'ordine rispetto alle finalità d'indagine²⁴. La violazione di tali modalità di acquisizione, peraltro, è direttamente sanzionata dalla norma, che sancisce l'inutilizzabilità dei dati raccolti in assenza di autorizzazione (art. 132, comma 3-*quater*).

Anche i presupposti per l'acquisizione sono mutati a seguito dell'intervento legislativo del 2021, che, nello specifico, ha meglio precisato le categorie di reati con riferimento alle quali è possibile, per l'autorità competente, avere accesso ai

violazione di quella norma di legge nazionale (l'art. 132) che individua e definisce l'interesse pubblico da addurre come base giuridica ai sensi dell'art. 6, par. 1, lett. e), del GDPR.

23. In argomento i giudici di Lussemburgo sono intervenuti a più riprese. Segnatamente, Corte giust. Ue, 8 aprile 2014 cause riunite C-293/12 e C-594/12, *Digital Rights* ha sin da subito chiarito che le categorie di soggetti abilitati all'accesso devono essere precisamente individuate e che l'acquisizione deve, in ogni caso, essere subordinata all'autorizzazione di un giudice o di una autorità amministrativa che possa qualificarsi come indipendente. Così anche Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*. In seguito, anche Corte giust. Ue, 2 marzo 2021, causa C-746/18, *Prokuratuur* specifica ulteriormente il ruolo del pubblico ministero nell'accesso ai dati conservati. Sebbene, infatti, la richiesta di accesso ragionevolmente provenga da costui, che – come noto – rappresenta l'autorità titolare dei poteri investigativi e ha il ruolo di coordinare le indagini, essa dovrà essere vagliata da una autorità (giudiziaria o amministrativa) in una posizione di terzietà, che non abbia, in altri termini, un interesse diretto alla conoscenza dei dati. Il pubblico ministero, infatti, in ragione del ruolo processuale di cui è investito e della sua qualità di titolare di obblighi investigativi, non riveste una posizione di imparzialità e, per tale ragione, la sua domanda di accesso dovrà essere esaminata da un organo che sia terzo ed estraneo alla dinamica processuale. Anche secondo Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature* il trattamento deve sempre avere luogo sotto il controllo di un giudice o di una autorità amministrativa indipendente che possa verificare il rispetto delle condizioni legittimanti una estesa conservazione delle informazioni. Da ultimo, anche la più recente Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner* ribadisce che l'organo di polizia, seppure centralizzato e di comando, dal quale proviene la richiesta di accesso ai dati, non ha, per sua natura, i requisiti di terzietà e indipendenza che l'autorità di controllo dovrebbe invece possedere.
24. Tuttavia, in via eccezionale, quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, ovvero alle ricerche di un latitante, il pubblico ministero dispone la acquisizione dei dati con decreto motivato. Questo è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato (art. 132, comma 3-*bis*). Da segnalare, a margine della presente riflessione, è anche la recente introduzione del comma 3-*bis*.1, quale norma di coordinamento inserita dal d.lgs. 30 dicembre 2025, n. 215, che attua il Regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali. Tale disciplina si propone l'obiettivo di facilitare e accelerare l'accesso alle prove elettroniche utilizzate per indagare e perseguire i reati, indipendentemente dall'ubicazione dei dati, prevedendo che un'autorità giudiziaria in uno Stato membro dell'Unione possa richiedere allo stabilimento designato di un prestatore di servizi o ai suoi rappresentanti legali nominati in un altro Stato membro di produrre prove elettroniche (quali i dati degli abbonati, gli indirizzi del protocollo internet (IP) necessari a identificare un utente, e-mail, testi e messaggi in-app), ovvero di conservare (per un periodo di 60 giorni, prorogabile di ulteriori 30) i dati specifici in attesa di una futura richiesta di produzione. Allo scadere di tale periodo l'obbligo di conservazione cessa, a meno che l'autorità non abbia emesso un ordine di produzione relativo a quei medesimi dati.

dati conservati. Se, infatti, prima della riforma, i dati potevano essere acquisiti per l'accertamento e la repressione dei reati, senza alcuna precisazione ulteriore circa le categorie di fattispecie penali che, in ragione della loro gravità e del bene giuridico protetto, giustificavano una significativa ingerenza nei diritti fondamentali dell'individuo, dal 2021, i dati possono essere acquisiti, ai sensi del comma 3, soltanto se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 cod. proc. pen.²⁵

È introdotto inoltre un filtro selettivo in grado di limitare ulteriormente l'acquisizione, la quale è oggi subordinata anche alla presenza del c.d. *fumus commissi delicti*, ossia, in altri termini, alla sussistenza di sufficienti indizi di reati (fra quelli che rientrano nelle categorie individuate dalla norma) che possano giustificare l'intrusione nella sfera privata degli individui.

Sulla conformità della normativa italiana ai principi elaborati dalla giurisprudenza eurounitaria in materia di *data retention* riflette una recente pronuncia della Corte di giustizia del 2024, che, per la prima volta, è chiamata ad affrontare una questione di legittimità sollevata con riferimento all'art. 132 nella sua attuale formulazione²⁶.

Confermata quale condizione per l'acquisizione dei dati relativi al traffico telefonico e telematico l'autorizzazione di un giudice o di una autorità amministrativa indipendente²⁷, il ragionamento dei giudici di Lussemburgo si sofferma sulla nozione di "reato grave" adottata dal legislatore nazionale. Questa, che si basa su un limite edittale massimo *ex ante* individuato dalla legge, viene ritenuta legittima perché fondata su di un criterio oggettivo. In altri termini, una soglia fissata con riferimento alla pena della reclusione non inferiore nel massimo a tre anni non appare – nella prospettiva della Corte – eccessivamente bassa rispetto alla finalità di evitare che l'accesso ai dati da parte delle autorità diventi la regola e trascenda, dunque, l'ambito delle eccezioni²⁸. Peraltro, gli stessi giudici promuovono la verifica di requisiti aggiuntivi che, unitamente ai parametri di selezione già evocati dalla norma, dovrebbero essere in grado di invertere l'idea di proporzionalità. Precisamente, occorre appurare la sussistenza di indizi di reati che rientrano nella individuata nozione di "reato grave" (come previsto dallo stesso art. 132, al comma 3); la rilevanza dei dati richiesti per l'accertamento dei fatti, mediante un c.d. test di necessità; e la possibilità per l'autorità di negare l'accesso, se richiesto nel contesto di un'indagine per reati manifestamente non gravi²⁹.

25. Ovvero se sussistono sufficienti indizi di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti.

26. Si tratta di Corte giust. Ue, 30 aprile 2024, causa C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano*.

27. Motivo principale, questo, per cui il legislatore italiano – come anticipato – era già intervenuto del 2021, individuando nell'autorizzazione giudice, e non più nel decreto pubblico ministero, il provvedimento che legittima l'accesso ai dati.

28. Però, non a torto si è osservato che, facendo corrispondere all'idea di "reato grave" tutte le fattispecie penali i cui limiti edittali rientrano nei limiti della previsione introdotta dal legislatore del 2021, quelle che, per contro, ne rimangono escluse sono di minima rilevanza, ciò che non consentirebbe, a ben vedere, di circoscrivere nemmeno l'acquisizione entro i confini della proporzionalità, come da tempo auspica la Corte Ue (v. soprattutto Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner*). In senso critico rispetto a tale scelta legislativa v. FLOR-MARCOLINI 2022, p. 54 s., ad avviso dei quali la previsione in commento "non può minimamente soddisfare", poiché essa "dà l'illusione di aver effettuato una delimitazione del perimetro delle violazioni, ma in realtà non lascia fuori che le contravvenzioni e pochi delitti di davvero infima gravità". Nemmeno è da trascurare che il concetto stesso di "reato grave", non trovando una sua precisa enunciazione nell'ambito del diritto eurounitario, è destinato a mutare in ragione delle diverse considerazioni e valutazioni di ciascuno Stato membro, con l'esito che le fattispecie penali per la repressione delle quali è consentito conservare e acquisire informazioni di natura personale saranno sicuramente differenti nei singoli ordinamenti nazionali. Ne deriva il concreto rischio di lasciare spazio ad applicazioni elusive dell'art. 15 della Direttiva *e-privacy* e così, di riflesso, si profilano margini per una inaspettata e indebita ingerenza nei diritti fondamentali degli individui.

29. L'autorità indipendente deve, infatti, avere sempre la possibilità di intervenire al fine di riequilibrare, se vi è necessità, il bilanciamento tra le esigenze di natura investigativa, da un lato, e i diritti fondamentali alla riservatezza e alla protezione dei dati personali, dall'altro.

Ad una conservazione generalizzata e indifferenziata (e protratta per un periodo di tempo molto esteso) segue, dunque, un (eventuale) accesso solo a condizione che questo superi un vaglio di necessità che ha riguardo alla stretta rilevanza di quei dati per esigenze di lotta alla criminalità grave e alla proporzionalità dell'acquisizione stessa agli interessi pubblici nel concreto perseguiti.

L'art. 132 sembra allora collocare il momento selettivo dei dati nella sola fase della "consegna" di questi all'autorità, dando per implicita una preliminare conservazione generalizzata³⁰. La novella del 2021 non ha, infatti, introdotto alcun profilo di novità con riferimento alle categorie di dati conservati e rimane ferma su di un modello di conservazione generalizzato ed indifferenziato, che non pone alcuna limitazione in ordine alle categorie di dati che devono essere trattenuti dal fornitore. Ne consegue un incremento esponenziale del rischio di lesione del diritto alla riservatezza e alla protezione dei dati personali, anziché una sua contemporaneizzazione; e ciò a dispetto delle indicazioni della giurisprudenza eurolunitaria che, all'opposto, promuovono – come detto – criteri idonei a limitare anche la conservazione (e non solo l'accesso, peraltro successivo e solo eventuale) alle sole informazioni strettamente necessarie per far fronte ad esigenze di pubblica sicurezza, sul modello della conservazione selezionata³¹.

4. Il ruolo del diritto della protezione dei dati personali nella conservazione e acquisizione di informazioni per finalità di contrasto alla criminalità: profili di criticità

I profili segnalati, a ben vedere, denunciano ancora un qualche margine di incompatibilità della disciplina interna sulla *data retention* non solo con lo statuto elaborato in materia dalla Corte di giustizia,

ma anche con il diritto della protezione dei dati personali, come ora si tenterà di chiarire³².

Il parametro normativo a cui riferirsi per valutare tale (in)compatibilità è rappresentato dalla direttiva (UE) 2016/680 (nota anche come *Law Enforcement Directive* o, più brevemente, direttiva LED, attuata nel nostro ordinamento con il d.lgs. 18 maggio 2018, n. 51), ma anche – e forse soprattutto – dal Regolamento (UE) 2016/679, più comunemente noto come GDPR (o RGPD, nella versione italiana).

Come già si è avuto modo di ricordare, sono due i trattamenti in cui le misure di *data retention* si sostanziano: il primo, rappresentato dalla conservazione, per determinati periodi di tempo (anche prolungati), dei dati (anche) personali da parte del fornitore dei servizi di comunicazione elettronica; il secondo, temporalmente e logicamente successivo al primo, che ha luogo con l'acquisizione da parte dell'autorità giudiziaria dei dati necessari al perseguimento delle finalità di pubblica sicurezza da questa addotte a fondamento della propria richiesta. Ora, mentre del secondo trattamento è indubbiamente titolare l'autorità competente, che provvederà alla individuazione di determinate finalità per le quali i dati devono essere acquisiti, specificando le più generali esigenze di prevenzione, indagine, accertamento e repressione di reati dei quali già sussistano sufficienti indizi, la conservazione delle informazioni compete, invece, ad un soggetto privato, il *provider* del servizio di comunicazione elettronica. Questi, invero, non determina autonomamente le finalità e i mezzi di tale trattamento; esse, piuttosto, sono *ab origine* individuate dal diritto eurolunitario (art. 15, direttiva *e-privacy*) e dal diritto nazionale (art. 132 Codice in materia di protezione dei dati personali), che del primo costituisce attuazione. Non è però di ostacolo alla qualificazione di un soggetto come titolare del trattamento il fatto che questi lo ponga in essere per finalità e mezzi che sono individuati

30. Alla medesima conclusione giungono anche FLOR-MARCOLINI 2022, p. 109.

31. Cfr., in particolare, le già citate Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*, e Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner*, ove vengono suggerite e ampiamente descritte misure di c.d. *targeted retention*.

32. Per un'analisi delle residue criticità in ambito penale e processuale penale v. diffusamente FLOR-MARCOLINI 2022, p. 107 ss. e DEMARTIS 2022, p. 306 s., che in particolare si sofferma sull'assenza di una disciplina dedicata ai dati di ubicazione, che possono entrare nella disponibilità del *provider* anche in assenza di traffico telefonico e telematico.

direttamente dalla legge, ai sensi dell'art. 4, n. 7), secondo periodo, GDPR³³.

Di conseguenza, soltanto con riferimento al secondo trattamento (acquisizione dei dati oggetto di previa conservazione) dovrebbe trovare applicazione la direttiva LED, il cui ambito di operatività è limitato ai trattamenti di dati personali posti in essere dalle "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"³⁴. Di contro, il trattamento che consiste nella conservazione sembra rientrare nella sfera applicativa del GDPR e delle tutele – più elevate rispetto a quelle della direttiva LED – che esso individua a protezione dei soggetti interessati e delle informazioni personali che li identificano o li rendono identificabili³⁵.

Occorre, dunque, osservare criticamente la fase della conservazione dei dati nel prisma dei principi che ne governano il trattamento secondo le previsioni del GDPR e non alla luce della, sia pure simile, disciplina della direttiva LED.

L'immediato esito di tale riflessione è rappresentato dalla considerazione per cui la soluzione del legislatore italiano, che sposta dalla conservazione all'accesso il momento di selezione dei dati, rischia di entrare in aperto conflitto anzitutto con il principio di minimizzazione, che va interpretato

nel senso più rigoroso di cui al GDPR³⁶. Se infatti il trattamento che consiste nella acquisizione dei dati deve rientrare entro il già ricordato parametro dalla nozione di "reato grave" e il filtro selettivo è rappresentato dalla sussistenza di indizi di tali reati, la conservazione avviene invece – come detto – in modo generalizzato, senza che abbia spazio alcun tipo di vaglio preliminare che consenta di parametrare alle finalità del trattamento i dati raccolti. La minimizzazione non pare certamente in linea con una raccolta generalizzata e indifferenziata di informazioni relative al traffico delle comunicazioni telefoniche e telematiche, senza che – come a più riprese suggerito dalla stessa Corte di giustizia – vengano adottati criteri idonei a circoscrivere – nello spazio, nel tempo, o in base ad altre valutazioni – le categorie di dati che devono essere sottratte alla regola generale della cancellazione o anonimizzazione, per fare fronte a finalità ulteriori di sicurezza pubblica. La mancata implementazione di misure di conservazione targhettizzata, in altre parole, non soltanto è pratica in contrasto con il principio eurounitario della proporzionalità, ma nemmeno sembra essere fedele all'esigenza di custodire, in vista di una eventuale acquisizione, solo i dati che siano adeguati, pertinenti e limitati a quanto necessario per le finalità (speciali) per le quali possono essere oggetto di ulteriore trattamento³⁷.

33. Sul punto riflette anche la stessa Corte di giustizia, secondo cui per attribuire la qualità di titolare del trattamento ad una entità, ai sensi dell'articolo 4, n. 7, secondo periodo, del GDPR non è necessario che tale entità eserciti un'influenza sulla determinazione delle finalità e dei mezzi di tale trattamento, previste, invece, dallo stesso diritto nazionale. Cfr. Corte giust. Ue, 27 febbraio 2025, causa C-638/23, *Amt der Tiroler Landesregierung*.

34. Cfr. art. 1, par. 1, della direttiva.

35. A meno che non si voglia considerare l'idea che le peculiari finalità che con la conservazione ci si propone di perseguire non siano idonee ad attrarre nella sfera di applicabilità della direttiva LED anche il primo trattamento.

36. Il principio è enunciato dal GDPR, all'art. 5, par. 1, lett. c), ma è presente anche nella direttiva (UE) 2016/680, nel suo art. 4, par. 1, lett. c), nell'ambito della quale esso deve essere valutato in misura attenuata in ragione delle finalità dei trattamenti che rientrano nel suo ambito d'applicazione. In generale, sul principio di minimizzazione, v. almeno BATTISTINI-MATARAZZO-ZANETTI 2023, p. 231 ss.; ROßNAGEL-RICHTER 2023, p. 279 ss.; DELL'UTRI 2019, p. 179 ss. e 209 ss.; COLAPIETRO-IANNUZZI 2017, p. 106 ss.

37. Il principio di minimizzazione è da mettere in connessione con il principio di proporzionalità, di cui è espressione l'art. 52 della Carta dei diritti fondamentali dell'Unione europea. Mentre la proporzionalità, nel contesto della protezione dei dati personali, persegue l'obiettivo primario di contenere entro limiti minimi le lesioni di tale diritto fondamentale, compresso per lasciare più ampia operatività ad un diritto di pari rango, e perciò opera *ex ante* sul piano della selezione della finalità che mediante il trattamento possono soddisfare tale diritto, la minimizzazione, di contro, viene in rilievo in un momento logicamente e temporalmente successivo,

Ulteriori profili di contrasto emergono anche con il principio di integrità e riservatezza del trattamento³⁸: in un simile assetto il potenziale rischio per gli utenti è, infatti, incrementato dalla mancata individuazione, all'interno del testo normativo, di precise misure volte all'adozione di standard elevati di protezione³⁹.

Il concetto di rischio evoca, dunque, un ulteriore rilevante profilo problematico della disciplina italiana sulla *data retention*; profilo, questo, che, peraltro, rappresenta – come si vedrà – uno dei punti di contatto più evidenti tra la riflessione di diritto penale sostanziale e processuale e l'ambito privatistico della protezione dei dati personali.

Il generico richiamo, con l'art. 132-ter, all'art. 32 del GDPR, ha sicuramente inteso estendere, anche a tale ambito, le previsioni in materia di sicurezza del Regolamento, ma, nel farlo, il legislatore ha omissso di identificare misure di protezione (anche minime) da cui non poter prescindere, che sarebbero state certamente utili all'operatore privato per far fronte ad un rischio certamente elevato sia in ragione della indiscriminata raccolta di informazioni e della loro conservazione per un periodo di tempo molto esteso sia in considerazione delle conseguenze negative di cui pure le esigenze di lotta alla criminalità risentirebbero in ipotesi di violazione dei dati.

Posto che, in ogni caso, al trattamento che consiste nella conservazione dei dati da parte del *provider* pare debba applicarsi il GDPR (e non la direttiva LED), il mancato riferimento a specifici profili di

sicurezza non potrebbe trovare giustificazione nel diverso rapporto tra il diritto alla protezione dei dati personali dei soggetti interessati e le finalità di pubblica sicurezza perseguite con il trattamento che costituiscono l'ambito di operatività della direttiva del 2016. Sebbene, infatti, dette finalità rendano leciti periodi di conservazione prolungati ed ammettano la raccolta di elevate quantità di informazioni, con la conseguenza che i diritti dei soggetti interessati possono risultare compressi, l'ambito della sicurezza – così come previsto nella direttiva – non pare subire alcuna restrizione rispetto a quanto previsto dalla disciplina generale in materia di protezione dei dati personali⁴⁰. Al contrario, in ragione di un livello di rischio che è, per natura, elevato, il principio di integrità e riservatezza dei dati personali dovrebbe trovare, nell'ambito che ci occupa, un primario campo di applicazione.

Risulta così essenziale l'individuazione di precise ed efficaci misure di sicurezza, che, nella loro applicazione concreta, sono da considerarsi direttamente funzionali ad invertere – sia nella fase di conservazione sia in quella di accesso ai dati del traffico telefonico e telematico – anche il principio di proporzionalità, nel suo senso di minor ingerenza possibile – mediante l'adozione di adeguate garanzie – nella situazione giuridica compressa in favore di quella che, all'esito di un bilanciamento, è da tutelare in via preminente.

Di tale individuazione viene investito il singolo *provider*, a cui competerà la scelta e l'attuazione

per circoscrivere il trattamento ai soli dati adeguati, pertinenti e limitati alle finalità che già sono state oggetto di bilanciamento (v. sul punto ROßNAGEL–RICHTER 2023, p. 281). Un trattamento che ignori le esigenze di minimizzazione risulterà, perciò, in conflitto anche con il principio di proporzionalità.

38. Cfr. art. 5, par. 1, lett. f), GDPR (richiamato anche dall'art. 4, par. 1, lett. f) della direttiva LED).

39. Già a partire da Corte giust. Ue, 8 aprile 2014 cause riunite C-293/12 e C-594/12, *Digital Rights*, la Corte europea ha affermato la necessità di adottare specifiche regole volte a garantire la sicurezza e la protezione dei dati raccolti. Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*, ha in seguito ribadito che la sicurezza dei dati conservati deve essere implementata mediante l'introduzione dell'obbligo per i *provider* di adottare, durante il periodo di conservazione, degli standard di protezione elevati e, al contempo, con l'imposizione, allo scadere del periodo di tempo di riferimento, della cancellazione irreversibile delle informazioni. Ha precisato, infine, Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*, che la compressione dei diritti dell'individuo a fronte di interessi generali di contrasto alla criminalità grave deve essere accompagnata da garanzie procedurali idonee a mitigare la lesione dei diritti fondamentali degli utenti.

40. Cfr., in particolare, l'art. 29 della direttiva, di cui l'art. 16 del d.lgs. 18 maggio 2018, n. 51 rappresenta attuazione, ove è previsto – sulla scorta del modello del GDPR – che il titolare del trattamento (e il responsabile del trattamento), “tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio”.

degli strumenti più idonei a contenere i rischi che incombono sui diritti e le libertà fondamentali dei soggetti interessati, avvalendosi degli strumenti che il GDPR stesso mette a disposizione.

Al pari di qualsiasi titolare del trattamento, anche il fornitore di servizi di comunicazione elettronica che sia tenuto, ai sensi dell'art. 132, ad ultra-conservare le informazioni del traffico telefonico e telematico per l'ipotesi in cui queste si rivelino necessarie alle autorità di pubblica sicurezza è da considerarsi obbligato a procedere – secondo il modello dell'*accountability*⁴¹ – a valutare i rischi del trattamento che pone in essere e ad implementare, di conseguenza, le misure tecniche e organizzative “per garantire un livello di sicurezza adeguato al rischio”⁴². Nonostante, infatti, le regole generali e i principi che concorrono a definire l'*accountability* trovino espressa enunciazione in alcune norme del GDPR, quali gli artt. 5, par. 2, 24 e 32, le “misure tecniche e organizzative” non possono prescindere da un intervento diretto del titolare, che dovrà riempirle di contenuto all'esito di una attività di analisi e di gestione del rischio declinata nella prospettiva del singolo trattamento, anche di quello che risponde a finalità di sicurezza pubblica⁴³.

Fra le misure tecniche ed organizzative che il titolare del trattamento può mettere in atto pare assumere particolare rilievo quella della pseudonimizzazione⁴⁴. Il trattamento di dati personali con modalità che non consentano il loro collegamento

ad una determinata persona fisica senza l'impiego di informazioni aggiuntive, conservate separatamente, identifica senz'altro una delle misure tecniche e organizzative intese a garantire che la conservazione dei dati avvenga nel rispetto di standard adeguati di protezione.

L'indiscutibile vantaggio di una simile misura consiste sicuramente nella sua reversibilità. Il collegamento tra l'informazione e la persona fisica viene meno, mediante la rimozione di qualsiasi riferimento diretto del dato al soggetto interessato, ma al contempo rimane possibile – allorquando si riveli necessaria – la possibilità di una sua re-identificazione, per il tramite di una “chiave” in grado di ricollegare il dato alla persona fisica.

Ciò si rivela, allora, nella prospettiva delle investigazioni digitali, di essenziale importanza, e al contempo pare soddisfare – anche nel contesto di questa indagine – il principio di limitazione della conservazione⁴⁵, per effetto del quale la restrizione temporale del trattamento non interviene sul periodo di conservazione delle informazioni in sé; piuttosto, ciò che il legislatore eurounitario ha inteso circoscrivere entro limiti temporali precisi è la relazione tra i dati e la persona fisica a cui essi sono riferiti e che ne consentono l'identificazione o l'identificabilità.

Ruolo di non secondaria importanza è anche quello svolto da altri strumenti di *accountability*, quali quelli che rispondono ai concetti di *data protection* (o *privacy*) *by design* e *by*

41. Il principio di *accountability* promuove un vero e proprio modello nella adozione di standard di sicurezza. Questo, semplicisticamente tradotto nella versione italiana del Regolamento con il termine “responsabilizzazione”, identifica invero un più ampio concetto che evoca anche la responsabilità del titolare del trattamento di assicurare la conformità di questo al GDPR, ciò che si traduce in una sua responsabilizzazione circa l'adozione di adeguati strumenti che la possano realizzare, e a cui si aggiunge, da ultimo, anche la disponibilità della prova di tale conformità. Sul principio di *accountability* v. almeno GATTI 2025, p. 876 ss.; ALBANESE-CARDINALI 2023, p. 501 ss.; CARLEO 2021, p. 359 ss.; AMORE 2020, p. 414 ss.; FINOCCHIARO 2019, p. 2778 ss. e LUCCHINI GUASTALLA 2018, p. 106 ss.

42. Cfr. art. 32 GDPR.

43. Tale intervento diretto del titolare del trattamento, peraltro, non si esaurisce con l'adozione, ma trova estensione anche ai successivi interventi del riesame e dell'aggiornamento, ove necessario, delle misure introdotte. Cfr., per esempio, GATTI 2025, p. 881 ss.

44. Cfr. art. 4, par. 1, n. 7, GDPR. In commento v., tra gli altri, ALMADA-MARANHAO-SARTOR 2023, p. 162 ss. Sul punto v. anche il considerando n. 28 del GDPR, ove si chiarisce che “l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati”.

45. Cfr. art. 5, par. 1, lett. e), GDPR. Sul principio di limitazione della conservazione v., per esempio, ROßNAGEL-RIECHTER 2023, p. 285 ss.

*default*⁴⁶. In assenza di un criterio temporale che sia a sufficienza ristretto da poter garantire buoni livelli di sicurezza, le modalità di progettazione dei mezzi impiegati nella conservazione e le impostazioni predefinite degli stessi potrebbero, nel concreto, consentire di applicare quelle misure di conservazione targhettizzata che impiegano criteri geografici, ovvero quelli basati sulle persone in qualche misura vicine ad ambienti criminosi, per filtrare i soli dati che potranno potenzialmente risultare rilevanti per le finalità di prevenzione, indagine, accertamento e perseguimento di reati, con l'esito di far così rientrare il trattamento in questione entro i confini della conformità al principio di minimizzazione⁴⁷, e di proporzionalità⁴⁸.

Criticità decisamente minori sembra, da ultimo, sollevare il trattamento condotto dall'autorità giudiziaria che consiste nella acquisizione dei dati rilevanti per le finalità che le sono proprie, il quale è da far rientrare – come anticipato – nell'ambito di applicazione della direttiva LED. L'accesso, che è ammesso se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, è limitato a tali ipotesi specifiche (individuate dallo stesso legislatore) e, sebbene tale limitazione non sia così rigorosa, escludendo – di fatto – tali categorie i soli reati di lieve entità, essa potrebbe in una qualche misura trovare giustificazione – quantomeno dal punto di vista della protezione dei dati personali – nelle lievemente meno stringenti previsioni di tutela della direttiva in tale ambito, che legittimamente comprime la protezione delle informazioni dei soggetti interessati, e i loro diritti, in favore di esigenze di natura pubblicistica, come ammesso anche dallo stesso GDPR, all'art. 23.

Qualche dubbio invece residua sulla compatibilità di tale secondo trattamento con il principio della proporzionalità, poiché troppo ampio pare essere lo spazio operativo (lasciato aperto dalla ampia nozione di "reato grave") delle esigenze di pubblica

sicurezza, a discapito di una eccessiva compressione della riservatezza degli utenti. Anche qui, però, vale la pena considerare l'idea che la proporzionalità possa essere ripristinata per il tramite dell'adozione dei già richiamati strumenti di *accountability* che, *ex ante*, innalzano il livello di sicurezza dei dati personali sin dalla fase della loro conservazione.

5. Qualche osservazione conclusiva

Emerge, in definitiva, con la massima evidenza come nel settore delle investigazioni digitali – per quanto qui più rileva, nell'applicazione di misure di *data retention* – la dimensione pubblicistica, che, come detto, prende forma nell'acquisizione di dati che risultano rilevanti ai fini di prevenzione, indagine, accertamento e repressione di reati, abbisogni della cooperazione di soggetti privati, i fornitori di servizi di comunicazione elettronica (titolari del trattamento) che, pur agendo in applicazione di regole di natura privatistica, conservino tali dati e, al contempo, assicurino che l'accesso abbia luogo entro limiti adeguati di sicurezza e integrità delle informazioni.

Tali soggetti – anche in questo specifico ambito – risultano oltremodo "responsabilizzati", perché la mancata, scorretta o inidonea implementazione di misure di sicurezza volte a contenere il rischio specifico li espone ad interventi correttivi da parte dell'Autorità garante o, eventualmente, all'applicazione di sanzioni amministrative. Ma non solo. Per il caso di violazione del Regolamento viene in rilievo, sul piano del *private enforcement*, anche il profilo risarcitorio. Se, infatti, il *provider*, titolare del trattamento, soggetto a precisi ed eccezionali obblighi di ultra-conservazione delle informazioni motivati da interessi di natura pubblicistica, abbia mancato di adottare misure tecniche ed organizzative, o se queste, ancor più essenziali nella situazione in cui il diritto alla protezione dei dati personali regredisce per lasciare spazio ad altre e parimenti rilevanti esigenze di lotta alla criminalità, dovessero, sulla base di una valutazione del caso concreto, rivelarsi

46. Essenziale rimane altresì, ai fini della determinazione – a monte – del livello di rischio, la valutazione di impatto del trattamento previsto sulla protezione dei dati personali.

47. Indubbio è infatti il rapporto di strumentalità delle misure intese ad inverare i concetti di *data protection by design* e *data protection by default* rispetto al principio di minimizzazione. Sul punto v., per esempio, VOIGT-VON DEM BUSSCHE 2024, p. 63 ss. e 138 s.

48. Perché, come osservato dalla stessa Corte di giustizia, misure di tale sorta sarebbero ideonee a garantire un più equo bilanciamento dei diritti e interessi in conflitto.

inadeguate, sarà ritenuto responsabile del danno in ipotesi subito dai soggetti interessati coinvolti⁴⁹.

Peraltro, non si può non notare come, così configurati, gli operatori privati vengano a rivestire un ruolo non secondario anche quali fattori correttivi di una disciplina che, specialmente nella determinazione dei periodi di conservazione dei dati del traffico telefonico e telematico, non sembra porsi perfettamente in linea né con il diritto della protezione dei dati personali né con il principio eurounitario della proporzionalità. È solo grazie alle misure di *accountability* introdotte dal *provider* e agli strumenti di sicurezza che questi attua in applicazione di tale modello che la conservazione generalizzata e indifferenziata può essere in una qualche misura temperata, riportando così il trattamento entro i confini di liceità e parimenti scongiurando una – ancorché parziale – disapplicazione dell'art. 132 del Codice in materia di protezione dei dati personali per il suo contrasto con il diritto eurounitario.

Al fine di non aggravare – anche in termini di costi – la posizione già di per sé onerosa, in termini di “responsabilizzazione” del titolare del trattamento, sarebbe, allora, auspicabile un intervento organico e aggiornato da parte del legislatore eurounitario⁵⁰. Gli strumenti normativi del diritto dell'Unione, specie se adottati nella forma del regolamento, si rivelano infatti maggiormente idonei a raccogliere le elaborazioni della Corte di giustizia in un unico *corpus* normativo, a cui gli Stati membri siano chiamati ad adeguarsi senza apprezzabili margini di discrezionalità, nella consapevolezza che solo una disciplina uniforme, direttamente applicabile nei diversi contesti nazionali, può realizzare il necessario contemperamento, conforme agli standard (anche di sicurezza) europei, tra le esigenze pubblicistiche, da un lato, e la tutela dei diritti alla riservatezza e alla protezione dei dati personali dei singoli individui, dall'altro⁵¹.

Riferimenti bibliografici

- F. ALBANESE, I. CARDINALI (2023), *Il principio di responsabilizzazione (accountability)*, in F. Bravo (a cura di), “Dati personali. Protezione, libera circolazione e governance, 1. Principi”, Pacini Giuridica, 2023
- M. ALMADA, J. MARANHÃO, G. SARTOR (2023), *sub Art. 4(5)*, in I. Spiecker gen. Döhmman, V. Papakonstantinou, G. Hornung, P. De Hert (Eds.), “General Data Protection Regulation. Article-by-Article Commentary”, Beck-Hart-Nomos, 2023
- G. AMORE (2020), *Fairness, Transparency e Accountability nella protezione dei dati personali*, in “*Studium iuris*”, 2020, n. 4
- S.G. BATTISTINI, L. MATARAZZO, L. ZANETTI (2023), *Il principio di minimizzazione dei dati*, in F. Bravo (a cura di), “Dati personali. Protezione, libera circolazione e governance, 1. Principi”, Pacini Giuridica, 2023

49. Cfr. art. 82 GDPR. Così ragionando, peraltro, viene messa in luce la stretta connessione tra *accountability* e responsabilità, tale per cui le misure di sicurezza discrezionalmente adottate dal titolare del trattamento diventano parametro di valutazione del rispetto della normativa. Sul punto v. almeno GATTI 2025, p. 893 ss. L'art. 82, letto in connessione all'approccio dell'*accountability*, pare allora avvalorare la conclusione della Corte di giustizia, che qualifica la responsabilità del Regolamento come una responsabilità per colpa, con inversione dell'onere della prova (cfr. Corte giust. Ue, 21 dicembre 2023, C-667/21).

50. In senso conforme v. FLOR-MARCOLINI 2022, p. 119, i quali suggeriscono un intervento legislativo, a livello eurounitario e/o nazionale, che individui i termini della cooperazione (o *co-regulation*) tra settore pubblico e privato nella prevenzione, nell'indagine, nell'accertamento e nel perseguimento dei reati.

51. Se poi si considera che l'obbligo di conservazione dei dati relativi alle comunicazioni elettroniche, da cui discende la possibilità per le autorità di contrasto di avere a questi accesso, è strumento di essenziale importanza per l'accertamento e la repressione delle più diverse forme di criminalità, anche e soprattutto quando la loro esecuzione si estende oltre i confini nazionali, ancor meglio si comprende l'esigenza che la disciplina di riferimento sia inquadrata nel contesto normativo eurounitario, così da garantire un più elevato livello di cooperazione – anche giudiziaria – in materia penale.

- R. CARLEO (2021), *Il principio di accountability nel GDPR. Dalla regola alla auto-regolazione*, in “Nuovo diritto civile”, 2021, n. 1
- C.M. CASCIONE (2014), *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della Corte di giustizia e gli echi del datagate*, in “Nuova giurisprudenza civile commentata”, 2014, n. 11
- C. COLAPIETRO, A. IANNUZZI (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro (a cura di), “Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679”, Editoriale Scientifica, 2017
- M. DELL'UTRI (2019), *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cufaro, R. D'Orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, Giappichelli, 2019
- F. DEMARTIS (2022), *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in “Diritto penale e processo”, 2022, n. 3
- G. FINOCCHIARO (2019), *Il principio di accountability*, in “Giurisprudenza italiana”, 2019, n. 12
- R. FLOR, B. PANATTONI (2023), *Digital criminal investigation in Italy. The intersection between data protection and cybersecurity*, in “New Journal of European Criminal Law”, vol. 14, 2023, n. 4
- R. FLOR, S. MARCOLINI (2022), *Dalla data retention alle indagini ad alto contenuto tecnologico*, Giappichelli, 2022
- R. FLOR (2015), *Dalla 'Data retention' al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de iure condendo'*, in G. Resta, V. Zeno-Zencovich (a cura di), “Il diritto all'oblio su internet dopo la sentenza Google Spain”, Roma TrE-Press, 2015
- R. FLOR (2014), *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. “data retention” contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in “Diritto penale contemporaneo”, 2014, n. 2
- S. GATTI (2025), *Il principio di accountability e la sua attuazione nel regolamento generale sulla protezione dei dati*, in R. Bocchini (a cura di), “Trattato Le piattaforme digitali. e-Agorà”, Giappichelli, 2025
- E. GRILLO (2024), *Sulla conservazione sistematica e generalizzata di dati genetici e biometrici per finalità di polizia*, in “Nuova giurisprudenza civile commentata”, 2024, n. 4
- M. LANDOLFI (2021), *La Corte di Giustizia UE interviene ancora sulla conservazione e sull'accesso ai dati di traffico e di ubicazione: alcune riflessioni sulla disciplina interna*, in “Studium iuris”, 2021, n. 12
- E. LUCCHINI GUASTALLA (2018), *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in “Contratto e impresa”, 2018, n. 1
- A. ROßNAGEL, P. RICHTER (2023), *sub Art. 5*, in I. Spiecker gen. Döhmman, V. Papakonstantinou, G. Hornung, P. De Hert (Eds.), “General Data Protection Regulation. Article-by-Article Commentary”, Beck-Hart-Nomos, 2023
- L. TRUCCO (2014), *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in “Giurisprudenza italiana”, 2014, n. 8-9
- P. VOIGT, A. VON DEM BUSSCHE (2024), *The EU General Data Protection Regulation (GDPR). A practical Guide*, 2nd ed., Springer, 2024



DENISE BORIERO

Il sequestro di dispositivi e informazioni digitali

Il contributo analizza il sequestro di dispositivi e informazioni digitali nel processo penale, evidenziando le tensioni tra esigenze investigative e tutela dei diritti fondamentali. La crescente centralità degli strumenti informatici ha reso smartphone, computer e account digitali depositi di una vasta quantità di dati personali e comunicativi, mettendo in crisi le tradizionali categorie del sequestro, poiché l'oggetto dell'acquisizione è sempre più il contenuto informativo anziché il supporto materiale. L'elaborato approfondisce le caratteristiche del dato digitale e le modalità di acquisizione della prova informatica, con particolare attenzione alle garanzie di autenticità, integrità e tracciabilità del dato. Vengono inoltre esaminati il quadro normativo nazionale, europeo e sovranazionale nonché il ruolo della giurisprudenza nell'affermazione dei principi di proporzionalità, pertinenza e minimizzazione delle acquisizioni digitali, in una prospettiva di equilibrio tra efficacia investigativa, diritto di difesa e tutela della riservatezza.

Prova digitale – Sequestro informatico – Investigazioni digitali – Digital forensics – Digital due process

The seizure of digital devices and electronic information

This paper examines the seizure of digital devices and digital information in criminal proceedings, highlighting the tensions between investigative needs and the protection of fundamental rights. The growing centrality of digital technologies has transformed smartphones, computers, and online accounts into repositories of vast amounts of personal and communicative data, challenging traditional concepts of seizure, as the true object of acquisition is increasingly the informational content rather than the physical device itself. The study explores the distinctive features of digital data and the methods used to acquire digital evidence, with particular attention to the requirements of authenticity, integrity, and traceability. It also analyzes the national, European, and supranational legal frameworks governing digital investigations, as well as the role of case law in shaping the principles of proportionality, relevance, and data minimization in digital seizures. The analysis ultimately focuses on achieving a balance between investigative effectiveness, the right to defense, and the protection of privacy.

Digital evidence – Digital seizure – Digital investigations – Digital forensics – Digital due process

L'Autrice è Membro del Centro di Scienze della Criminalità e della Sicurezza dell'Università di Trento e di Verona; Dottoranda del Corso di Studi sulla Criminalità Organizzata dell'Università degli Studi di Milano

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli

SOMMARIO: 1. Introduzione. Il sequestro della prova digitale: evoluzione tecnologica e crisi delle categorie tradizionali. – 2. Il dispositivo digitale tra supporto materiale e contenuto informativo. – 3. La nozione di informazione digitale e la complessità del dato informatico. – 4. Il sequestro digitale nel quadro delle investigazioni informatiche. – 4.1. Il sequestro probatorio di dispositivi e informazioni digitali. – 4.2. Sequestro preventivo di dispositivi e informazioni digitali. – 4.3. Sequestro conservativo di dispositivi digitali. – 5. Fasi operative del sequestro informatico e acquisizione dei dati digitali. – 6. Garanzie difensive e diritti fondamentali. – 7. Conclusioni.

1. Introduzione. Il sequestro della prova digitale: evoluzione tecnologica e crisi delle categorie tradizionali

Il sequestro di dispositivi e informazioni digitali costituisce oggi una delle principali aree di frizione tra esigenze investigative e tutela dei diritti fondamentali nel processo penale. La centralità assunta dagli strumenti informatici nella vita personale e professionale dell'individuo ha infatti trasformato smartphone, computer e account digitali in contenitori di una quantità estremamente ampia ed eterogenea di dati, spesso idonei a ricostruire in modo particolarmente penetrante abitudini, relazioni, spostamenti, comunicazioni e attività economiche del soggetto sottoposto a indagine.

In tale contesto, l'applicazione delle tradizionali categorie del sequestro evidenzia significative criticità. Con riferimento al sequestro probatorio, ad esempio, l'apprensione del supporto materiale non coincide più necessariamente con l'acquisizione della prova, mentre la distinzione tra "cosa" e "dato" tende progressivamente a sfumare. Il dispositivo digitale non costituisce, infatti, soltanto un bene materiale suscettibile di vincolo, ma soprattutto un punto di accesso a una pluralità di contenuti informativi autonomamente rilevanti sul piano probatorio.

Tale peculiarità incide direttamente sui presupposti di legittimità e sulle modalità esecutive del vincolo ablatorio. Diversamente dal sequestro tradizionale, l'acquisizione di dispositivi informatici pone problemi di selezione del materiale rilevante, di delimitazione dell'oggetto del vincolo

e, soprattutto, di proporzionalità dell'ingerenza investigativa. La possibilità tecnica di estrarre integralmente il contenuto di un dispositivo comporta il rischio di acquisizioni generalizzate di dati non pertinenti rispetto al fatto oggetto di indagine, con conseguente incidenza sulla riservatezza e sulla segretezza delle comunicazioni.

La giurisprudenza nazionale ed europea più recente ha progressivamente evidenziato la necessità di distinguere tra il sequestro del "contenitore" materiale, del supporto, e l'acquisizione del contenuto informativo, valorizzando i criteri di pertinenza e proporzionalità nella selezione dei dati rilevanti. In particolare, il dibattito si è concentrato sul tema delle acquisizioni massive, delle copie forensi integrali e delle garanzie procedurali necessarie a evitare forme di ricerca meramente esplorativa incompatibili con i principi del giusto processo.

Ulteriori criticità emergono con riferimento ai dati conservati in ambiente remoto e ai servizi cloud, rispetto ai quali la tradizionale dimensione territoriale del sequestro mostra evidenti limiti applicativi. La dissociazione tra disponibilità materiale del dispositivo e localizzazione effettiva del dato impone infatti di confrontarsi con problematiche di giurisdizione, cooperazione internazionale e rapporti con i fornitori di servizi digitali, evidenziando altresì una crescente interazione tra soggetti pubblici e operatori privati nella gestione, conservazione e acquisizione delle informazioni. Ne deriva una progressiva ibridazione delle tradizionali categorie pubblicistiche

dell'attività investigativa, in un quadro normativo ancora frammentario e non pienamente coordinato.

L'analisi del sequestro di dispositivi e informazioni digitali impone dunque di verificare se gli strumenti processuali vigenti siano effettivamente idonei a governare le peculiarità della prova informatica o se, al contrario, l'evoluzione tecnologica richieda una più profonda revisione delle categorie tradizionali dei mezzi di ricerca della prova.

2. Il dispositivo digitale tra supporto materiale e contenuto informativo

Prima di affrontare le problematiche concernenti il sequestro della prova digitale, occorre svolgere una precisazione preliminare rispetto alla nozione di "dispositivo digitale". Sotto il profilo strettamente tecnico, infatti, il concetto non presenta particolari difficoltà definitorie, riferendosi comunemente a qualsiasi apparato elettronico idoneo alla memorizzazione, elaborazione o trasmissione di dati informatici, quali computer, smartphone, tablet, hard disk, server o ulteriori supporti di memoria digitale.

La vera complessità emerge tuttavia sul piano giuridico-processuale e concerne la necessità di distinguere – come anticipato – il dispositivo quale bene materiale dal contenuto informativo in esso conservato o accessibile per il suo tramite. In tale prospettiva, il sequestro del bene assume carattere meramente strumentale rispetto alla reale finalità investigativa, consistente nell'acquisizione del dato digitale. Ne deriva la necessità di delimitare con particolare rigore l'attività investigativa ai soli dati pertinenti all'accertamento del fatto, in applicazione dei principi di pertinenza e proporzionalità, considerata la potenziale estensione illimitata dell'accesso alle informazioni contenute nel dispositivo.

Il rischio è, infatti, quello di determinare una compressione eccessiva dei diritti fondamentali dell'interessato, unitamente a una indebita estensione del potere investigativo.

Proprio in ragione di tali criticità, la giurisprudenza ha progressivamente evidenziato la necessità di evitare forme di sequestro esplorativo prive di adeguata delimitazione dell'oggetto della ricerca, andando a redigere vere e proprie linee guida sulle perquisizioni e sui sequestri digitali¹.

In particolare, si richiede che, a seguito dell'apprensione del dispositivo, venga immediatamente effettuata una copia integrale del contenuto, con successiva restituzione del bene all'avente diritto e analisi dei dati secondo criteri di pertinenza e proporzionalità rispetto al capo d'imputazione.

In tale contesto, la Corte di Cassazione ha talvolta utilizzato la nozione di "copia mezzo", quale strumento funzionale alla separazione tra acquisizione e analisi del dato.

Il provvedimento di sequestro deve inoltre essere sorretto da una motivazione rafforzata, idonea a dar conto sia del nesso di pertinenza tra l'ipotesi di reato e il bene oggetto di vincolo, sia delle specifiche operazioni tecniche da eseguire e della loro durata.

La necessità della duplicazione integrale risponde altresì all'esigenza di preservare l'integrità della prova informatica. Il dato digitale, infatti, presenta caratteristiche ontologicamente differenti rispetto alla prova documentale tradizionale, essendo connotato da volatilità, immaterialità e suscettibilità di alterazione anche in assenza di modificazioni del supporto fisico. Ne deriva l'importanza centrale delle tecniche di copia forense e delle procedure idonee a garantire autenticità, immutabilità e tracciabilità dell'acquisizione.

Ulteriori complessità derivano dalla frequente dissociazione tra disponibilità del dispositivo e localizzazione effettiva del dato, che talvolta rende difficoltosa – se non impossibile – l'individuazione del luogo di conservazione dell'informazione e del soggetto che ne detiene il controllo. Tale fenomeno impone, inoltre, forme sempre più strette di cooperazione tra autorità pubbliche e operatori privati, atteso che le infrastrutture di archiviazione e gestione dei dati sono spesso affidate a provider e servizi cloud.

In definitiva, non soltanto la categoria della prova digitale risulta in tensione con gli schemi tradizionali, in quanto solo parzialmente riconducibile alle categorie probatorie classiche, ma più in generale è l'intero impianto concettuale del diritto penale sostanziale e processuale ad essere sottoposto a una progressiva rielaborazione². Ne risultano investite categorie fondamentali quali la competenza, la territorialità, la nozione stessa

1. Cass., Sez. VI, 22 settembre 2020 (dep. 2 dicembre 2020), n. 34265. Per un commento, si veda PITTIRUTI 2021.

2. Si veda, tra molti, DANIELE 2011.

di fatto penalmente rilevante e le coordinate tradizionali di imputazione e accertamento, le quali mostrano crescenti difficoltà di adattamento rispetto a fenomeni caratterizzati da immaterialità, distribuzione transnazionale dei dati e immediata replicabilità delle informazioni digitali³.

3. La nozione di informazione digitale e la complessità del dato informatico

Un ulteriore profilo preliminare concerne la definizione di “informazione digitale”, categoria che costituisce il reale oggetto delle moderne investigazioni informatiche e che, proprio per la sua ampiezza e mutevolezza, presenta rilevanti difficoltà di sistematizzazione sul piano giuridico.

Per informazione digitale deve intendersi, in senso ampio, qualsiasi contenuto informativo rappresentato in forma binaria e generato, elaborato, trasmesso o conservato mediante sistemi informatici o telematici, indipendentemente dalla sua immediata percepibilità da parte dell'utente e dalla modalità con cui esso viene reso accessibile attraverso dispositivi o interfacce digitali.

In tale prospettiva si colloca la definizione elaborata dalla Convenzione di Budapest del Consiglio d'Europa del 2001 sulla criminalità informatica (c.d. Convenzione sul cybercrime), che, all'art. 1 lett. b) qualifica il dato informatico come “qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione”.

Ne emerge sin da subito come tale categoria sia connotata da una significativa stratificazione interna, che eccede la sola dimensione del contenuto immediatamente fruibile. Accanto alle informazioni immediatamente percepibili – quali testi, immagini, file audio e video o comunicazioni elettroniche – assumono infatti crescente rilievo ulteriori livelli informativi, spesso non visibili all'utente ma dotati di significativa attitudine probatoria.

In primo luogo, si evidenziano i metadati, ossia dati relativi ad altri dati, i quali accompagnano ogni operazione digitale e consentono la ricostruzione di elementi essenziali quali la data di creazione o modifica di un file, il dispositivo utilizzato, le coordinate di geolocalizzazione o le modalità di accesso. In secondo luogo, assumono rilievo i log di accesso, vale a dire le tracce informatiche che registrano le interazioni tra utente e sistema, permettendo di individuare accessi, autenticazioni e attività svolte all'interno di piattaforme digitali.

Ulteriori profili informativi sono rappresentati dalle informazioni di sistema, comprendenti dati relativi al funzionamento del dispositivo, alle reti alle quali esso si è connesso, agli indirizzi IP utilizzati e alle configurazioni hardware e software. Infine, un ruolo sempre più significativo è svolto dai dati di traffico telematico, i quali consentono di ricostruire flussi comunicativi, tempi, destinatari e modalità delle interazioni digitali.

Tali informazioni sono suscettibili di sequestro nell'ambito delle indagini penali.

Sotto il profilo classificatorio, i dati informatici possono essere ricondotti a una duplice direttrice sistematica⁴.

In prima battuta, sul piano tecnico-operativo, è possibile distinguere tra:

- *stored data*, ossia i dati memorizzati stabilmente all'interno di un sistema informatico o di un supporto digitale;
- *data in transit*, vale a dire i dati in fase di trasmissione tra sistemi informatici attraverso reti di comunicazione.

In seconda battuta, sul piano del contenuto e della funzione informativa, si distinguono:

- *traffic data* (dati di traffico), da intendersi come i dati informatici definiti dalla convenzione sopra citata;
- *personal data* (dati personali), intesi, ai sensi dell'art. 3, n. 1, della direttiva (UE) 2016/680, come “qualsiasi informazione riguardante

3. Per un quadro generale sulle tensioni tra le categorie classiche del diritto penale sostanziale e processuale con riferimento ai reati informatici si veda RUGGIERI-PICOTTI 2011. Per approfondire il tema del *locus commissi delicti* con riferimento ai reati informatici, si veda ad esempio CORONA 2021 e ATERNO 2023. In tema di legge penale nello spazio, si veda ad esempio FLOR 2019; per la letteratura straniera KOBRIN 2001. Sulle esigenze relative alle garanzie, si rimanda invece, *ex multis*, a CENTORAME 2025, DINACCI 2025, FLOR 2023, FLOR-PANATTONI 2023, FLOR-MARCOLINI 2022.

4. Per un approfondimento FLOR 2025.

una persona fisica identificata o identificabile” direttamente o indirettamente, “in particolare con riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici dell’identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica”;

- *content data* (dati di contenuto), i quali attengono al contenuto sostanziale delle comunicazioni e delle interazioni digitali, comprendendo tutte le informazioni trasmesse mediante sistemi informatici e telematici. In tale categoria rientrano, tra gli altri, messaggi di testo, comunicazioni vocali, immagini, contenuti audio e video, nonché ulteriori forme di corrispondenza elettronica, secondo una nozione ormai consolidata anche nelle più recenti fonti internazionali in materia di criminalità informatica.

Come già evidenziato, tali informazioni presentano una intrinseca volatilità, essendo la loro esistenza strettamente connessa ai sistemi che le generano e le conservano. Esse possono essere alterate, sovrascritte o cancellate anche in assenza di modificazioni percepibili del supporto fisico e risultano spesso accessibili esclusivamente mediante infrastrutture tecnologiche esterne e dinamiche. Ne deriva che l’informazione digitale si configura come un fenomeno non soltanto complesso e stratificato, ma altresì strutturalmente instabile, la cui acquisizione e conservazione richiedono specifiche cautele tecniche e giuridiche.

A corollario delle investigazioni digitali emerge quindi la disciplina della *digital forensics*, la quale, mediante l’impiego di protocolli tecnici standardizzati e procedure di acquisizione controllata, consente la corretta cristallizzazione e conservazione delle tracce informatiche, garantendo che il dato acquisito mantenga piena integrità, autenticità e non alterazione rispetto al contenuto originario.

Accanto ai profili di complessità tecnica e volatilità del dato, spicca infine il carattere fortemente intrusivo del sequestro di informazioni digitali. La peculiare capacità ricostruttiva dei dati informatici consente infatti l’accesso ad una quantità estremamente ampia e dettagliata di informazioni, tale da distinguere il sequestro digitale dalle tradizionali

forme di apprensione. Ne deriva un significativo ampliamento della capacità di penetrazione dell’attività investigativa nella sfera privata del soggetto interessato, con la conseguente necessità di un rigoroso bilanciamento tra esigenze di accertamento penale e tutela dei diritti fondamentali della persona.

4. Il sequestro digitale nel quadro delle investigazioni informatiche

Le considerazioni sin qui svolte consentono di comprendere come il sequestro digitale si collochi all’interno di un contesto investigativo profondamente diverso rispetto a quello cui erano originariamente rivolte le tradizionali categorie processual-penalistiche. Le investigazioni digitali, infatti, come evidenziato, si sviluppano in un ambiente caratterizzato da velocità, mutevolezza, volatilità e ubiquità del dato informatico, nel quale le informazioni risultano potenzialmente illimitate, immediatamente replicabili e spesso dislocate in infrastrutture tecnologiche transnazionali.

Parallelamente, l’evoluzione delle forme di criminalità contemporanea, sempre più caratterizzate dall’utilizzo di tecnologie di comunicazione avanzate, sistemi crittografici, piattaforme decentralizzate e strumenti di anonimizzazione, ha ulteriormente accentuato la centralità della prova digitale e delle tecniche di acquisizione informatica⁵. In tale contesto, il rischio è che l’attività di ricerca della prova finisca per trasformarsi, ove non adeguatamente delimitata, in una più ampia e indistinta attività di ricerca di notizie di reato, mediante forme di acquisizione massiva e indiscriminata di dati personali e comunicativi. La particolare capacità espansiva delle investigazioni digitali impone pertanto di interrogarsi sui limiti del potere investigativo e sulle garanzie necessarie a evitare indebite compressioni dei diritti fondamentali dell’individuo.

La difficoltà del diritto positivo di adattarsi con rapidità all’evoluzione tecnologica ha determinato, in questo settore, una significativa distanza tra innovazione tecnica e regolamentazione normativa. Le investigazioni digitali risultano infatti regolate da un sistema multilivello, composto da fonti interne, sovranazionali e convenzionali, la cui effettività

5. In rete e grazie alla rete non si sono sviluppate soltanto nuove forme di criminalità, ma si sono trasformate anche quelle tradizionali, comprese le organizzazioni mafiose; sul punto v. PICARELLA 2025.

è stata progressivamente integrata dall'elaborazione giurisprudenziale nazionale ed europea.

La limitata tipizzazione normativa degli strumenti di indagine informatica ha comportato l'attribuzione alla giurisprudenza di un ruolo centrale nella definizione dei limiti e delle modalità di esercizio dei poteri investigativi⁶. È stata infatti la prassi applicativa, insieme agli orientamenti delle corti nazionali e sovranazionali, a confrontarsi con l'impatto delle investigazioni digitali sui principi costituzionali, contribuendo all'adattamento degli strumenti tradizionali di ricerca della prova alle esigenze di contrasto alla criminalità tecnologica.

In tale prospettiva, il quadro normativo e giurisprudenziale si è sviluppato attorno a profili essenziali: le modalità di acquisizione e utilizzabilità della prova digitale, i limiti di ammissibilità delle tecniche investigative alla luce dei diritti fondamentali, le regole di conservazione e autenticazione del dato informatico, le problematiche della cooperazione internazionale e dell'acquisizione transfrontaliera delle prove, nonché le garanzie difensive e i poteri concretamente esercitabili dalla polizia giudiziaria nelle indagini informatiche.

L'assenza di una disciplina organica ha inoltre determinato l'adattamento dei tradizionali mezzi di ricerca della prova all'ambiente digitale. Perquisizioni, ispezioni, sequestri e attività di osservazione sono stati progressivamente reinterpretati alla luce delle peculiarità del contesto informatico, subendo significative trasformazioni funzionali e operative. Ne è derivato un ampliamento rilevante della capacità conoscitiva dell'autorità investigativa, che incide non solo sulle modalità di esecuzione degli atti, ma talvolta sulla loro stessa natura sostanziale.

Sul piano normativo interno, il principale riferimento resta la disciplina del sequestro probatorio

di cui all'art. 253 c.p.p., ai sensi del quale (comma 1) "l'autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti". Tale disposizione, concepita in relazione a beni materiali, è stata progressivamente estesa in via interpretativa anche a dispositivi digitali e dati informatici, evidenziando una tensione tra categorie tradizionali e realtà tecnologica⁷.

In tale evoluzione si manifesta una delle principali criticità sistematiche della materia: nel sequestro digitale l'oggetto effettivo dell'attività investigativa non coincide più necessariamente con il supporto materiale, bensì con i dati in esso contenuti o accessibili tramite esso, con conseguente degradazione del bene fisico a mero strumento di accesso all'informazione.

A ciò si affiancano le innovazioni introdotte dalla legge 18 marzo 2008, n. 48, di ratifica della Convenzione di Budapest sul cybercrime⁸, che ha inserito specifiche disposizioni relative ai sistemi informatici e telematici. Emerge, in particolare, l'art. 247, comma 1-bis, c.p.p., che disciplina la perquisizione di sistemi informatici mediante misure tecniche idonee a garantire la conservazione dei dati e la loro immodificabilità, nonché l'art. 254-bis c.p.p., relativo al sequestro di dati presso fornitori di servizi informatici, telematici e di telecomunicazioni, volto a regolare l'acquisizione di informazioni detenute da provider e operatori delle comunicazioni.

Il quadro è stato ulteriormente rafforzato dalla legge 28 giugno 2024, n. 90 in materia di cybersicurezza nazionale e reati informatici, che ha inciso su diversi profili processuali, ampliando il catalogo dei reati rilevanti e intervenendo su competenze, durata delle indagini e poteri di coordinamento

6. Si segnala la recentissima pronuncia della quinta sezione penale della Suprema Corte di fine aprile 2026 che, intervenendo sul tema del sequestro probatorio di dispositivi informatici e asset digitali, ha dichiarato illegittimo il sequestro che si traduce in un'acquisizione indiscriminata del patrimonio digitale del soggetto sottoposto ad indagini, in mancanza di criteri selettivi previamente determinati e di termini per la restituzione del materiale non pertinente.

7. Si ricorda che la prima giurisprudenza in materia di reti informatiche riconosceva nel software un bene materiale, una res incorporata nel supporto materiale, al fine di poter applicare anche ad esso la disciplina codicistica. Solo successivamente, con l'emersione della dimensione reticolare e dematerializzata dell'informazione digitale, si è progressivamente affermata una concezione autonoma del dato informatico quale entità immateriale ma giuridicamente rilevante, suscettibile di tutela e apprensione indipendentemente dal supporto che lo contiene.

8. Consiglio d'Europa, Convenzione di Budapest sulla criminalità informatica, 23 novembre 2001. Sul punto, si veda LUPÀRIA 2009.

investigativo, oltre a introdurre discipline derogatorie in materia di intercettazioni per reati contro sistemi informatici di rilievo strategico⁹.

In questa traiettoria si colloca anche il recente disegno di legge¹⁰ volto all'introduzione dell'art. 254-ter c.p.p., finalizzato a rafforzare le garanzie di tutela della riservatezza mediante un obbligo di selezione rigorosa dei soli dati pertinenti, secondo criteri di necessità e proporzionalità.

Un ulteriore profilo rilevante attiene al rapporto con la disciplina europea in materia di protezione dei dati personali. In aggiunta, la Direttiva LED¹¹, attuata con il d.lgs. n. 51/2018, ha contribuito a definire un sistema fondato sui principi di proporzionalità, necessità e minimizzazione del trattamento, costituendo un parametro imprescindibile per la conformazione delle investigazioni digitali.

Le investigazioni informatiche si collocano, inoltre, in un contesto multilivello nel quale il diritto dell'Unione europea incide in modo significativo sull'equilibrio tra efficacia investigativa e tutela dei diritti fondamentali. Oltre alla Direttiva 2016/680 già citata, si sottolineano la Direttiva PNR¹² e l'AI Act¹³, destinato a incidere anche sull'impiego di sistemi di intelligenza artificiale nelle attività investigative, unitamente alla disciplina sulla

cooperazione giudiziaria e alla regolazione dei rapporti con i fornitori di servizi digitali.

Sul piano sovranazionale, assumono rilievo gli strumenti elaborati dalle Nazioni Unite, in particolare le Convenzioni di Palermo¹⁴ e di Mérida¹⁵, che disciplinano tecniche investigative speciali nel contrasto alla criminalità organizzata e alla corruzione. La recente Convenzione ONU sulla criminalità informatica¹⁶ ha inoltre introdotto specifiche disposizioni in materia di perquisizione e sequestro di dati elettronici, intercettazione e raccolta in tempo reale dei dati di traffico, richiamando il rispetto dei diritti umani e del principio di proporzionalità.

Un ruolo centrale continua a essere svolto dal Consiglio d'Europa attraverso la Convenzione di Budapest¹⁷, primo strumento internazionale organico in materia di criminalità informatica, successivamente integrato dal Secondo Protocollo addizionale, volto a rafforzare la cooperazione internazionale e l'acquisizione transfrontaliera delle prove digitali.

4.1. Il sequestro probatorio di dispositivi e informazioni digitali

Con riferimento a quanto già illustrato nei paragrafi precedenti, le principali forme di sequestro

9. Nel complesso, la materia delle investigazioni digitali è stata interessata da molteplici e successivi interventi normativi che hanno inciso su diversi istituti del codice di procedura penale, determinando una profonda riorganizzazione del sistema delle garanzie e degli strumenti investigativi in ambito informatico. Tra questi, si segnala in particolare la disciplina del captatore informatico, oggetto di ripetute riforme (d.lgs. n. 216/2017, l. n. 3/2019, l. n. 7/2020 e l. n. 137/2023). Tali profili, per la loro complessità e ampiezza, non possono essere qui approfonditi, ma vengono richiamati solo in via generale in considerazione della loro rilevanza sistematica all'interno dell'evoluzione della disciplina delle investigazioni digitali.

10. Disegno di Legge (ddl) n. 806, noto come ddl Zanettin-Bongiorno. Per un approfondimento sulle novità proposte in materia di sequestro di dispositivi e di dati si vedano DELLA TORRE 2025 e CAIANIELLO 2025.

11. Direttiva (UE) 2016/680 relativa 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, nonché alla libera circolazione di tali dati (c.d. Law Enforcement Directive).

12. Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (Passenger Name Record – PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

13. Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (Artificial Intelligence Act).

14. Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, 15 novembre 2000.

15. Convenzione delle Nazioni Unite contro la corruzione, 31 ottobre 2003.

16. Assemblea generale delle Nazioni Unite, Convenzione ONU sulla criminalità informatica, adottata il 24 dicembre 2024.

17. Cfr. nota 8.

rilevanti nell'ambito delle investigazioni digitali riconducono al sequestro probatorio, disciplinato dal codice di procedura penale e tradizionalmente configurato come uno dei mezzi di ricerca della prova maggiormente significativi nelle indagini informatiche palesi¹⁸. È proprio la citata dissociazione tra supporto fisico e dato digitale a rappresentare uno degli elementi di maggiore discontinuità rispetto alle tradizionali categorie del sequestro probatorio.

In ambito informatico, inoltre, il sequestro può avere ad oggetto una pluralità eterogenea di elementi – proprio alla luce della complessa natura del dato – quali siti web, infrastrutture di rete, dispositivi digitali o singole porzioni di dati¹⁹. Rientrano in tale prospettiva anche misure incidenti sull'accessibilità delle risorse online, quali l'oscuramento di siti Internet, il sequestro di server contenenti materiale illecito o il blocco di account utilizzati per la commissione di attività fraudolente.

Particolare attenzione è riservata dall'ordinamento alla tutela dell'integrità della prova digitale. In tale direzione si colloca l'art. 260, comma 2, c.p.p., il quale prevede che, quando il sequestro abbia ad oggetto dati, informazioni o programmi informatici, la loro duplicazione debba avvenire mediante copie su adeguati supporti, secondo procedure idonee a garantirne la conformità all'originale e l'immodificabilità. La disposizione recepisce le esigenze proprie della *digital forensics*, imponendo l'impiego di tecniche di copia forense e di sistemi di conservazione volti a preservare la genuinità e l'affidabilità del dato acquisito.

Il sequestro può essere disposto dal pubblico ministero o dal giudice e viene generalmente eseguito dalla polizia giudiziaria specializzata, anche mediante strumenti tecnici quali la duplicazione forense dei supporti, la cifratura dei dati o misure di inibizione dell'accesso a risorse online, tra cui il DNS blocking o il blocco degli indirizzi IP.

Completa il quadro il rilievo assunto dai principi elaborati dalla giurisprudenza, che – anche

in materia di sequestro probatorio – impongono costantemente il rispetto dei criteri di proporzionalità, pertinenza e adeguata motivazione del provvedimento ablatorio, a garanzia dell'equilibrio tra esigenze investigative e tutela dei diritti fondamentali.

4.2. Sequestro preventivo di dispositivi e informazioni digitali

Accanto al sequestro probatorio, l'ordinamento prevede il sequestro preventivo, disciplinato dall'art. 321 c.p.p., configurabile come misura cautelare reale finalizzata a impedire la protrazione o l'aggravamento delle conseguenze del reato, ovvero la commissione di ulteriori illeciti. Nell'ambito delle investigazioni digitali, tale istituto assume particolare rilievo quando dispositivi informatici quali computer, smartphone, tablet o server risultano funzionalmente connessi alla realizzazione dell'attività criminosa o idonei a consentirne la continuazione.

A differenza del sequestro probatorio, che è strumentale all'acquisizione della prova, il sequestro preventivo è caratterizzato da una finalità eminentemente cautelare: esso non è diretto all'accertamento del fatto, bensì alla neutralizzazione del pericolo derivante dalla libera disponibilità del bene. In ambito digitale, ciò si traduce nell'esigenza di impedire l'accesso a dati sensibili, la prosecuzione di attività fraudolente, la diffusione di contenuti illeciti o l'utilizzo del dispositivo come strumento operativo per la commissione di nuovi reati.

Il sequestro preventivo di dispositivi informatici può riguardare l'intero bene oppure specifiche funzionalità o contenuti, sebbene nella prassi l'apprensione materiale del dispositivo rappresenti la modalità più frequente. Tale soluzione è spesso giustificata dall'esigenza di impedire immediatamente qualsiasi utilizzo del sistema informatico, soprattutto nei casi in cui esso risulti strettamente funzionale all'attività illecita, come nelle ipotesi di

18. Accanto a queste, si apre il mondo delle investigazioni digitali occulte, quale, ad esempio, l'utilizzo del captatore informatico. Tra i numerosi contributi su questo strumento, si vedano, ad esempio, TORRE 2017 e MAGGIO 2021. Per uno studio sulle investigazioni digitali, si rimanda a NICOLINI 2026, SIGNORATO 2024, TORRE 2024, NOCERINO 2021, MARCOLINI 2015, RIVELLO 2014, LUPÁRIA-ZICCARDI 2007 e MARINELLI 2007. Un approfondimento, invece, sulle perquisizioni online si può rinvenire in MARCOLINI 2010.

19. Per un approfondimento sul sequestro di dispositivi digitali si rimanda, *ex multis*, a LORENZETTO 2025, SIGNORATO 2025, GRAMUGLIA 2021, CAMPANARO 2012, VITKOV 2012, BETTONI 2012 e ATERNO 2008.

truffe online, cyberstalking, accessi abusivi a sistemi informatici o diffusione di materiale illecito.

Il provvedimento richiede la sussistenza dei presupposti tipici delle misure cautelari reali, ossia il *fumus commissi delicti* e il *periculum in mora*²⁰. Quest'ultimo assume nel contesto digitale una particolare rilevanza, potendo consistere nel rischio di alterazione, cancellazione o dispersione dei dati, nella prosecuzione dell'attività illecita tramite il dispositivo ovvero nella compromissione dell'efficacia delle indagini in corso. Ne consegue che il sequestro deve essere sorretto da un'adeguata motivazione, che dia conto non solo della configurabilità del reato, ma anche della concreta necessità della misura in relazione al pericolo da neutralizzare. La giurisprudenza, inoltre, richiede il rigoroso rispetto dei principi di proporzionalità e adeguatezza.

4.3. Sequestro conservativo di dispositivi digitali

Un cenno merita, infine, il sequestro conservativo, disciplinato dagli artt. 316 e ss. c.p.p., volto a garantire le obbligazioni civili derivanti dal reato, quali il pagamento della pena pecuniaria o il risarcimento del danno in favore della parte civile. In tale prospettiva, anche dispositivi informatici possono essere assoggettati alla misura esclusivamente nella loro dimensione patrimoniale, in quanto beni suscettibili di valutazione economica e, dunque, potenzialmente aggredibili ai fini della garanzia creditoria. Diversamente, invece, i dati informatici non assumono autonoma rilevanza quale oggetto del vincolo, se non nei limiti in cui risultino incorporati o funzionalmente riconducibili a un bene patrimoniale²¹.

5. Fasi operative del sequestro informatico e acquisizione dei dati digitali

La procedura di sequestro di un dispositivo informatico si articola, in via generale, attraverso una sequenza di fasi logicamente progressive. In primo luogo, si procede all'identificazione del dispositivo da sottoporre a vincolo, che può avvenire presso l'abitazione, il luogo di lavoro o altri contesti nella disponibilità dell'indagato. A tale fase segue l'adozione del decreto

di sequestro da parte dell'autorità giudiziaria, secondo la disciplina normativa di riferimento.

Successivamente si realizza l'intervento operativo sul dispositivo, che comprende le attività di messa in sicurezza del sistema, spesso mediante l'attivazione della modalità aereo o l'utilizzo di strumenti di protezione forense, al fine di impedirne l'alterazione o l'uso da remoto. In questa fase può essere eseguita, ove necessario, la duplicazione forense dei dati, mediante la creazione di una copia integrale della memoria del dispositivo, idonea a garantire la conservazione dell'originale e l'analisi separata dei contenuti.

La fase successiva riguarda l'analisi dei dati acquisiti, effettuata mediante software forensi specializzati, che consentono l'estrazione e l'esame di informazioni quali fotografie, video, comunicazioni elettroniche, e-mail, dati di geolocalizzazione, cronologia di navigazione e ulteriori evidenze digitali rilevanti.

Al termine delle operazioni, viene redatto un verbale analitico contenente la descrizione delle attività svolte e l'elenco dei dati estratti, mentre la copia forense viene conservata integra e messa a disposizione delle parti, secondo le garanzie previste dall'ordinamento.

Elemento centrale dell'intero procedimento è rappresentato dalla catena di custodia, ossia il complesso delle regole e delle procedure volte a garantire la conservazione, la tracciabilità e l'integrità del reperto informatico dal momento dell'acquisizione fino al suo eventuale utilizzo in sede processuale²². Ogni fase di trattamento del dispositivo o dei dati deve essere accuratamente documentata mediante verbali, registrazioni e sistemi di controllo, idonei a escludere alterazioni, manipolazioni o contaminazioni della prova. La compromissione della catena di custodia può infatti incidere in modo significativo sull'affidabilità del dato e, conseguentemente, sulla sua utilizzabilità processuale.

La crescente dimensione transnazionale dei dati digitali impone, inoltre, il ricorso a strumenti di cooperazione giudiziaria internazionale. In ambito europeo assumono particolare rilievo gli ordini europei di produzione e conservazione delle prove elettroniche, finalizzati a consentire l'acquisizione

20. Per un approfondimento in materia di misure cautelari reali si rinvia, *ex multis*, a CORDERO 1991 e SPANGHER 2017.

21. Per una riflessione sul valore del dato si rimanda a D'AGOSTINO PANEBIANCO 2023.

22. Sulla catena di custodia del dato informatico si rimanda a BARTOLI-MAIOLI 2015.

rapida di dati detenuti da fornitori di servizi stabiliti in altri Stati membri, superando in parte le tradizionali lentezze delle rogatorie internazionali. L'utilizzo di tali strumenti richiede tuttavia il rispetto dei differenti ordinamenti giuridici e delle garanzie poste a tutela dei diritti fondamentali.

Infine, una delle principali criticità operative nelle indagini digitali riguarda l'accesso a sistemi protetti da password, autenticazione multifattoriale o crittografia avanzata. La diffusione di tecniche di cifratura end-to-end e di sistemi di protezione biometrica rende spesso complesso, se non impossibile, l'accesso immediato ai dati, imponendo il ricorso a strumenti tecnici altamente specialistici e a metodologie investigative sempre più sofisticate.

6. Garanzie difensive e diritti fondamentali

L'evoluzione delle tecnologie digitali e l'intensificazione delle attività investigative fondate sull'utilizzo di dati informatici impongono la progressiva elaborazione di un modello di *digital due process*, inteso quale adattamento delle garanzie del giusto processo alle peculiarità dell'ambiente digitale²³. Tale impostazione muove dal presupposto che le garanzie processuali tradizionali non possano essere semplicemente trasposte nel contesto tecnologico, ma debbano essere reinterpretate alla luce delle caratteristiche strutturali della prova digitale, quali la volatilità, la replicabilità e la sua intrinseca immaterialità.

In tale prospettiva, il *digital due process* si articola attorno ad alcuni principi fondamentali, tra i quali assumono rilievo la tracciabilità delle operazioni tecniche, la trasparenza delle modalità di acquisizione, la piena effettività del contraddittorio e la verificabilità indipendente del dato informatico. Particolare importanza riveste, inoltre – come visto –, la catena di custodia, intesa come continuità documentata delle operazioni di conservazione e manipolazione del reperto digitale, la quale

costituisce presupposto essenziale per garantirne l'affidabilità e l'utilizzabilità probatoria.

Tale sistema di garanzie si innesta necessariamente sul piano dei diritti fondamentali, imponendo un costante bilanciamento tra esigenze investigative e tutela della sfera privata dell'individuo. In questo senso, i dispositivi digitali sono sempre più frequentemente qualificati come estensione della dimensione personale dell'individuo, in quanto contenitori di informazioni idonee a riflettere la sua identità relazionale, comunicativa e comportamentale, con la conseguenza che su di essi si concentra una particolarmente elevata "aspettativa ragionevole di riservatezza"²⁴.

La giurisprudenza sovranazionale ha contribuito in modo significativo a delineare i confini di tale tutela. La Corte europea dei diritti dell'uomo ha infatti ricondotto le manifestazioni della vita privata anche alla dimensione digitale e alle forme di espressione della personalità online, riconoscendo la protezione dell'art. 8 CEDU anche rispetto al trattamento di dati e comunicazioni elettroniche (tra le altre, *Smirnova c. Russia*, 2003; *Copland c. Regno Unito*, 2007; *Bărbulescu c. Romania*, 2017). In tale prospettiva, la Corte ha inoltre elaborato criteri di valutazione della legittimità delle attività investigative tecnologiche, richiedendo che l'ingerenza sia prevista dalla legge, persegua uno scopo legittimo e risulti necessaria in una società democratica, secondo un rigoroso giudizio di proporzionalità (*Yüksel Yalçınkaya c. Turchia*, 2023).

Anche la giurisprudenza costituzionale nazionale si è progressivamente adeguata a tale evoluzione, estendendo la tutela della vita privata e della segretezza delle comunicazioni alla dimensione tecnologica. In particolare, è stato ribadito che la libertà e la segretezza della corrispondenza, di cui all'art. 15 Cost., si estendono alle comunicazioni elettroniche (Corte cost. n. 170/2023), che i limiti alle stesse devono essere predeterminati e giustificati (Corte cost. n. 2/2021), e che il domicilio

23. Per un approfondimento sul tema della due diligence e delle garanzie procedurali nel contesto europeo succeduto al Digital Service Act si rimanda a GENTILE 2024.

24. L'espressione "aspettativa ragionevole di riservatezza" è stata introdotta per la prima volta nel 1967 dalla giurisprudenza statunitense, all'interno della storica sentenza della Corte Suprema *Katz v. United States*. Tale principio ha sancito il superamento del criterio della violazione fisica della proprietà privata, stabilendo che la tutela costituzionale della riservatezza "protegge le persone, non i luoghi". Questo concetto ha ridefinito il diritto alla privacy a livello globale, influenzando profondamente la giurisprudenza europea e italiana in materia di intercettazioni, sorveglianza digitale e protezione dei dati personali.

rappresenta una proiezione spaziale della persona (Corte cost. n. 135/2002). In tale quadro, anche i dati biometrici — quali impronte digitali, riconoscimento facciale e dati vocali — assumono una particolare rilevanza quale categoria di dati personali altamente sensibili, la cui utilizzazione investigativa richiede un rigoroso rispetto dei principi di proporzionalità e minimizzazione del trattamento.

Ne consegue che il bilanciamento tra esigenze investigative e diritti fondamentali si configura come elemento strutturale del sistema, tanto più evidente nell'ambito della prova digitale.

Sul versante delle garanzie difensive, l'art. 24 Cost. estende la tutela del diritto di difesa anche alle attività di acquisizione e analisi della prova informatica. Nei casi più complessi è quindi prevista la partecipazione della difesa alle operazioni tecniche, anche mediante la nomina di consulenti tecnici di parte, nonché la possibilità di intervenire nelle attività caratterizzate da irripetibilità, secondo le regole del contraddittorio anticipato.

La prova digitale è inoltre soggetta alla disciplina generale in tema di utilizzabilità prevista dal codice di procedura penale. Violazioni delle modalità di acquisizione, del contraddittorio o delle garanzie difensive possono comportare l'inutilizzabilità del dato, con conseguente esclusione dal compendio probatorio. In caso di violazioni procedurali, possono altresì configurarsi nullità, relative o assolute, a seconda della gravità del vizio, le quali possono essere fatte valere mediante i rimedi impugnatori previsti dall'ordinamento, quali riesame, appello o ricorso per cassazione.

Il profilo delle garanzie assume particolare rilievo per quanto riguarda i mezzi di ricerca della prova atipici, i quali ricorrono frequentemente nell'ambito dei reati informatici, caratterizzati dall'assenza di una disciplina legislativa specifica e da un limitato controllo giurisdizionale preventivo. In tali ipotesi, infatti, viene meno sia il vaglio tipico del legislatore, sia il controllo del giudice del dibattimento, previsto, invece, in relazione ai mezzi di prova atipici ai sensi dell'art. 189 c.p.p., con conseguente ampliamento degli spazi di discrezionalità nell'acquisizione del dato probatorio.

In definitiva, la giurisprudenza europea evidenzia come la prova digitale si collochi in una posizione di intersezione tra tutela della riservatezza e garanzie del giusto processo, imponendo

agli ordinamenti nazionali un costante adeguamento delle categorie processuali tradizionali. Ne emerge un modello europeo di equità digitale del processo, nel quale la legittimità della *digital evidence* non dipende esclusivamente dalla sua utilità investigativa, ma dalla qualità e dall'effettività delle garanzie che ne accompagnano l'acquisizione e l'utilizzazione.

7. Conclusioni

Alla luce delle criticità emerse nel corso dell'analisi, appare necessario valorizzare un'interpretazione sistematica della disciplina del sequestro e orientata ai principi costituzionali e convenzionali, con particolare riferimento al diritto di difesa, al giusto processo e alla tutela della riservatezza. In tale prospettiva, il sequestro di dispositivi e dati digitali impone una lettura evolutiva delle norme codicistiche, idonea a tenere conto delle peculiarità strutturali dell'ambiente informatico e della natura immateriale delle informazioni ivi contenute.

In questa cornice si colloca il concetto di *digital due process*, inteso come criterio ermeneutico funzionale ad adeguare le garanzie processuali tradizionali alle modalità operative del sequestro informatico. Esso consente di enfatizzare l'esigenza di un contraddittorio effettivo anche sul piano tecnico, nonché la necessità di assicurare la tracciabilità delle operazioni di acquisizione e la verificabilità delle modalità di estrazione e conservazione dei dati.

In prospettiva *de iure condendo*, una prima direttrice di intervento potrebbe consistere nell'introduzione di una disciplina organica del sequestro digitale, o di uno specifico statuto delle attività di apprensione informatica, che disciplini in modo puntuale le modalità esecutive, la duplicazione forense, la conservazione dei dati e le forme di accesso ai medesimi. Tale intervento dovrebbe altresì prevedere criteri chiari di validità e utilizzabilità, con particolare attenzione alla tutela della catena di custodia e alla completa documentazione delle operazioni compiute.

Più in generale, si evidenzia l'esigenza di un intervento legislativo di sistema, volto a ridurre la frammentazione normativa attualmente esistente e a garantire standard tecnici uniformi, idonei ad assicurare la controllabilità delle attività di sequestro informatico e l'effettiva partecipazione della difesa sin dalle fasi iniziali dell'acquisizione del dato.

In conclusione, il sequestro di dispositivi e informazioni digitali non rappresenta soltanto un'evoluzione tecnica dei tradizionali mezzi di ricerca della prova, ma costituisce un ambito nel quale si misura la

capacità dell'ordinamento di mantenere un equilibrio effettivo tra esigenze investigative e tutela dei diritti fondamentali, nell'attuale contesto di progressiva digitalizzazione delle indagini penali.

Riferimenti bibliografici

- S. ATERNO (2023), *Profili penali della vita nel Metaverso*, in G. Cassano, G. Scorza (a cura di), "Metaverso. Diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini Giuridica, 2023
- S. ATERNO (2008), *Acquisizione e analisi della prova informatica*, in "Diritto e Procedura Penale", Dossier, La prova scientifica nel processo penale, 2008
- L. BARTOLI, C. MAIOLI (2015), *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in "Informatica e diritto", 2015
- M. BETTONI (2012), *Il sequestro preventivo di siti web tramite ordine agli ISP: osservazioni sui casi Moncler e Vajont.info*, in "Cyberspazio e diritto" 2012, n. 1
- M. CAIANIELLO (2025), *Ancora in tema di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali (disegno di legge C. 806)*, in "Sistema Penale", 2025
- C. CAMPANARO (2012), *Legittimo il sequestro preventivo del sito internet se i contenuti sono diffamatori*, in "Diritto Penale Contemporaneo", 2012
- F. CENTORAME (2025), *Le indagini Tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in "Cassazione Penale", 2025, n. 2
- F. CORDERO (1991), *Procedura penale*, I ed., Giuffrè, 1991
- F. CORONA (2021), *Il cybercrime: soggetto, oggetto e condotta*, in Id. (a cura di), "Reati informatici e investigazioni digitali", Pacini Giuridica, 2021
- M. D'AGOSTINO PANEBIANCO (2023), *Il "dato": bene immateriale con un proprio valore intrinseco*, in "Ambienteditto", 2023, n. 2
- M. DANIELE (2011), *La prova digitale nel processo penale*, in "Rivista di Diritto Processuale", 2011
- J. DELLA TORRE (2025), *Spunti di riflessione sulla proposta di legge in materia di sequestro di dispositivi e di dati*, in "Sistema Penale", 2025
- F. DINACCI (2025), *Sequestro di dispositivi informatici: imposizioni tecnologiche e scelte interpretative. Alla ricerca di un recupero della legalità probatoria*, in "Archivio Penale", 2025
- R. FLOR (Ed.) (2025), *Investigations in the digital environment: procedural principles, rules and multi-actor cooperation*, Technical Report, 2025
- R. FLOR (2023), *Lawful hacking, vulnerabilità tecnologica e diritto penale, fra esigenze di accertamento dei reati e tutela di beni giuridici di nuova generazione*, in L. Picotti (a cura di), "Automazione, diritto e responsabilità", Edizioni Scientifiche Italiane, 2023
- R. FLOR (2019), *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime. Diritto e procedura penale dell'informatica", Utet Giuridica, 2019
- R. FLOR, S. MARCOLINI (2022), *Dalla Data Retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022

- R. FLOR, B. PANATTONI (2023), *Digital criminal investigations in Italy. The intersection between data protection and cybersecurity*, in "New Journal of European Criminal Law", vol. 14, 2023, n. 4
- G. GENTILE (2024), *Between Online and Offline Due Process: The Digital Services Act*, in A. Engel, X. Groussot, G.T. Petursson (Eds.), "New Directions in Digitalisation", Springer, 2024
- V. GRAMUGLIA (2021), *Sequestro probatorio del reperto digitale e manifestazioni distorsive dell'attività di indagine*, in "Diritto di Internet", 2021
- S.J. KOBRIN (2001), *Territoriality and the Governance of Cyberspace*, in "Journal of International Business Studies", 2001
- E. LORENZETTO (2025), *I sequestri di smartphone, dispositivi informatici e memorie digitali*, in G. Di Paolo, L. Pressacco (a cura di), "Indagini e prove nella società digitale. Questioni attuali e prospettive future", Università degli Studi di Trento, 2025
- L. LUPÁRIA (a cura di) (2009), *Sistema penale e criminalità informatica: profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (L. 18 marzo 2008, n. 48)*, Giuffrè, 2009
- L. LUPÁRIA, G. ZICCARDI (a cura di) (2007), *Investigazione penale e tecnologia informatica*, Giuffrè, 2007
- P. MAGGIO (2021), *Intercettazioni no limits: il captatore informatico "per istradamento"*, in "Processo penale e giustizia", 2021
- S. MARCOLINI (2015), *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in "Cassazione Penale", 2015, n. 2
- S. MARCOLINI (2010), *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in "Cassazione Penale", 2010, n. 7-8
- C. MARINELLI (2007), *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007
- M. NICOLINI (2026), *La Cassazione torna sul tema del sequestro finalizzato all'acquisizione di prove digitali consolidando l'evoluzione dello statuto del PM come organo di giustizia*, in "Sistema Penale", 2026
- W. NOCERINO (2021), *Nuove tecnologie e processo penale – Il tramonto dei mezzi di ricerca della prova nell'era 2.0*, in "Diritto Penale e Processo", 2021
- L. PICARELLA (2025), *Criminalità in rete: Dalle piattaforme illegali alle cybermafie*, Donzelli editore, 2025
- M. PITTIRUTI (2021), *Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in "Sistema penale", 2021
- P.P. RIVELLO (2014), *La prova scientifica*, Giuffrè, 2014
- F. RUGGIERI, L. PICOTTI (a cura di) (2011) *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Giappichelli, 2011
- S. SIGNORATO (2025), *Il sequestro di dispositivi e informazioni digitali*, in "Sistema Penale", 2025
- S. SIGNORATO (2024), *Indagini e prove digitali*, in "Rivista di Diritto Processuale", 2024
- G. SPANGHER (2017), *Le misure cautelari reali: "figlie di un dio minore"*, in "Libro dell'anno del diritto 2017", Treccani, 2017
- M. TORRE (2024), *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in "Diritto penale e processo", 2024, n. 6
- M. TORRE (2017), *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017

V. VITKOV (2012), *Il sequestro preventivo di siti web: nota a Corte di Cassazione, Sez. V penale, sentenza del 19 settembre 2011, n. 46504*, in “Cyberspazio e diritto”, 2012, n. 1



FEDERICA DELAINI

Verso un diritto penale della sicurezza digitale? La cyber-compliance del Regolamento DORA

Il contributo si inserisce nel dibattito sulle sfide che il diritto penale è chiamato ad affrontare nell'era della digitalizzazione, muovendo dall'evoluzione della criminalità informatica e dalla pervasività delle nuove tecnologie, che hanno posto in crisi il paradigma repressivo tradizionale. In tale contesto, il legislatore europeo ha adottato un approccio pragmatico e settoriale per contrastare le emergenti forme di criminalità, anticipando la soglia di tutela dei beni giuridici coinvolti. Questa politica legislativa segna una trasformazione verso la giuridicizzazione del rischio informatico e il rafforzamento della resilienza operativa digitale, attraverso l'adozione di pratiche organizzative virtuose e l'impiego della sicurezza informatica come strumento di prevenzione normativa. L'analisi si concentra sul settore finanziario, bancario e assicurativo, divenuti, a livello europeo, laboratori di sperimentazione giuridica. In questo quadro, il *Digital Operational Resilience Act* emerge come un modello di *governance* orientato alla prevenzione e alla proattività. L'obiettivo è individuare i caratteri "mobilitatori" che possono sostenere la tecnica legislativa penalistica nel quinto dominio.

*Diritto penale nell'era digitale – Criminalità informatica – Giuridicizzazione del rischio informatico
Cybersecurity governance – Digital Operational Resilience Act (DORA)*

Towards a Criminal Law of Digital Security? Cyber compliance under the DORA Regulation

This article contributes to the ongoing debate on the challenges faced by criminal law in the digital age, starting from the evolution of cybercrime and the pervasive nature of new technologies, which have called into question the conventional repressive paradigm. In this context, the European legislator has adopted a pragmatic and sectoral approach aimed at addressing emerging forms of cybercrime while anticipating the threshold of protection of the legal interests involved. This legislative policy marks a significant transformation towards the juridification of cyber risk and the strengthening of digital operational resilience, grounded in the adoption of virtuous organisational practices and in the use of cybersecurity as a regulatory prevention tool. The analysis focuses on the financial, banking and insurance sectors, which have become, at the European level, laboratories of legal experimentation. Within this framework, the Digital Operational Resilience Act emerges as a model of governance geared towards prevention and proactivity. The article aims to identify the "mobilising" features that may support criminal legislative technique within the fifth domain.

*Criminal law in the digital age – Cybercrime – Juridification of cyber risk – Cybersecurity governance
Digital Operational Resilience Act (DORA)*

L'Autrice è dottoranda in Diritto penale nel programma di Dottorato in Scienze giuridiche europee e internazionali dell'Università di Verona. Il suo dottorato innovativo industriale è finanziato dall'Unione Europea nell'ambito del programma Next Generation EU, Missione 4, Componente 1, CUP B31I23000810004, in collaborazione con Generalfinance S.p.A.

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli

SOMMARIO: 1. Introduzione. Le sfide del diritto penale nell'era digitale. – 2. Verso un nuovo paradigma preventivo-proattivo. – 3. Dal rischio al diritto: la costruzione europea della resilienza operativa digitale. – 4. Il Digital Operational Resilience Act: una governance multidisciplinare e multilivello tra prevenzione, co-regolazione e responsabilità multistakeholder. – 4.1. Il regime di responsabilità in caso di violazione del Regolamento DORA. – 4.2. I presidi a tutela della sicurezza informatica della supply-chain. – 4.3. L'impatto del Regolamento DORA sulla prassi contrattuale attuale. – 5. Il Regolamento DORA come modello di best practice e la cybersecurity come nuova architrave normativa dei mercati digitali. – 6. Riflessioni conclusive. I caratteri "mobilitatori" del diritto penale della sicurezza digitale.

1. Introduzione. Le sfide del diritto penale nell'era digitale

Nell'epoca della digitalizzazione, il diritto, e, in particolare, il diritto penale, si muove su un terreno segnato da un'elevata ambiguità e da una repentina mutevolezza, che impone al penalista di interrogarsi sulla strategia più efficace per dominare la globalizzazione tecnocentrica che interessa la nostra realtà sociale, economica e giuridica. Il progresso tecnologico ha ormai permeato ogni ambito della nostra esistenza e impone anche al diritto di adeguarsi, dal momento che la normativa si sostanzia nell'insieme delle regole che stabiliscono *chi vince e a quale prezzo*.

Analogamente a quanto accade con l'interazione tra uomo e macchina, che potenzia le capacità dell'individuo, anche il crimine informatico può beneficiare di tale sinergia. Per tale ragione, il diritto penale, lungi dall'assumere una connotazione squisitamente antropocentrica, potrebbe più opportunamente ampliare il suo sguardo alle modalità tecnologicamente connotate che possono sia contribuire alla commissione dei reati, sia, attualmente, caratterizzarla in via esclusiva.

Questa evoluzione sollecita una riflessione sulla metodologia che il diritto penale potrebbe adottare per contrastare efficacemente il cybercrime. Nello specifico, il diritto penale dell'informatica sta attraversando una trasformazione di portata epocale, che riveste una valenza paradigmatica,

implicando un ripensamento delle categorie fondamentali della scienza penalistica.

L'evidenza empirica dimostra che un sistema fondato esclusivamente su logiche repressive si rivela inefficace, in quanto interviene quando il danno ha già avuto luogo. Al contrario, la promozione di strategie preventive – siano esse normative, tecniche o culturali – può ridurre la necessità di ricorrere alla sanzione penale, rafforzandone l'efficacia complessiva.

In tale prospettiva, la deterrenza assume una dimensione strutturale, non più fondata esclusivamente sulla minaccia della pena, bensì sull'anticipazione del rischio e sulla costruzione di un ambiente digitale sicuro e resiliente, attraverso comportamenti organizzativi e tecnico-informativi virtuosi.

Il contributo si propone di esaminare le frontiere e i limiti della nuova era che si è inaugurata per la tecnica penalistica, caratterizzata da un'importante espansione della legislazione europea, che evidenzia come un linguaggio minimo non sia più praticabile. Le direttive e i regolamenti hanno subito una trasformazione significativa, denotando uno sviluppo in senso pregnante, secondo una duplicità di direttrici, sistematiche e settoriali allo stesso tempo.

Inoltre, la nuova legislazione si distingue per una trasformazione concettuale di cruciale rilevanza, sintetizzata dall'espressione "dal rischio al diritto". Il rischio tecnologico, che, attualmente, è stato elevato a potenziale rischio sistemico a causa

dell'interconnessione infrastrutturale e della pervasività dei servizi digitali, è stato riconosciuto come una categoria autonoma di diritto, soggetta a una regolamentazione specifica e orientata alla prevenzione. Questo cambiamento segna il passaggio da una concezione puramente gestionale del rischio informatico a una sua piena "giuridicizzazione", con conseguente attribuzione di obblighi, responsabilità e standard organizzativi funzionali alla tutela di interessi primari.

Si tenterà, pertanto, di esaminare le caratteristiche innovative del nuovo quadro regolatorio europeo, che vede la sfida tecnologica collocarsi al centro della riflessione giuridica contemporanea.

A ciò si aggiunga che le entità finanziarie, bancarie e assicurative assumono un ruolo strategico e sistemico all'interno del mercato unico europeo, in quanto presidiano la stabilità dei mercati, la continuità dei flussi di pagamento, l'allocazione del credito e, più in generale, il funzionamento dell'economia reale. Di conseguenza, la loro resilienza operativa non assume rilievo esclusivamente in termini di microprudenza, ma si configura come condizione imprescindibile per la tutela della stabilità complessiva del sistema e per la salvaguardia di diritti fondamentali quali l'iniziativa economica, il risparmio e la protezione dei dati personali.

In tale contesto, gli attacchi informatici non rappresentano più eventi sporadici, ma fenomeni con il potenziale di generare effetti dirompenti, amplificati dall'elevata interconnessione tra operatori, infrastrutture e fornitori terzi di servizi digitali. La compromissione di sistemi critici può determinare conseguenze di vasta portata, tra cui interruzioni di servizi essenziali, perdite patrimoniali significative, erosione della fiducia degli investitori e dei risparmiatori, nonché ripercussioni sistemiche che possono incidere sull'ordine pubblico economico.

La cybersecurity nel settore finanziario, bancario e assicurativo assume, dunque, una rilevanza di interesse pubblico primario, richiedendo un approccio regolatorio integrato.

Quale corollario, il *Digital Operational Resilience Act*, c.d. Regolamento DORA, si configura come un modello di best practice per la gestione delle minacce informatiche derivanti dall'erogazione di servizi digitali nei settori sopracitati. L'approccio metodologico adottato ha saputo valorizzare i concetti di prevenzione, proattività, multidisciplinarietà, co-regolazione e responsabilità

multilivello, delineando un sistema organico di resilienza operativa digitale.

Più precisamente, l'analisi si concentrerà sull'esame dei presidi introdotti per garantire la sicurezza della *supply-chain*, concepiti come requisiti contrattuali minimi obbligatori ai fini della compliance normativa, da cui dipende la *cyber-resilience* delle entità finanziarie, bancarie e assicurative. È emerso che tali presidi anticipano il momento di tutela a partire dalla configurazione contrattuale del servizio esternalizzato nel quale la minaccia cyber potrebbe manifestarsi. L'obiettivo primario del legislatore europeo è stato quello di consolidare un presidio sistemico contro le minacce informatiche, trasformando la sicurezza digitale da mero requisito tecnico a componente strutturale della tutela dei diritti fondamentali nell'economia digitale.

L'implementazione di una strategia legislativa che eleva la cybersecurity a nuova pietra angolare dei mercati digitali evidenzia la trasformazione sostanziale che sta attraversando il diritto penale dell'informatica.

La presente indagine si prefigge di esaminare gli emergenti caratteri di cui la tecnica penalistica potrebbe avvalersi ai fini del contrasto delle forme di criminalità cibernetiche nell'era contemporanea.

Nell'arsenale del penalista, infatti, riveste particolare importanza l'introduzione di misure preventive e proattive, come la sicurezza informatica. Tuttavia, affinché quest'ultima possa dirsi pienamente efficace, è necessario avviare un dialogo intenso e costante con le discipline scientifiche e tecniche, anche extragiuridiche, che possono contribuire a gettare solide fondamenta per il diritto penale nell'epoca della sicurezza digitale.

2. Verso un nuovo paradigma preventivo-proattivo

Il diritto penale, inteso come strumento di repressione e concepito esclusivamente per l'uomo, risulta antiquato rispetto all'incessante avanzamento del progresso tecnologico. Tale branca dell'ordinamento si è storicamente sviluppata come un "diritto di reazione", intervenendo *ex post*, ovvero una volta che il fatto lesivo, anche in termini di messa in pericolo del bene giuridico protetto, si è verificato, con l'obiettivo di sanzionare e dissuadere dal ripetersi di comportamenti penalmente illeciti. Questo paradigma, che per secoli ha rappresentato

il fulcro della legalità sostanziale, mostra, tuttavia, i suoi limiti nel contesto digitale.

Negli ultimi anni il diritto penale è stato chiamato a confrontarsi con una mutazione strutturale della criminalità economica e tecnologica¹. Il cyberspazio², per sua natura transnazionale e decentralizzato, ha eroso i fondamenti del paradigma repressivo tradizionale, sovvertendone principi consolidati.

La sequenza tipica rappresentata da fatto, accertamento e sanzione, si è dimostrata progressivamente inadeguata di fronte a fenomeni che si manifestano in millisecondi e si estendono a diverse giurisdizioni. Ciò in quanto i cyber-attacchi e la manipolazione dei dati o dei sistemi algoritmici non seguono più le logiche spazio-temporali intrinseche alla condotta umana³. Peraltro, queste nuove forme di criminalità non possono definirsi nemmeno “bloodless”, atteso l’impatto che sono in grado di provocare sui destinatari quando la minaccia, originariamente limitata all’ambiente digitale, diviene fisica. Basti pensare all’attuale

contesto geopolitico, caratterizzato da una *escalation* di “guerre ibride diffuse”, nelle quali la maggior parte degli attacchi sono stati perpetrati non mediante l’impiego di armi convenzionali, ma attraverso l’uso di tecnologie innovative, potenzialmente letali per intere comunità⁴.

Dal punto di vista della tecnica penalistica, il fenomeno si inserisce in un universo radicalmente diverso da quello della criminalità non cyber, privo dei riferimenti spaziali e temporali su cui il diritto penale tradizionalmente si fonda⁵. Gli attacchi informatici si sviluppano nell’ordine dei millisecondi, attraversano più giurisdizioni e sono in grado di produrre effetti sistemici prima ancora di essere rilevabili.

La natura strutturalmente globale del cyberspazio influisce significativamente sulla configurazione della fattispecie incriminatrice. In merito, si evidenziano le difficoltà applicative che le categorie penalistiche classiche (*locus commissi delicti*⁶, azione, evento⁷ e bene giuridico tutelato⁸) incontrano laddove trasposte nel cyberspazio. Ciò nonostante,

1. Per un approfondimento a riguardo, si rinvia a CORASANTI 2025; per la letteratura straniera, cfr. PARKER 1974; MENELLY 1985. Circa le difficoltà definitorie del concetto di criminalità informatica, si rinvia, tra i tanti, a PECORELLA 2006.
2. Termine coniato da William Gibson nel 1986 nell’ambito della letteratura Cyberpunk. Per un approfondimento cfr. FLOR 2019-A; PIETROPAOLI 2019.
3. Per una disamina della materia si rinvia a CUOMO 2000; PADOVAN 2023; MORGANTE 2025.
4. Il primo caso di *cyberwarfare* risale all’attacco dell’Estonia del 2007, uno dei paesi al mondo maggiormente informatizzato, noto per la vicenda “*Il soldato di bronzo*”, in occasione del quale per la prima volta nella storia uno Stato membro della NATO ha richiesto l’attivazione dell’art. 5 del Trattato istitutivo dell’Alleanza Atlantica, a seguito di un attacco di natura cibernetica alle proprie infrastrutture digitali. Tuttavia, alla richiesta non venne dato seguito in quanto l’Estonia, pur fortemente danneggiata dai *cyberattacks*, non aveva subito vittime o distruzioni fisiche alle infrastrutture critiche e si ritenne di non poter ravvisare gli estremi dell’applicabilità della disposizione difettando il requisito “contro l’integrità territoriale di uno Stato”. A questo proposito, vedasi ATERNO 2022, pp. 215-217.
5. La questione dell’applicazione del diritto penale per sanzionare condotte perpetrate in ambito digitale è stata oggetto di approfondimento da parte di FIORINELLI 2024, p. 110 ss.
6. Questo profilo problematico è stato investigato in maniera significativa da CORONA 2021; ATERNO 2023. In talune circostanze, è stata adottata la “fisicizzazione” degli elementi del reato, collocando la condotta nel luogo dell’autore materiale e l’evento nel luogo della vittima, conferendo così materialità ad un reato virtuale. Per un approfondimento a riguardo vedasi CARREA 2017; FLOR 2019-B; RAZZANTE 2023.
7. L’elemento oggettivo del reato è stato esaminato in questi termini da PICOTTI 2000, p. 16 ss., CUOMO-IZZU 2002, p. 1018; CUOMO-RAZZANTE 2009; MATTARELLA 2022, p. 809.
8. La riflessione a riguardo è stata sviluppata da DONINI 2013, p. 6. In riferimento al concetto di imprescindibilità epistemologica del bene giuridico tutelato si rinvia a FLOR 2022, p. 145 che alla nota 38 rimanda a ROCCO 1913; PISAPIA 1948; PAGLIARO 1965; STELLA 1973; BETTIOL 1959; NEPPI MODONA 1965; BRICOLA 1973; MANTOVANI 1977; PULITANÒ 1981; VASSALLI 1982; FIANDACA 1982; ANGIONI 1983; STILE 1985; DONINI 2003; DONINI 1999.

tale regione continua a rivestire un'importanza strategica per gli Stati, in quanto ospita la maggior parte delle attività economiche, sociali e governative, nonché delle interazioni tra i Paesi⁹, di talché, “Il clic di un computer ha oggi un peso molto superiore al grilletto di una pistola”¹⁰.

È sufficiente considerare che, nell'anno 2025, in Italia, si è verificato un aumento significativo del numero di realtà aziendali che sono dovute ricorrere alla cassa integrazione per i propri dipendenti a causa di attacchi *ransomware* che hanno compromesso seriamente la produzione e la stabilità finanziaria aziendale, causandone talvolta il tracollo¹¹.

Quale conseguenza, nel contesto digitale, la prevenzione assume una rilevanza sistemica e sistematica, non limitandosi esclusivamente alla protezione dell'ormai unanimemente riconosciuto bene giuridico della “sicurezza informatica”¹², ma estendendosi alla costruzione di condizioni organizzative e tecnologiche che ne prevengono la compromissione o la messa in pericolo. All'interno dell'armamentario del penalista emerge la *cybersecurity*¹³, intesa sia come il processo che come il risultato di garantire la sicurezza nel cyberspazio. Tale misura precauzionale rappresenta il *nuovo volto della prevenzione penale*, che opera non solo su un piano individuale, ma anche su quello collettivo e collettivistico delle strutture e delle infrastrutture tecnologiche e organizzative la cui compromissione potrebbe arrecare pregiudizio a intere collettività.

A conferma di tale trasformazione concettuale, le nuove discipline di matrice europea estendono l'ambito applicativo delle regole di sicurezza

informatica agli assetti aziendali, alle infrastrutture tecniche, alle filiere di fornitura e, in generale, agli ecosistemi di dati. Per l'effetto, la *cybersecurity* contribuisce a delineare un livello di protezione anticipato rispetto al momento in cui si verifica l'effettiva lesione dell'integrità delle informazioni, dei programmi o dei sistemi informatici, al fine di tutelare l'affidabilità e la fiducia collettiva della sicurezza dei rapporti giuridici instaurati tramite l'uso di strumenti tecnologici e spazi virtuali¹⁴.

Ai fini della presente analisi, con il termine “sicurezza informatica” ci si riferirà alla sicurezza delle informazioni, ossia di dati organizzati e significativi¹⁵. La cruciale importanza dei dati deriva dalla loro natura dinamica e trasformativa: una volta elaborati e contestualizzati, i dati sono potenzialmente in grado di essere convertiti in informazioni¹⁶, che costituiscono risorse strategiche e gli asset più preziosi e ambiti dell'ecosistema contemporaneo, divenuti oggi il fulcro della competizione economica, oltre che il principale obiettivo e la nuova moneta di scambio della criminalità in ambiente informatico.

In tale prospettiva, la *cybersecurity* si configura come un nuovo paradigma di diritto preventivo-proattivo, che realizza un'ibridazione tra diritto penale, diritto amministrativo, regolazione economica e informatica, capace di affiancare alla punizione, la necessaria e non più procrastinabile costruzione di comportamenti organizzativi ottimali, la cui omissione determina l'applicabilità di sistemi di diritto punitivo settoriali, ossia, sanzioni amministrative, oltre che l'operatività delle ordinarie discipline penalistiche vigenti, ai sensi

9. Per ulteriori approfondimenti, si veda BUCKLAND-SCHREIER-WINKLER 2015, p. 7 ss.; MARTINO 2018, I, p. 69; RAMADHAN 2021, p. 161 ss.; SHARMA 2022, p. 50 ss.; e, in tema di *cyberdiplomacy*, FRACCHIOLLA 2022, pp. 463-484.

10. La citazione è tratta da MATTARELLA 2022, p. 44.

11. DI CUIA 2025; FADDA 2025.

12. Per un compiuto approfondimento della affermata autonomia del bene giuridico della sicurezza informatica rispetto ai beni giuridici tradizionali vedasi CUOMO 2000, PICOTTI 2011 p. 229 ss., MATTARELLA 2022, p. 813, che rinvia sul rapporto tra bene strumentale e finale, a FIORELLA 1987; CORONA 2023; FLOR 2023, p. 138; PADOVAN 2023, p. 13 ss.

13. Per un'analisi dei tentativi di concettualizzazione sistematica dell'espressione *cybersecurity* vedasi URGESSA 2020; FLOR 2023, p. 143; BLAŽIČ-BLAŽIČ 2024.

14. La riflessione sul punto è tratta da Flor 2023, pp. 139-141 al cui approfondimento si rinvia anche in riferimento alla concezione dell'area di intersezione fra dimensioni individuale e collettiva.

15. Per tale scelta semantica si rinvia ad ATERNO 2022, pp. 181-182.

16. CUOMO-RAZZANTE 2009, pp. 5-6.

del d.lgs. 231/2001 ovvero del combinato disposto degli artt. 110 e 40 cpv. c.p.¹⁷

Il diritto penale fornisce la *ratio*, l'idea di tutela anticipata, mentre il diritto europeo, di cui il *Digital Operational Resilience Act*¹⁸, che rappresenta un esempio virtuoso, ne costituisce la traduzione operativa. La sicurezza informatica non si limita più ad assumere le vesti di una misura di protezione tecnica, ma si configura come uno strumento di prevenzione normativa volto a mitigare *ex ante* i rischi sistemici associati alle nuove forme di criminalità informatica.

3. Dal rischio al diritto: la costruzione europea della resilienza operativa digitale

La risposta europea alla sfida della criminalità informatica si fonda su una *trasformazione concettuale*: dal rischio al diritto. L'opera legislativa delle istituzioni europee, che hanno assunto un ruolo pionieristico in materia¹⁹, non si è, infatti, limitata a gestire il rischio tecnologico, ma lo ha tradotto in

obblighi giuridici, vincoli di governance e responsabilità operative, mediante l'introduzione di discipline di stampo preventivo e proattivo implementate secondo un approccio pragmatico²⁰ e settoriale, e attraverso una metodologia multidisciplinare e multilivello, in linea con la strategia di *security-by-design*²¹ a lungo propugnata dalle istituzioni europee.

Il percorso ha avuto inizio con l'adozione del Regolamento generale sulla protezione dei dati (GDPR)²², che ha introdotto il principio di accountability, ponendo l'accento sulla responsabilità attiva e documentata dei soggetti obbligati. Successivamente, il *Cybersecurity Act*²³, le *Directive NIS*²⁴, il *Data Act*²⁵ e il *Digital Markets Act*²⁶ hanno contribuito a edificare un sistema multidimensionale in cui la resilienza operativa digitale è divenuta elemento strutturale del mercato unico europeo, non a caso invocato, ai sensi dell'art. 114 TFUE, quale base giuridica per l'adozione delle discipline appena citate. Il denominatore comune di tali normative è stato individuato nella volontà,

17. Cfr. PIVA 2022, p. 537.

18. Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, cui, d'ora in poi, ci si riferirà con "Regolamento DORA".

19. Il percorso del legislatore europeo ha avuto inizio nel 2013, con la *Strategia sulla Cybersicurezza*. Per una disamina più approfondita della questione si rinvia a GONZÁLEZ FUSTER-JASMONTAITE 2020, pp. 97-115.

20. Tale qualificazione si deve a FLOR 2019-A, p. 457.

21. Per ampliare ulteriormente l'analisi del concetto di *security-by-design* si rinvia a MARCIALIS 2023, p. 391, che evidenzia la necessità di progettare i sistemi informatici secondo una visione olistica e non soltanto frammentaria o di tipo modulare.

22. Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

23. Regolamento (UE) 2019/881 relativo all'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (regolamento sulla cibersicurezza).

24. Direttiva (Ue) 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione e Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

25. Regolamento (Ue) 2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

26. Regolamento (UE) n. 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contenibili nel settore digitale e che modifica le direttive (UE) m. 2019/1937 e (UE) n. 2020/1828 (Regolamento sui mercati digitali). Per un approfondimento sulla configurazione dei mercati digitali mediante una regolazione cooperativa e multi-partecipativa si veda LICASTRO 2025.

più o meno manifesta, di istituzionalizzare approcci trasversali di prevenzione digitale a protezione del mercato comune.

L'Unione europea si è proposta come un vero e proprio laboratorio giuridico per la regolazione del cyberspazio, promuovendo un approccio integrato che unisce il diritto dell'informatica, il diritto dei mercati e il diritto penale, ibridandolo al diritto amministrativo. Il concetto di "resilienza operativa digitale" è stato elevato a principio di governance, con una funzione paragonabile a quella della stabilità finanziaria. Si delinea un nuovo diritto della sicurezza informatica, che coinvolge istituzioni, imprese e individui in un sistema di co-regolazione e corresponsabilità multistakeholder.

Il legislatore europeo non si è limitato a imporre sanzioni *ex post*, ma ha definito un quadro preventivo in cui la resilienza digitale è divenuta un obbligo di conformità e un presupposto della legittimità operativa. L'innovazione si sostanzia nella formalizzazione giuridica del rischio tecnologico²⁷, che viene così classificato come una categoria di diritto: il rischio viene normato, valutato, comunicato e attribuito ad un responsabile. Tale cambiamento di prospettiva comporta che il rischio non è più inteso come un evento da eludere, ma, piuttosto, come un fattore da amministrare secondo principi giuridici e logiche aziendali.

Il diritto europeo ha adottato il linguaggio della prevenzione tecnica e lo ha trasformato in linguaggio di legalità, spostando l'asse della tutela penale: la lesione non è più esclusivamente l'attacco informatico o il danno economico, anche reputazionale, bensì l'omissione nella gestione del rischio, la mancanza di vigilanza, l'assenza di cultura organizzativa interna e esterna della sicurezza informatica.

La transizione "dal rischio al diritto" rappresenta il fondamento teorico per comprendere come DORA non si limiti a rivestire il ruolo di uno strumento di regolazione finanziaria, bancaria e assicurativa, ma si configuri come un modello di governance esportabile²⁸ a tutti i mercati digitali, in quanto la sua logica è in grado di estendersi oltre il suo ambito applicativo. La nuova tendenza è quella di accettare l'idea dell'estrema dinamicità dei mercati, oltre che la normatività della tecnologia di cui essi sono impregnati²⁹.

4. Il Digital Operational Resilience Act: una governance multidisciplinare e multilivello tra prevenzione, co-regolazione e responsabilità multistakeholder

Il Regolamento DORA, il cui obiettivo risiede nella salvaguardia della resilienza operativa digitale dei sistemi informatici a fronte di *cyber-attack*, introduce un *corpus* normativo che integra principi di gestione del rischio ICT e continuità operativa, delineando una governance che coinvolge le organizzazioni operanti nel settore finanziario, bancario e assicurativo, ma anche le relative Autorità garanti, nazionali³⁰ ed europee (EBA, ESMA, EIOPA), e i fornitori terzi di servizi ICT.

Con la sua emanazione, gli operatori sono stati chiamati a una continua propensione verso un miglioramento omnicomprensivo nella gestione della cybersecurity, che viene concepita come un mezzo precauzionale indefettibile nella moderna società delle reti. Nello specifico, la necessità dell'intervento regolatore è sorta dalla constatazione di una crescente dipendenza dei settori coinvolti dai processi digitali³¹.

27. Tale rischio ricomprende, a tutt'oggi, nella sua tassonomia, anche gli l'utilizzo di strumenti di intelligenza artificiale. Sull'interazione tra il Regolamento DORA e l'AI Act si rinvia a FARAONE 2024.

28. Questa via è stata anche indicata da MICHIELI 2024, cui si rinvia per una trattazione del Regolamento DORA.

29. Su tali aspetti si vedano le riflessioni di LESSIG 1999.

30. A livello italiano, le Autorità garanti sono state istituite dal d.lgs. n. 23/2025, che, all'art. 3, prevede la partecipazione al forum di sorveglianza di Banca d'Italia, Consob, Ivass e Covip, cui viene attribuita la qualifica di Autorità competenti per il rispetto degli obblighi posti dal Regolamento DORA a carico dei soggetti vigilati, secondo le rispettive attribuzioni di vigilanza, nonché per le segnalazioni di gravi incidenti informatici e per le segnalazioni volontarie di minacce informatiche significative.

31. I dati su cui si basa la riflessione sono stati tratti da ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA 2025. Sul punto, si rinvia anche alle opere di MICHIELI 2024; RAFFAELE 2024.

Primariamente, è d'obbligo sottolineare che il legislatore europeo ha optato per l'adozione del "più forte" degli atti di normazione secondaria a livello unionale, quello del regolamento, dotato per sua stessa natura del connotato della vincolatività e dell'efficacia *erga omnes*, in ragione dell'importanza del settore di intervento³². La suddetta scelta normativa riveste una notevole rilevanza all'interno del quadro regolatorio in esame, suggerendo una nuova direzione per la normazione europea, che sembra, sempre più spesso, muoversi verso l'abolizione del ricorso alle direttive e, al contrario, verso la concentrazione della tecnica legislativa sui regolamenti³³. Tale cambiamento di indirizzo potrebbe contribuire in modo significativo alla neutralizzazione della frammentazione dell'ordinamento eurolunitario, accrescendone l'efficacia e la capacità deterrente.

Le entità finanziarie³⁴, in considerazione del delicato *core business* di cui trattano e che costituisce, sempre più di sovente, il *quid* tanto desiderato dalla criminalità informatica, svolgono una funzione sociale che impatta tanto sulla macroeconomia, che interessa il sistema-Paese, quanto sulla microeconomia, la quale coinvolge, quotidianamente, ogni singolo risparmiatore³⁵. Pertanto, l'investimento in materia di protezione dei dati, dei sistemi e delle infrastrutture nel settore Fintech è un fattore determinante per la tutela della persona, oltre che del sistema economico nazionale e europeo³⁶. L'acquisita consapevolezza che il *cyber-risk* può rappresentare un rischio strutturale negli

attuali modelli di business e un rischio di potenziale impatto sistemico³⁷, non più relegabile alla sola sfera dei rischi operativi, si è tradotta nelle nuove norme comuni sulla resilienza operativa digitale, per tale intendendosi la capacità di costruire, assicurare e riesaminare l'integrità e l'affidabilità operativa dei sistemi, garantendo, direttamente, oppure indirettamente, anche tramite il ricorso a fornitori terzi, l'intera gamma delle capacità connesse alle ICT necessarie per garantire la sicurezza delle infrastrutture di rete.

La struttura del Regolamento DORA si fonda su cinque pilastri fondamentali³⁸: (i) *ICT risk management*, che richiede un'accurata identificazione, valutazione e mitigazione dei rischi ICT e impone agli istituti finanziari di istituire solidi quadri di governance e di controllo interni; (ii) *ICT Incident Management*, in forza del quale devono adottare un processo standardizzato per identificare, gestire e segnalare adeguatamente gli incidenti ICT significativi; (iii) *Digital Operational Resilience Testing*, che si sostanzia nell'esecuzione di test regolari della resilienza organizzativa per garantire la preparazione a un'ampia gamma di rischi ICT, inclusi programmi completi per identificare, affrontare e mitigare le vulnerabilità; (iv) *ICT Third Party Risk Management*, che sottolinea l'importanza di gestire con attenzione i rischi derivanti da partnership esterne e richiede di valutare, approfondire e mantenere solide relazioni contrattuali con le terze parti; (v) *Information Sharing* che incoraggia la condivisione di informazioni sulle minacce

32. In questi termini si è espresso BARBARA 2022, p. 508 cui si rinvia per un approfondimento della normativa europea analizzata.

33. Sulla medesima scia, si ritiene che si sia posta anche l'emanazione del Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

34. L'espressione "entità finanziarie" verrà utilizzata per indicare sinteticamente le organizzazioni dei tre diversi settori destinatari dell'applicazione del Regolamento DORA: bancario, finanziario e assicurativo. Per un approfondimento circa l'ambito applicativo del Regolamento vedasi PÉREZ-CARRILLO 2023; BUSCH 2024; MICIELI 2024.

35. Cfr. CHIOCCIO 2022.

36. Per un approfondimento si rinvia a GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2020.

37. A questo riguardo, si vedano i dati riportati da ANGELINI 2024, pp. 1-6; ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA 2025, p. 112.

38. Il tema della governance dei rischi contrattuali alla luce dell'emanazione del Regolamento DORA è stato trattato da SCHNEIDER 2022; GHIGNATTI 2024.

informatiche per promuovere la resilienza collettiva e, promuovendo una cultura di condivisione collaborativa, mira a migliorare la preparazione e le capacità di risposta complessive del settore.

Il Regolamento DORA non è stato concepito come una normativa autonoma e indipendente, ma piuttosto come il risultato di una strategia legislativa complessa³⁹, progettata secondo un approccio settoriale, partecipativo e multilivello. Tale strategia muove le mosse dalla tendenza – sempre più incalzante – ad affidare la gestione dei servizi digitali a fornitori esterni⁴⁰, per motivi che includono l'ottimizzazione dei costi e delle risorse, la focalizzazione sul *core business*, la considerazione dell'esperienza maturata dall'*outsourcer* e della garanzia delle prestazioni, il *reengineering* dei processi e la mitigazione dei rischi.

Tuttavia, i fornitori di servizi digitali rappresentano una delle principali vie attraverso le quali si diffondono le minacce informatiche. Quale corollario, avendo riguardo al management delle esternalizzazioni, sono stati introdotti numerosi obblighi contrattuali che richiedono il possesso di specifiche *technicalities*⁴¹, quali l'analisi e la gestione dei rischi, la realizzazione di stress test, l'attività di vigilanza, l'attenzione ai contenuti contrattuali e ai regimi di responsabilità, per equilibrare i rapporti di forza e di dipendenza tra i settori *Finance* e *ICT*, al fine di tutelare gli interessi degli investitori e del sistema europeo⁴².

La neonata normativa configura la cybersecurity come una responsabilità multi-stakeholder, che necessita di essere implementata in vari livelli di governo, economia e società, coinvolgendo personale, consigli di amministrazione e Autorità garanti. È stata prevista una stretta collaborazione tra tutti gli attori, pubblici e privati, che compongono la filiera della protezione dei nuovi interessi digitali, al fine di strutturare strategie trasversali di prevenzione dagli attacchi informatici.

È stata delineata una *regolazione partecipativa*, in cui al regolatore pubblico spetta definire la normativa che influenzerà la struttura del governo societario dell'ente privato, mediante la previsione di obblighi *ex ante*, e al regolato (le istituzioni finanziarie) il compito di integrarne il contenuto *by design* nell'architettura dei propri modelli di *outsourcing*, secondo una logica collaborativa costruita su un'intensa partnership pubblico-privata. In tale contesto, è stato osservato il ruolo attivo affidato alle Autorità garanti, sia a livello nazionale che europeo, che svolgono la funzione di sorveglianza del nuovo quadro normativo, al fine di supportare i regolatori nella formulazione di strategie di conformità efficaci che considerino gli obblighi *ex ante*. Tali obblighi rappresentano le nuove coordinate per il mercato digitale europeo. Il legislatore ha, pertanto, implementato un sistema di conformità cooperativa, basato sul dialogo tra regolati, regolatore e guardiani. Le istituzioni sono concepite come partner attivi nei meccanismi di regolazione economica e di contrasto alle forme di criminalità informatica che presentano un impatto sistemico⁴³.

Il passaggio graduale dalla gestione interna dei servizi digitali all'affidamento a soggetti terzi ha reso essenziale esercitare un controllo efficace sull'*accountability*⁴⁴ del fornitore. L'obiettivo è verificare l'adozione di comportamenti proattivi e di misure volte a garantire la corretta implementazione del quadro di resilienza operativa digitale. Più precisamente, nel settore della sicurezza informatica, l'*accountability* si manifesta nella capacità di dimostrare il rispetto degli obblighi previsti dalla normativa, anticipando potenziali eventi dannosi e prevedendo misure organizzative e tecniche adeguate a prevenire una serie ampia di rischi calcolati. Tale approccio metodologico include la gestione di situazioni critiche e l'identificazione di eventi

39. Cfr. la pagina del sito della Commissione europea sul *Digital Finance Package* del 2020.

40. Il tema della co-dipendenza tra settore finanziario e ICT e dei fenomeni rilevanti generati per il diritto dell'economia che hanno conferito al FinTech un'autonoma rilevanza di mercato è stato approfondito da PIGNATTI 2024, p. 649.

41. Si pensi, a titolo esemplificativo, ai requisiti stabiliti in riferimento ai livelli di servizio, ai *thread-lep-penetration tests* e alle *exit strategies* di cui all'art. 30, co. 2, del Regolamento DORA.

42. L'osservazione è tratta da PIGNATTI 2024, p. 653.

43. Per un approfondimento circa le origini storiche dell'istituto della funzione di compliance si veda MILLER 2014, p. 2.

44. Così, LORÈ-MUSACCHIO 2021.

rischiosi, con l'obiettivo di sviluppare risposte che garantiscano un margine di sicurezza concreto.

L'Europa ha adottato un approccio che considera l'accountability e la governance come elementi cruciali per la resilienza operativa digitale, promuovendo l'integrazione del principio della compliance nelle normative. La logica sottostante è analoga a quella che ha guidato la progettazione del già citato GDPR, ma anche dell'*AI Act* e del *Data Act*, normative che presentano una connessione diretta con la struttura dei processi di gestione dei dati, sia personali che non personali, e con i rapporti contrattuali instaurati con i fornitori. L'approccio delineato incorpora una strategia integrata, al fine di sviluppare un sistema di gestione delle terze parti nell'ambito della politica complessiva di neutralizzazione dei rischi sistemici ICT. Inoltre, il framework impone l'adozione di una nuova cultura aziendale, basata su un approccio non solo quantitativo, ma anche qualitativo, e rivolta non solo alle istituzioni finanziarie, ma anche ai fornitori.

Infatti, affinché si possa garantire un'effettiva e proficua conformità alla normativa, numerose prescrizioni impongono inediti e onerosi adempimenti in materia di cybersecurity che riguardano non solo l'organizzazione interna, ma anche quella esterna. In un contesto sempre più interconnesso⁴⁵, le attività finanziarie affidano all'esterno lo svolgimento di operazioni anche di cruciale rilevanza e la dipendenza che si crea tra l'entità e il fornitore può comportare vulnerabilità significative, soprattutto laddove il terzo non sia in grado di assicurare e di mantenere in modo stabile e continuativo standard di sicurezza informatica elevati e adeguati al contesto, spaziale, temporale e tecnologico, nel quale il servizio viene erogato.

Per comprendere meglio l'importanza e la crucialità della scelta normativa europea, è opportuno esaminare il comparto di disposizioni che impongono alle entità finanziarie, in sede di stipula dei contratti di fornitura di servizi ICT, di rispettare standard specifici per garantire che le clausole contrattuali siano conformi a un livello comune e che sia possibile monitorare adeguatamente le attività svolte dai fornitori. Il legislatore ha, quindi, ideato un regime *ad hoc* per la gestione dei rapporti con le terze parti, con l'obiettivo di rendere cyber resilienti i rischi derivanti dall'esternalizzazione, soprattutto se a supporto di funzioni essenziali o importanti⁴⁶. Ciò in quanto non è sufficiente che l'entità finanziaria sia resiliente, ma è indispensabile che lo siano anche i suoi fornitori.

4.1. Il regime di responsabilità in caso di violazione del Regolamento DORA

All'interno degli accordi di esternalizzazione, concepiti come strumento principe per la corretta ed equilibrata gestione della condizione di dipendenza del settore finanziario dai fornitori di servizi ICT, è necessario includere requisiti contrattuali specificamente individuati dal legislatore europeo, che consentono di monitorare i potenziali rischi e di mitigare gli effetti negativi derivanti dallo squilibrio di potere sopra descritto.

Per elaborare contratti di esternalizzazione cyber-resilienti, l'entità finanziaria dovrà muovere le mosse dalla consapevolezza delle minacce ICT cui è maggiormente esposta, attraverso l'analisi dei rischi, nota come *risk based approach*, che trae ispirazione dalle esperienze maturate in altri settori, come quello della responsabilità amministrativa delle persone giuridiche⁴⁷. Tale approccio

45. Anche su questo tema, si rinvia nuovamente all'opera di MICHIELI 2024; RAFFAELE 2024.

46. L'art. 3, paragrafo 1, punto 22) del Regolamento DORA definisce "funzione essenziale o importante" una funzione la cui interruzione comprometterebbe sostanzialmente i risultati finanziari di un'entità finanziaria o ancora la solidità o la continuità dei suoi servizi e delle sue attività. La medesima definizione si applica alla funzione la cui esecuzione interrotta, carente o insufficiente comprometterebbe sostanzialmente il costante adempimento, da parte dell'entità finanziaria, delle condizioni e degli obblighi inerenti alla sua autorizzazione o di altri obblighi previsti dalla normativa applicabile in materia di servizi finanziari.

47. Così come disciplinata dal decreto legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", che ha introdotto nell'ordinamento italiano il principio della responsabilità amministrativa degli enti per reati commessi nel loro interesse o vantaggio da amministratori, dirigenti o dipendenti. La suddetta normativa estende la responsabilità oltre la persona fisica e prevede sanzioni di natura pecuniaria, interdittiva e di confisca. Al fine di esonerare l'ente da tale responsabilità, si rende necessario implementare un Modello

si prefigge di ridurre l'asimmetria informativa tra le parti coinvolte⁴⁸, al fine di implementare i meccanismi e le misure organizzative e gestionali idonee a mitigare l'impatto di un rischio informatico sull'attività finanziaria. Risulta peculiare come tali rischi e opportunità risiedano al di fuori dell'ambito finanziario, richiedendo professionalità e competenze specifiche per la loro efficace gestione⁴⁹.

Quanto alle responsabilità in caso di violazione della normativa, il sistema sanzionatorio disegnato dal legislatore europeo si applica esclusivamente alle entità finanziarie, nello specifico all'organo di gestione⁵⁰. Ai sensi del Regolamento DORA, il fornitore terzo incorrerà soltanto nelle responsabilità di natura contrattuale derivanti dal contratto di esternalizzazione stipulato con l'entità finanziaria⁵¹. Ciò implica che il consiglio di amministrazione sarà responsabile non solo delle procedure e dei quadri interni e del modo in cui sono stati predisposti, ma anche della sicurezza e dell'adeguatezza dei presidi elaborati dalla società terza incaricata della gestione delle informazioni e dei dati sensibili oggetto del servizio esternalizzato.

La limitazione della responsabilità alle sole entità finanziarie e non anche ai fornitori, appariva, tuttavia, eccessivamente gravosa e, finanche,

violativa del principio di proporzionalità a cui la nuova legislazione dichiarava espressamente di ispirarsi⁵². Ciò in ragione del fatto che spesso queste organizzazioni faticano a rivestire un ruolo da protagoniste nella negoziazione delle clausole dei contratti di *outsourcing* che, nella maggior parte dei casi, fanno capo a contratti standardizzati, predisposti unilateralmente da parte del fornitore e senza possibilità di modifica.

Per tale ragione, nel periodo di *vacatio* tra l'emanazione del Regolamento DORA e la sua entrata in vigore (avvenuta il 17 gennaio 2025, fatta eccezione per gli intermediari finanziari *ex art.* 106 TUB, per i quali ne è stata posticipata l'entrata in vigore di due anni⁵³), i fornitori, non essendo soggetti a sanzioni in caso di mancata ottemperanza, non hanno mostrato disponibilità a uniformare le proprie scritture contrattuali alla nuova legislazione europea. Era, quindi, previsto un meccanismo simile a quello vigente in materia di privacy: il rispetto degli adempimenti rilevanti restava in capo all'ente finanziario e non gravava direttamente sul fornitore.

Un rilevante cambio di scenario si è avuto soltanto con il d.lgs. n. 23 del 10 marzo 2025⁵⁴, che, in adeguamento al Regolamento DORA, ha esteso l'ambito applicativo delle sanzioni anche ai fornitori

Organizzativo, di Gestione e Controllo (MOGC) idoneo a prevenire i reati presupposto, sottoposto ad un Organismo di Vigilanza (OdV).

48. Più in generale, sul tema delle asimmetrie di potere esistenti tra banche e fornitori di servizi tecnologici, si rinvia a CARDANI-GIRARDI 2024.

49. Così, PIGNATTI 2024, p. 654 cui si rinvia per la disamina della diversa natura dei rischi connessi alla sicurezza informatica.

50. La responsabilità dell'organo di gestione costituisce il principio guida, in quanto gravato dalla valutazione dell'adeguatezza delle clausole contrattuali che disciplinano i rapporti con i fornitori di servizi ICT ai sensi dell'art. 5, par. II, del Regolamento DORA.

51. I risvolti di tale quadro normativo sono stati analizzati da PIGNATTI 2024.

52. Cfr. art. 8 Regolamento DORA.

53. Ciò è quanto è stato previsto dall'art. 17 del Decreto legislativo 10 marzo 2025, n. 23, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, e per il recepimento della direttiva (UE) 2022/2556, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario", in forza del quale il decreto entra in vigore il giorno successivo a quello della sua pubblicazione, salvo per gli intermediari finanziari cui è dedicato l'art. 6, commi 1 e 2, del decreto, per i quali la normativa si applica a decorrere dal 1° gennaio 2027.

54. Il d.lgs. n. 23/2025 si caratterizza per un'ampia estensione dell'ambito di applicazione del Regolamento DORA: la nuova normativa riguarda i soggetti che operano come intermediari finanziari, ossia Bancoposta S.p.A., Cassa

di servizi ICT, che, a seconda della tipologia di soggetto al quale erogano i propri servizi, sono soggetti a regimi sanzionatori diversi. Più nello specifico, le sanzioni sono applicabili tanto nei confronti delle persone giuridiche (le condotte più gravi sono sanzionate da 30.000 € al 10% del fatturato; quelle meno gravi da 30.000 €, con un massimo editale del 7%), quanto nei confronti delle persone fisiche che svolgono funzioni di amministrazione, direzione o controllo, e che possono venire colpite anche dalla sanzione amministrativa accessoria dell'interdizione⁵⁵. Inoltre, l'attenzione e la responsabilizzazione degli organi di vertice evidenziano la strategicità del rischio cyber, che non può essere più considerato una tematica esclusivamente tecnica, ma deve permeare l'intera attività del Consiglio, grazie all'*induction* dei consiglieri di amministrazione e dei componenti degli organi amministrativi, che devono possedere competenze sempre più avanzate in governance della cybersecurity.

In tal modo, il legislatore italiano ha ulteriormente implementato il carattere multilivello e multi-responsabilità di questa normativa di settore, introducendo logiche di diritto punitivo mediante la creazione di un sistema sanzionatorio estremamente oneroso in caso di mancata conformità.

4.2. I presidi a tutela della sicurezza informatica della supply-chain

L'articolo 30, paragrafo 2, del Regolamento DORA stabilisce una serie di criteri guida applicabili a

tutto il ciclo di vita dell'accordo commerciale, che includono le fasi di conclusione, di esecuzione, di cessazione e anche il periodo post-contrattuale⁵⁶. La disposizione in esame stabilisce, altresì, un repertorio di standard minimi, al fine di armonizzare le condizioni di fornitura dei servizi ICT nel mercato europeo.

Tra i requisiti che incidono maggiormente sulla capacità dell'organizzazione di garantire la propria sicurezza informatica, si menziona, in primo luogo, quello di cui alla lettera e), che, nell'ottica di implementare i presidi a fronte di *cyber-risk*, prevede specifiche previsioni in riferimento ai livelli di servizio, ossia la metrica del servizio che il fornitore si impegna a rispettare. L'obiettivo è quello di misurare la qualità del servizio erogato, definendo il livello qualitativo standard garantito, a cui vengono associati parametri oggettivi per monitorarne il rispetto. Questi parametri, noti come *Key Performance Indicators* (KPI), comunemente vengono valutati attraverso strumenti e software dedicati, nonché algoritmi di calcolo. A titolo esemplificativo, per l'ipotesi di erogazione di un servizio di data center, gli indicatori chiave di qualità del servizio possono essere distinti in quattro categorie: la disponibilità, la reattività a un input, il rispetto dei tempi di reportistica e la performance.

Corre l'obbligo di evidenziare che, seppure i contratti in esame rientrano, nella maggior parte dei casi, nella categoria dei contratti di durata, essi sono soggetti a una rapida obsolescenza tecnologica⁵⁷, con la conseguenza che si rende necessario

depositi e prestiti e gli intermediari finanziari di cui al TUB, con la specificazione che Banca d'Italia può individuare una categoria di intermediari da considerarsi significativi anche per tipologia di attività svolte e a cui applicare il management framework completo in luogo di quello semplificato. La normativa ha introdotto forme mirate di accordo informativo tra le Autorità competenti DORA e la Guardia di Finanza. Tale intervento è strettamente legato al fatto che gli incidenti che hanno un impatto su reti, sistemi informativi e servizi informativi inerenti al settore finanziario possono derivare da attacchi esterni compiuti da soggetti non interessati soltanto a testare la vulnerabilità dei livelli di sicurezza, bensì anche ad acquisire la disponibilità di dati ed elementi informativi di carattere strategico in grado di minare gli interessi economico-finanziari del Paese e suscettibili di essere sfruttati per fini illeciti, *in primis* nel settore dei mercati finanziari, immobiliari, nonché in quello fiscale, doganale, della spesa pubblica e in materia di valuta, titoli, valori e mezzi di pagamento. Per tale ragione, è stato previsto il coinvolgimento della Guardia di Finanza, istituzione cui è normativamente riconosciuta la competenza per la ricerca, la prevenzione e il contrasto degli illeciti economico-finanziari perpetrati sfruttando i mezzi tecnologico-informatici.

55. Cfr. art. 10 d.lgs. n. 23/2025. Queste sanzioni non sono assicurabili con polizze e rendono tale disciplina sensibilmente diversa rispetto a quella prevista dalla Direttiva NIS II e recepita in Italia con il d. lgs. n. 138 del 2024.

56. La materia è stata ampiamente tratta anche da PÉREZ CARRILLO 2023, p. 1151.

57. In questi termini si sono espressi PORTOLANO–MAZZA 2023.

che i fornitori positivizzano all'interno delle scritture contrattuali il grado di evoluzione informatica che sono in grado di raggiungere con le proprie infrastrutture e con i propri servizi informatici e il cui rispetto si impegnano a garantire mediante la stipula.

Il service provider è tenuto a descrivere puntualmente i livelli di servizio, che si traducono nell'assunzione di obbligazioni, attraverso l'accordo su standard tecnici e qualitativi, metriche di performance attese, penali e modalità di monitoraggio e *reporting*. Questo aspetto è particolarmente rilevante nel contesto della *supply chain*, dove il livello di servizio è un indicatore chiave della probabilità di evitarne una carenza e della capacità dell'entità finanziaria di soddisfare le richieste e le aspettative dei clienti.

In aggiunta, è necessario che il fornitore, considerata la velocità dell'innovazione tecnologica, si impegni a prevedere e effettuare processi periodici di revisione e aggiornamento degli SLAs, allo scopo di neutralizzare, quanto possibile, il pericolo che i servizi prestati si rivelino obsoleti, così ponendo in serio pericolo la *business continuity* dell'entità finanziaria.

Estremamente rilevante appare anche la previsione di cui alla lettera f), che impone di prevedere, in sede contrattuale, la prestazione di assistenza senza costi aggiuntivi ovvero ad un costo stabilito *ex ante* qualora si verifichi un incidente connesso al servizio ICT prestato. Il verificarsi di un incidente informatico costituisce uno degli scenari peggiori ai quali l'entità finanziaria può andare incontro e al ricorrere del quale risulta di cruciale rilevanza il ruolo e la collaborazione prestata dal fornitore che eroga e gestisce, altresì in termini di manutenzione, il servizio oggetto di minaccia. Al fine di garantire la massima tempestività nell'intervento, il fornitore dovrebbe predeterminare il costo dell'assistenza che si impegna a garantire, secondo condizioni economiche definite già in sede contrattuale. Il profilo della predeterminazione dei costi consente di intervenire con prontezza e, in tali casistiche, la rapidità della risposta può permettere una ristrutturazione del servizio tanto più proficua e sicura. Considerata la difficoltà di prevedere *ex ante* tutti i possibili casi di incidente ICT e i rimedi necessari per ciascuno di essi, sarebbe opportuno che il

fornitore prevedesse, in sede contrattuale, esemplificazioni, da ritenersi non esaustive. Il contratto di fornitura potrebbe stabilire specifiche procedure di intervento in ordine ad ogni potenziale *cyber attack*, in riferimento a ciascuna sezione di funzionamento del servizio e assetti incentrati sul calcolo dei "giorni uomo", ovvero delle "ore uomo", richiesti per la gestione e l'efficace e tempestiva risoluzione dell'incidente di sicurezza informatica. L'entità finanziaria dovrebbe, quindi, verificare la completa e esaustiva predisposizione di un impianto contrattuale avente a oggetto le procedure e le tempistiche che devono essere osservate, i soggetti che gestiscono le comunicazioni e quelli che forniranno concretamente supporto ai fini del ripristino dei sistemi interessati dall'incidente.

Ulteriori e viepiù pregnanti obblighi sono poi previsti dall'articolo 30, paragrafo 3, in relazione ai fornitori di funzioni essenziali ovvero importanti. L'incidenza di tali attività sui risultati finanziari e sulla solidità e continuità dei servizi giustifica, secondo il legislatore europeo, l'introduzione di un regime "aggravato" che impone previsioni volte a rafforzare i vincoli contrattuali⁵⁸. La legislazione eurounitaria ha implementato standard minimi inerenti la descrizione dettagliata dei livelli di servizio, e, nello specifico, ha imposto, in sede contrattuale, l'esauritiva indicazione degli obiettivi quantitativi e qualitativi perseguiti, affinché l'entità finanziaria possa svolgere un proficuo monitoraggio, altresì, in termini di applicazione di misure correttive per il caso di violazione da parte del fornitore degli SLAs concordati. Inoltre, il fornitore dovrebbe essere tenuto contrattualmente ad impegnarsi a comunicare all'entità finanziaria, entro un congruo termine, l'implementazione di sviluppi tecnici, informatici ovvero tecnologici all'erogazione del servizio che potrebbero alterarne, ovvero comprometterne, la stabilità, oppure la sicurezza dei prodotti o del servizio erogato, e, non da ultimo, il soddisfacimento dei livelli di servizio assicurati.

Al fine di salvaguardare la sicurezza informatica delle ICT, il fornitore FEI dovrebbe impegnarsi a partecipare allo svolgimento del *threat-led-penetration-test*, per tale intendendosi un quadro informatico in grado di imitare le tecniche e le procedure di attori reali che generano minacce e che vengono percepiti come una minaccia autentica.

58. Così PIGNATTI 2024, p. 663.

Tale test consente di eseguire una verifica in ordine ai sistemi di produzione attivi e critici, in maniera controllata, mirata e basata sull'analisi della vulnerabilità, con l'obiettivo di esaminare le capacità difensive e migliorarle. Attraverso tali test, un attacco cyber non viene semplicemente simulato, bensì realmente realizzato per mettere alla prova la tenuta del sistema di sicurezza apprestato. I risultati del test, che deve essere effettuato ogni tre anni, vengono utilizzati per determinare le misure correttive volte ad implementare la *cyber-resilience* dell'entità finanziaria.

Infine, il contratto di fornitura di servizi FEI dovrebbe prevedere una disciplina stringente in punto di risoluzione contrattuale, mediante la predisposizione esaustiva di strategie di uscita, che rispondono alla finalità di proceduralizzare dei periodi di transizione obbligatori, durante i quali il fornitore deve continuare a prestare i propri servizi, allo scopo di ridurre il rischio di perturbazioni in capo all'entità finanziaria. L'obiettivo è, dunque, quello di consentire all'organizzazione di superare l'attacco in modo contenuto e senza inconvenienti, mediante l'utilizzo di altri fornitori ovvero, in alternativa, l'adozione di soluzioni interne, in funzione della complessità del servizio. Analogamente a quanto detto in riferimento agli SLAs, anche le strategie di uscita dovrebbero tenere conto dei rischi che la risoluzione del contratto di esternalizzazione potrebbe determinare nella *business continuity* aziendale, anche a causa di possibili disfunzioni dei fornitori, ovvero del deterioramento della qualità dei servizi in considerazione dei rischi di indisponibilità, del degrado dei livelli di servizio, dei cambiamenti rilevanti sulla fornitura sino alla risoluzione del contratto. A titolo esemplificativo, dovrebbero essere contemplate ipotesi di perturbazione dell'attività commerciale conseguente a una fornitura inadeguata o carente, oppure di gravi rischi connessi all'adeguatezza e alla continuità del servizio. I piani preventivi di uscita sono volti a consentire all'intermediario di esercitare la risoluzione senza arrecare disagio, ovvero sconvolgimento alcuno, alle proprie attività commerciali e in assenza di impatti sul rispetto dei requisiti normativi e all'operatività della *supply chain*, ivi compresa la qualità dei servizi forniti ai

clienti finali. Infine, le *exit strategies* dovrebbero essere documentate accuratamente e sottoposte a test periodici che ne garantiscano la revisione e l'aggiornamento, al fine di garantire una piena e quanto più attenta conformità allo sviluppo tecnologico raggiunto sia dall'entità finanziaria sia dal fornitore. I piani di uscita dovrebbero essere realistici, fattibili e basati su scenari plausibili, oltre che prevedere un calendario di attuazione compatibile con le condizioni stabilite negli accordi contrattuali.

L'obiettivo finale consiste nel consentire all'entità finanziaria di identificare prontamente eventuali disfunzioni potenziali dei fornitori, nonché eventuali deterioramenti della qualità dei servizi e perturbazioni. Questo al fine di attivare meccanismi che consentano la risoluzione delle problematiche senza arrecare pregiudizio alla compliance, alla continuità e alla qualità dell'attività commerciale.

4.3. L'impatto del Regolamento DORA sulla prassi contrattuale attuale

In un contesto caratterizzato da una certa difficoltà degli operatori finanziari nell'imporre ai fornitori l'adozione di clausole contrattuali specifiche, assumono rilevanza gli obblighi che il quadro giuridico vigente impone alle entità finanziarie e ai fornitori. Questi ultimi, infatti, in sede di implementazione italiana del Regolamento DORA, sono divenuti anch'essi destinatari dell'oneroso quadro sanzionatorio previsto in caso di mancata conformità alla normativa. Un'attenta analisi ha messo in luce come gli obblighi in questione contribuiscano, seppur indirettamente, a garantire agli operatori finanziari una posizione di forza nelle trattative con il settore ICT, mitigando il rischio di svantaggio. In considerazione del quadro delineato, gli elementi standardizzati possono costituire un utile strumento per contrastare comportamenti opportunistici da parte dei fornitori. Tuttavia, non si può trascurare il fatto che le aziende ICT, oltre alla fase di conclusione dei contratti, sono in grado di esercitare un'influenza significativa anche sull'effettiva e corretta esecuzione delle prestazioni, poiché detengono un *know-how*, nella maggior parte dei casi esclusivo, proprio in tale ambito⁵⁹.

59. Il tema dello squilibrio delle competenze *tech* dell'organo di gestione nell'ambito di applicazione della normativa DORA è stato affrontato anche da ALFANO 2024.

Le Autorità nazionali ed europee, nell'esercizio delle loro funzioni di vigilanza sulla gestione dei rischi e sull'attività contrattuale con i fornitori, svolgono un ruolo fondamentale di strumenti istituzionali di garanzia, mitigando le asimmetrie informative e promuovendo la tutela del risparmio. In merito, mentre la vigilanza interna garantisce un livello minimo di autonomia tecnica dell'operatore rispetto ai fornitori di servizi ICT, la vigilanza esterna rende i fornitori, generalmente non esercenti direttamente attività finanziarie in senso stretto, soggetti, invece, alla vigilanza delle Autorità garanti dei settori finanziario, bancario e assicurativo, soggiacendo così alla disciplina specifica di settore. Il quadro così delineato riveste una particolare rilevanza, promuovendo la cooperazione e il coordinamento delle attività delle Autorità attraverso una rete comune, fattore determinante per la stabilità del mercato europeo⁶⁰.

Dal punto di vista dell'operatore, la disparità di potere contrattuale rispetto al fornitore ICT si traduce nella corrispondente esigenza di possedere competenze tecniche adeguate, anche attraverso il rafforzamento del ruolo della vigilanza interna, che si estende alla gestione dell'evoluzione tecnologica dei servizi esternalizzati⁶¹. È evidente, infatti, l'elevato grado di sofisticazione che ispira la disciplina europea, che è stata in grado di coniugare due discipline a tutt'oggi strettamente interdipendenti: il diritto e l'informatica. Come evidenziato dall'analisi dei requisiti contrattuali, il legislatore ha operato un'attenta integrazione di regole tecniche e regole giuridiche⁶², conseguendo un equilibrio armonioso tra i due settori. Tuttavia, a fronte della commistione nella progettazione della disciplina di tali saperi, si rende necessario

che l'implementazione sia affidata a persone, sia fisiche che giuridiche, che possiedono la competenza necessaria per gestire ambedue i volti della nuova legislazione, al fine di garantire il rispetto e la piena valorizzazione di entrambi i caratteri della normativa.

Con l'intento di intervenire sui fragili equilibri di autonomia privata, il Regolamento DORA propone un nuovo paradigma di gestione integrata dei rischi cibernetici, in sinergia con le altre voci di rischio rilevanti, introducendo un nuovo modello di *best practice* per le modalità e i contenuti con cui ha intercettato un ambito di rischio del mercato finanziario in evoluzione esponenziale.

La nuova regolamentazione ha, inoltre, coinvolto tutti gli stakeholders nel processo di implementazione, mediante l'elaborazione di un insieme di norme che partono da principi generali e giungono sino a quelli più tecnici di cui agli RTS e agli ITS⁶³, mantenendo la flessibilità di individuare il punto di equilibrio tra il principio di proporzionalità e la gestione della complessità.

L'obiettivo principale è stato attribuire alle entità finanziarie un ruolo proattivo e propositivo nella governance della *supply chain*, al fine di garantire che l'esternalizzazione venga progettata e formalizzata attraverso tavoli negoziali di proficuo dialogo tra le parti interessate, in grado di considerare le reciproche esigenze e consolidare una partnership produttiva e duratura con il fornitore, che riveste un ruolo di estrema rilevanza nell'assicurare la resilienza operativa digitale dell'organizzazione.

60. Per un approfondimento in relazione alla figura dei fornitori critici, vedasi PIGNATTI 2024, pp. 663-664.

61. La riflessione che si condivide è stata tratta da PIGNATTI 2024, pp. 666-667.

62. Sul concetto di comprensione della regola tecnologica ai fini di una corretta interpretazione delle fattispecie legali si rinvia a FLOR 2022, p. 143.

63. I regolamenti RTS e ITS rappresentano norme tecniche di dettaglio sviluppate dalle Autorità europee di vigilanza (EBA, ESMA, EIOPA) per specificare come applicare concretamente i requisiti di resilienza operativa digitale. Gli RTS (*Regulatory Technical Standards*) prevedono i criteri per la classificazione degli incidenti gravi, i requisiti per la gestione dei rischi ICT e le politiche di sicurezza per i fornitori terzi critici. Gli ITS (*Implementing Technical Standards*) forniscono modelli uniformi, formati e procedure per la segnalazione degli incidenti e la tenuta del registro delle informazioni sui contratti ICT. Di seguito i riferimenti: Regolamento delegato UE 2024/1772, Regolamento delegato (UE) 2024/1773, Regolamento delegato (UE) 2024/1774, Regolamento di esecuzione (UE) 2024/2956, Regolamento Delegato (UE) 2025/301, Regolamento di esecuzione (UE) 2025/302, Regolamento Delegato (UE) 2025/532, Regolamento delegato (UE) 2025/420.

5. Il Regolamento DORA come modello di best practice e la cybersecurity come nuova architettura normativa dei mercati digitali

La prospettiva delineata suggerisce che il Regolamento DORA ha contribuito a istituzionalizzare la responsabilità preventiva delle organizzazioni economiche coinvolte, affiancando alla sanzione postuma una *cyber-compliance* dinamica, che prevede l'obbligo di anticipare, gestire e condividere il rischio informatico con tutti i soggetti che compongono la catena di erogazione del servizio, da quelli privati alle Autorità garanti.

In quest'ottica, la normativa europea può ritenersi convogliare nel novero di quei modelli di co-regolazione⁶⁴ che si caratterizzano per l'adozione di forme di *responsive regulation*, note per reagire ai fallimenti e alle inefficienze dei mercati mediante la promozione di strategie di governance aziendali da attuarsi mediante la delega normativa delle funzioni di regolamentazione alle persone giuridiche private, seppur sotto il controllo rigoroso delle Autorità pubbliche deleganti⁶⁵.

L'architettura DORA, fondata su un paradigma virtuoso, configura un sistema regolatorio binario: preventivo-proattivo nella struttura, attraverso la regolamentazione preventiva dei processi e la gestione cautelativa dei rischi, e punitivo nella reazione, mediante la previsione di sanzioni economiche e interdittive di notevole entità. Il legislatore europeo, mediante la previsione di obblighi di conformità normativa in materia di cybersecurity, mira a neutralizzare le forme di criminalità informatica in una prospettiva *ex ante*, ovvero, sin dal momento della configurazione contrattuale del servizio attraverso il quale la minaccia si potrebbe introdurre. In linea con la necessaria anticipazione del momento di tutela nell'ambiente digitale, il congegnato meccanismo preventivo richiede la

partecipazione attiva e fattiva delle entità private, anche in termini di cooperazione con le Autorità garanti. In assenza, troverà applicazione un sistema sanzionatorio basato su logiche di diritto punitivo.

Il legislatore ha adottato un approccio omnicomprensivo e poliedrico al fenomeno della criminalità informatica, sviluppando strategie trasversali di carattere multilivello. In primo luogo, l'attenzione è stata focalizzata sulle potenzialità degli strumenti precauzionali in grado di prevenire il *cybercrime*, a partire dalla sicurezza informatica, che emerge come la nuova architettura normativa dei mercati digitali. In tale contesto, le entità private sono soggette a un duplice livello di attenzione: il sistema europeo le considera come attori chiave del sistema preventivo, che supporta il sistema di stampo repressivo, variamente implementato in forza della potestà legislativa diretta conferita dall'art. 83 TFUE⁶⁶.

La dimensione penalistica della regolamentazione assume una rilevanza sistematica: l'*accountability* organizzativa si collega concettualmente con la colpa per omessa vigilanza, figura cardine del diritto penale dell'economia. Il Regolamento DORA, nel delineare un sistema di responsabilità proattiva degli operatori finanziari, concepisce l'*accountability* come un parametro di diligenza qualificata, la cui violazione integra non soltanto un deficit di compliance regolamentare, ma può fungere da indice sintomatico di colpa ai fini della responsabilità penale personale del management e di quella para-penale dell'ente. Difatti, i reati informatici, ai sensi degli artt. 24 e 24-*bis* del D.lgs. 231/2001, sono reati presupposto della responsabilità amministrativa degli enti⁶⁷ e parimenti deve dirsi per il trattamento illecito di dati in violazione del Regolamento UE 679/2016 (GDPR), che definisce la "violazione dei dati personali" una "violazione di sicurezza"⁶⁸, cui segue la necessità di un raccordo

64. Questa definizione di co-regolazione è richiamata da LICASTRO 2025, p. 95 che rinvia a riguardo a BLACK 2001, p. 117.

65. Per una disamina in materia di *responsive regulation* cfr. AYRES-BRAITHWAITE 1992, p. 4.

66. Per un approfondimento sugli obblighi di penalizzazione europei vedasi VADALÀ 2025, pp. 103-175.

67. In particolare, dopo l'introduzione dell'articolo 24-*bis*, che ha esteso il catalogo dei reati presupposto per includere varie fattispecie di *cybercrime*, come l'accesso abusivo, il danneggiamento di sistemi informatici, e le frodi informatiche, in seguito alla ratifica della Convenzione di Budapest sulla criminalità informatica con la legge 48/2008. Per questi profili cfr. PIVA 2022, p. 525 ss.

68. Basti pensare che rispetto agli adempimenti imposti dal GDPR, la *cybersecurity* costituisce un "presidio comune", così ROMOLOTTI 2019.

tra la prevenzione da attacchi a danno dell'impresa e quella avente ad oggetto, ai sensi dell'art. 5 del d.lgs. 231/2001, reati informatici commessi anche o soltanto nel suo interesse o vantaggio⁶⁹. Siamo di fronte all'ennesimo banco di prova della governance aziendale, che può comportare persino una responsabilità penale e a titolo di concorso per omesso impedimento dell'evento ex artt. 110 e 40 cpv. c.p. Ciò in quanto, il principio di "digital due diligence", che permea la normativa europea sulla resilienza operativa, si traduce in un nuovo standard di colpa specifica, in grado di ridefinire i confini della colpevolezza omissiva nell'epoca della digitalizzazione. La creazione di un sistema di governance efficace non garantisce esclusivamente un vantaggio competitivo, ma implica anche l'assunzione di un impegno organizzativo rigoroso e la mancata ottemperanza, indipendentemente dagli obblighi settoriali sanzionati amministrativamente o penalmente, può comportare responsabilità di natura apicale, in quanto la protezione dei dati è diventata una condizione imprescindibile per la stessa sopravvivenza⁷⁰ dell'entità finanziaria.

In tale prospettiva, la cybersecurity si configura come l'architettura normativa della legalità economica e digitale europea: essa non può più essere considerata esclusivamente come un requisito tecnico, ma piuttosto come un bene giuridico collettivo di nuova generazione⁷¹, la cui tutela è garantita sia dal diritto penale che dal diritto della concorrenza. Viepiù, essa dovrebbe costituire il parametro razionale per l'orientamento delle scelte di politica criminale, valorizzando la sua qualifica di *comprehensive concept*, "sostanziale" e "prepositivo", edificato su un triplice livello: infrastrutture, informazioni e tutela dei dati personali⁷². Soltanto tale accezione può essere in grado di guidare in maniera coerente e sistematica l'attività del legislatore. Una concezione che ne riconosca la natura composita e trasversale consente, infatti, di ancorare le scelte legislative a una lettura sostanziale e non meramente formalistica dei beni giuridici, sottraendoli a mere contingenze emergenziali

o a pressioni tecnocratiche. Non vi è dubbio che, al fine di contrastare efficacemente la criminalità informatica, è necessario dotarsi di strumenti tecnologici avanzati; tuttavia, questi non possono essere impiegati in modo tecnocratico.

Ne consegue che la sicurezza informatica emerge come un ambito di pertinenza per la costruzione di interventi normativi proporzionati, razionali e orientati alla tutela effettiva dei diritti fondamentali⁷³, contribuendo a edificare un diritto penale della sicurezza digitale che sia al contempo efficace e garantista. Tale traguardo rappresenta, a sua volta, un presupposto fondamentale per l'architettura del sistema di giustizia penale nell'era digitale.

In conclusione, il modello DORA assume una configurazione circolare e non può essere considerato esclusivamente una disciplina settoriale, ma fornisce una grammatica giuridica comune che utilizza il linguaggio della resilienza e della cooperazione per la governance dei mercati digitali. La grammatica delineata si fonda su cinque concetti chiave: accountability, testing, auditing, reporting e vigilanza coordinata.

La sua esportabilità si radica nella capacità di promuovere l'interoperabilità e la fiducia tecnologica tra gli operatori economici e di diffondere la cultura della prevenzione e della cyber-resilienza come criterio di legittimazione dell'attività economica digitale.

La sfida che si potrebbe prospettare è quella di estendere tale paradigma a tutti i mercati digitali, al fine di garantire che il principio di resilienza operativa digitale venga pienamente riconosciuto come la nuova misura della legalità tecnologica.

In tale contesto, il giurista non può limitarsi a una mera interpretazione della norma, ma è chiamato a contribuire alla costruzione di una cultura della sicurezza informatica condivisa, in cui il diritto diventa il linguaggio della fiducia tecnologica. Tale trasformazione sembra indicare l'emergere di una nuova metodologia, strettamente legata al concetto di "diritto penale della sicurezza digitale", volta alla costruzione di un sistema normativo

69. In tema, RAZZANTE 2022, p. 34 ss.

70. In materia di obblighi di agire informato dei soggetti apicali cfr. MONGILLO 2022, p. 2.

71. In questo senso vedasi FLOR 2023, pp. 126-129.

72. La considerazione qui espressa trova approfondimento in FLOR 2023, pp. 144-145.

73. Sul concetto di *cybersecurity* come di un nuovo diritto fondamentale si rinvia a PAPAKONSTANTINO 2022.

caratterizzato da affidabilità sistemica anche sul piano tecnologico. In tal modo, la prevenzione, che tradizionalmente ha rivestito un ruolo “debole”, viene potenziata, assumendo valore cogente e misurabile attraverso procedure di audit e di vigilanza.

6. Riflessioni conclusive. I caratteri “mobilitatori” del diritto penale della sicurezza digitale

L'indagine ha perseguito l'obiettivo di articolare una proposta di lettura dell'attuale fisionomia del diritto penale nella specifica materia della sicurezza digitale, concentrandosi sui profili strutturali, assiologici e funzionali che ne definiscono l'essenza e ne orientano le traiettorie evolutive, con particolare attenzione alle implicazioni derivanti dalla progressiva permeabilità delle tecnologie nei processi giuridici ed economici. Dinanzi all'avanzata incessante della rivoluzione digitale – fenomeno caratterizzato da rapidità trasformativa e da tratti di contingente⁷⁴ instabilità, che ne accentuano la complessità, – la strategia che appare metodologicamente più efficace per contenere il disorientamento sistemico indotto da tale evoluzione sembra rinvenirsi nel ricorso al sistema delle definizioni. Tale sistema, concepito come strumento di delimitazione concettuale e presidio della funzione di garanzia propria del diritto, è inteso quale baluardo della certezza normativa e della tutela dei valori fondamentali dell'ordinamento.

L'individuazione dei caratteri “facilitatori” e “mobilitatori”⁷⁵ della scienza penalistica nell'era digitale ha costituito lo scopo finale della riflessione, scaturita dall'analisi delle scelte legislative a livello europeo, delle quali il Regolamento DORA, concepito per contrastare i fenomeni di criminalità informatica in un settore di assoluta strategicità per il sistema Paese e per il mercato unico eurounitario, rappresenta un esempio virtuoso. L'intento è stato quello di tentare di fornire un contributo all'edificazione di un paradigma penalistico valido

nel quinto dominio, in cui si intersecano tecnologie, tangibili e intangibili, e innovazione.

In primo luogo, si osserva il carattere *binario* delle scelte legislative in parola, che perseguono non soltanto la funzione repressiva, ma anche una componente *preventiva*, che assume una duplice rilevanza, sistemica e sistematica. La scienza penalistica, intesa come strumento di repressione, è concepita esclusivamente per l'essere umano. Tuttavia, nel contesto dei reati informatici, una delle ulteriori finalità che possono sostenerla e aggiornarla è la prevenzione, intesa come il complesso di misure e presidi di matrice culturale, tecnico-informatica e giuridica, che, in un'ottica precauzionale, sono in grado di scongiurare gli effetti potenzialmente deleteri della criminalità informatica.

A tutt'oggi, come evidenziato dalle previsioni del Regolamento DORA, i meccanismi preventivi si concentrano sulla creazione di condizioni organizzative e tecnologiche adeguate a neutralizzare una serie ampia di rischi calcolati e coinvolgono gli assetti aziendali, le infrastrutture tecniche disponibili, le filiere di fornitura avviate e gli ecosistemi di dati oggetto di trattamento.

Nello scenario tecnologico, le attività preventive e repressive, tradizionalmente considerate separate, formano un sistema complesso e dinamico, paragonabile a una fitta rete di “vasi comunicanti”⁷⁶. Questa interconnessione si manifesta con particolare evidenza nel cyberspazio, in cui le categorie tradizionali del diritto penale vengono significativamente sollecitate, a causa dell'asimmetria strutturale tra la velocità elevata con cui si sviluppa l'azione criminale e la lentezza delle risposte repressive.

Per tale ragione, la giustizia penale ha sviluppato una tendenza alla proiezione anticipatoria rispetto alla commissione del fatto di reato, finalizzata a neutralizzare le cyber minacce prima ancora che esse si concretizzino, attraverso l'implementazione di meccanismi di gestione preventiva, quali la cybersecurity, che si configura come un nuovo

74. Sul carattere contingente della tecnologia si rinvia a CALO 2026.

75. L'aggettivo “mobilitatore” è stato tratto dal Rapporto *Molto più di un mercato: velocità, sicurezza, solidarietà. Potenziare il mercato unico per garantire un futuro sostenibile e la prosperità di tutti i cittadini dell'UE* presentato il 18 aprile 2024 dall'ex Presidente del Consiglio italiano Enrico Letta al Consiglio europeo. Il rapporto mira a contribuire alla riflessione sul futuro dell'Unione europea e alla predisposizione dell'Agenda Strategica del Consiglio europeo per il periodo 2024-2029.

76. APRATI 2023, p. 469.

paradigma di diritto preventivo operante non solo su un piano individuale, ma anche su quello collettivo e collettivistico delle strutture e delle infrastrutture.

In tale prospettiva, il penalista è chiamato a concepire la sicurezza informatica come un bene giuridico collettivo, che incarna non soltanto la protezione dell'individuo, ma anche la stabilità e l'integrità dei sistemi tecnologici, da proteggere con strumenti normativi coordinati, quali standard minimi di sicurezza, obblighi di segnalazione di incidenti, piani di continuità operativa e sistemi di certificazione dei processi interni ed esterni.

La metodologia applicata dal legislatore europeo sembra focalizzata sulla *prevenzione situazionale*, con l'intento di ridurre le probabilità di attacco mediante la gestione di scenari critici e l'identificazione di situazioni a rischio, con l'obiettivo di sviluppare risposte che garantiscano un margine di sicurezza concreto.

Il volto preventivo del diritto penale nell'era digitale si caratterizza per la già menzionata ibridazione con il diritto amministrativo, nonché con il diritto della regolazione economica e il sapere tecnico-informatico. Alla sanzione viene affiancata la costruzione di comportamenti organizzativi virtuosi, la cui omissione determina l'applicabilità di sistemi di diritto punitivo, ossia sanzioni amministrative.

In questi termini, emerge il carattere *proattivo* del diritto penale contemporaneo, che non si limita più alla mera repressione del fatto, ma, nel cyberspazio, impone una riorganizzazione della risposta statale e privata secondo modalità, forme e tempi nuovi, allontanandosi dalla sua immagine tradizionale. La trasformazione concettuale attiene alla già citata traduzione della categoria del rischio informatico in una categoria autonoma di diritto, da cui discende l'obbligo di rispettare vincoli di governance interna ed esterna, e responsabilità operative. In quest'ottica, il Regolamento DORA impone alle entità finanziarie (e il d.gs. n. 23/2025 anche ai fornitori) rilevanti obblighi di conformità normativa, prescrivendo standard contrattuali minimi nell'esternalizzazione dei servizi ICT e concepisce l'*accountability* come un parametro di diligenza qualificata, che si collega concettualmente alla colpa per omessa vigilanza, la cui violazione integra non soltanto un deficit di compliance regolamentare, ma può fungere da indice sintomatico

di colpa ai fini della responsabilità penale personale del management e di quella para-penale dell'ente. Per l'effetto, le suddette entità sono tenute a svolgere un ruolo attivo, propositivo e partecipativo sia nel corso delle trattative contrattuali con i fornitori, sia nella propria governance interna, oltre che, ovviamente, nei rapporti con le Autorità garanti, pena l'irrogazione delle sanzioni previste dalla normativa.

Inoltre, è stato osservato che la normativa analizzata presenta un carattere spiccatamente *multidisciplinare*, sintomatico della complessità ontologica del fenomeno criminale in esame. Le sfide emergenti poste dal cybercrime hanno condotto il legislatore europeo a una rilevante trasformazione concettuale: il rischio tecnologico non può e non deve più essere eluso, ma governato. Il passaggio "dal rischio al diritto" ha segnato una rivoluzione epocale nella gestione e nella neutralizzazione dei rischi informatici, introducendo normative fondate su strategie trasversali di prevenzione, sia di carattere tecnico che giuridico. L'approccio integrato, che unisce il diritto penale, il diritto amministrativo, il diritto dell'informatica e la regolazione dei mercati, ha elevato il concetto di resilienza operativa digitale a principio di governance, con una funzione paragonabile a quella della stabilità finanziaria. Nel laboratorio giuridico europeo, la resilienza operativa è stata elevata a indicatore di affidabilità dell'intero ecosistema, incarnando la trasposizione giuridica della fiducia tecnologica. A conferma di tale transizione, il Regolamento DORA stabilisce un modello normativo che traduce il linguaggio tecnico della gestione del rischio in linguaggio giuridico. Il nuovo paradigma di gestione integrata dei rischi cibernetici risponde a un elevato livello di sofisticazione tecnica, sia a livello tecnologico che a livello giuridico, e richiede il rispetto di numerosi obblighi contrattuali che necessitano del possesso di specifiche competenze e conoscenze in materia di obsolescenza tecnologica, procedure e tempistiche di gestione di un incidente ICT, analisi e gestione dei rischi, implementazione di stress test, metriche di performance attese, sviluppi tecnici, strategie di uscita, attività di monitoraggio e di reporting, attenzione ai contenuti contrattuali e ai regimi di responsabilità. Il grado di tecnicità richiesto dai nuovi requisiti contrattuali minimi è evidenziato dalla severa produzione normativa

che interessa i Regolamenti di secondo livello, i già menzionati RTS e ITS.

La vigilanza interna dell'entità finanziaria si estende, pertanto, alla gestione dell'evoluzione tecnologica dei servizi esternalizzati e la disciplina si distingue per una profonda consapevolezza della dinamicità e della mutevolezza del mercato di riferimento, delineando un modello di gestione che affida a tutti i soggetti della filiera l'identificazione delle metodologie ottimali e degli strumenti più adeguati, al fine di garantire un assetto nel quale operano una sostanziale conformità con gli obiettivi e i contenuti della normativa.

In tale scenario, il diritto penale non può più limitarsi alla mera considerazione del fattore umano, ma dovrebbe, invece, integrarlo con il dato tecnologico e prestare attenzione alle potenzialità insite negli strumenti precauzionali, come la cybersecurity, che diventa il criterio ordinante dell'intera normativa.

Non da ultimo, il diritto penale all'epoca della sicurezza digitale richiede l'implementazione di tattiche di difesa attiva, che si configurano come forme di *cyber compliance* dinamica di carattere *multilivello*, e prevedono l'obbligo di anticipare, gestire e condividere il rischio ICT con tutti i soggetti che compongono la catena di erogazione del servizio. Questo implica il coinvolgimento attivo di tutte le entità private, ossia le organizzazioni operanti nel settore finanziario, bancario e assicurativo, i fornitori di servizi ICT, e pubbliche, che compongono la rete comune di protezione dei nuovi interessi nell'era digitale, quale fattore determinante per la stabilità del mercato europeo, coinvolgendo diversi livelli di governo aziendale, economia e società, tra i quali personale dipendente, consigli di amministrazione e Autorità garanti, nazionali ed europee.

A ciò si aggiunga che è prevista una stretta collaborazione tra tutti gli attori coinvolti, secondo logiche di *co-regolazione* o di *regolazione partecipativa*, tra il regolatore, il regolato e le Autorità "guardiane". Tale meccanismo riecheggia le forme di cooperazione pubblico-privata già note al legislatore europeo nell'ambito del diritto penale processuale e si ritiene, pertanto, che la normativa stia evolvendo verso la riproposizione di tali modelli collaborativi virtuosi anche nel contesto del diritto penale sostanziale.

Il discorso sulla fisionomia del diritto penale dell'informatica e, più nello specifico, del "diritto penale della sicurezza digitale" costituisce un tema *in fieri*: la sua evoluzione risentirà, inevitabilmente, degli strumenti con cui il penalista affronterà e maneggerà la sfida tecnologica.

La scienza penalistica, storicamente antropocentrica, risulta, tuttora, impreparata rispetto alle peculiarità e alla velocità che caratterizzano la rivoluzione tecnologica. In assenza di sviluppi rilevanti, sussiste il rischio che il diritto penale non riesca a preservare la propria competitività e la propria capacità deterrente rispetto a fenomeni che possiedono il potenziale di innescare reazioni a livello globale.

Il contributo si prefigge di offrire una lettura della normativa esaminata, concepita come proposta di riflessione destinata a contribuire al dibattito sulle dinamiche evolutive del diritto penale. Attualmente, la sua frammentazione interna, la sua visione persistentemente antropocentrica, la sua spiccata reattività e l'isolamento rispetto alle altre discipline, configurano un insieme di fattori che possono collocarlo in una condizione di criticità operativa. Tuttavia, tali limiti non possono essere invocati per giustificare una resa concettuale o metodologica della scienza penalistica.

Al contrario, la traiettoria delineata dal legislatore europeo – che promuove il riconoscimento della rilevanza di strumenti di contrasto preventivo, fondati su logiche punitivo-proattive, multidisciplinari, multilivello e di co-regolazione – si configura come un approccio potenzialmente capace di farsi carico delle sfide emergenti poste dalla criminalità informatica, conciliando rigore normativo e funzionalità.

La possibile soluzione all'attuale *impasse* tecnologico, a sostegno della scienza penalistica, sembra rinvenirsi nella costruzione di una sinergia tra i diversi saperi disciplinari e nella valorizzazione dell'eterogeneità degli strumenti adottati, anche con riferimento ai differenti destinatari della normativa. Tale approccio consente, da un lato, di potenziare l'efficacia della risposta penale e, dall'altro, di fronteggiare in maniera consapevole le potenzialità lesive insite nei dati, i quali rappresentano la nuova incarnazione tecnologica del potere e, al contempo, un terreno complesso di tensione tra innovazione, controllo e responsabilità.

Il Regolamento DORA rappresenta una testimonianza della trasformazione strategica delle scelte legislative europee nel senso sopra indicato, avendo adottato un'impostazione orientata verso una cultura della sicurezza informatica basata sulla regolazione partecipativa e giungendo ad assumere la funzione di un manifesto di prevenzione giuridica. Il linguaggio tecnico della resilienza è stato integrato con quello giuridico della responsabilità condivisa e la cybersecurity è stata riconosciuta come principio trasversale della stabilità economica europea, costituendo una responsabilità collettiva che contribuisce alla sopravvivenza e alla tenuta del mercato digitale.

In tale contesto, il sistema penalistico è chiamato a svolgere un ruolo pionieristico in un momento di trasformazione epocale, assumendo la sfida di

coniugare rigore normativo, efficacia preventiva e incisività operativa.

Il *file rouge* che ha guidato l'individuazione dei caratteri "facilitatori" e "mobilitatori" menzionati in precedenza risiede in una ravvisata esigenza di pragmatismo e concretezza nella materia. Tali criteri appaiono imprescindibili per l'edificazione di un "diritto penale della sicurezza digitale" solido, in quanto fondato su principi chiari, coerenti e capaci di resistere alla repentinità dell'evoluzione tecnologica, ed efficace, nella misura in cui consente interventi puntuali, proporzionati e tempestivi per fronteggiare le minacce informatiche emergenti. Un quadro giuridico concepito in tal modo sembra idoneo a confrontarsi efficacemente con le complesse dimensioni geo-politiche, sociali ed economiche di un'epoca caratterizzata da crescente tecnocentricità.

Riferimenti bibliografici

- G. ALFANO (2024), *Rischi informatici nel settore finanziario: strumenti di prevenzione e resilienza operativa digitale*, in "Rivista di Diritto Bancario", 2024, n. 4 suppl.
- P. ANGELINI (2024), *La cybersicurezza del settore finanziario: ruolo delle autorità e valore della cooperazione*, in "La cooperazione pubblico-privato per la resilienza cyber del settore finanziario italiano - Le opportunità per gli operatori e il ruolo del CERTF", Banca d'Italia, 2024
- F. ANGIONI (1983), *Contenuto e funzioni del concetto di bene giuridico*, Giuffrè, 1983
- R. APRATI (2023), *L'attività di prevenzione e l'acquisizione della notizia di reato*, in G. Colaiacovo (a cura di), "Sicurezza, informazioni e giustizia penale", Pacini Giuridica, 2023
- ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA (2025), *Rapporto Clusit 2025: l'evoluzione della minaccia cibernetica*, Security Summit, Milano, 11-13 marzo 2025
- S. ATERNO (2023), *Profili penali della vita nel Metaverso*, in G. Cassano, G. Scorza (a cura di), "Metaverso. Diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT", Pacini Giuridica, 2023
- S. ATERNO (2022), *Sicurezza informatica: aspetti giuridici e tecnici*, Pacini Giuridica, 2022
- I. AYRES, J. BRAITHWAITE (1992), *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, 1992
- G. BARBARA (2022), *La cybersecurity: minacce, evoluzione normativa, corporate governance e nuove prospettive*, in "Corporate Governance", 2022, n. 4
- G. BETTIOL (1959), *L'odierno problema del bene giuridico*, in "Rivista italiana di diritto e procedura penale", 1959, n. 1
- J. BLACK (2001), *Decentring regulation: understanding the role of regulation and self-regulation in a 'post-regulatory' world*, in "Current Legal Problems", vol. 54, 2001, n. 1
- A.J. BLAŽIČ, B.J. BLAŽIČ (2024), *Toward effective learning of cybersecurity: new curriculum agenda and learning methods*, in "Journal of Cybersecurity", vol. 10, 2024, n. 1

- F. BRICOLA (1973), *Teoria generale del reato*, in “Novissimo digesto italiano”, vol. XIV, 1973
- B. BUCKLAND, F. SCHREIER, T. WINKLER (2015), *Democratic governance challenges of cyber security*, in “DCAF Horizon 2015 Working Paper Series”, 2015, n. 1
- D. BUSCH (2024), *The future of Equivalence in the EU Financial Sector*, in “European Business Organization Law Review”, vol. 25, 2024, n. 1
- R. CALO (2026), *Law and Technology A Methodical Approach*, Oxford University Press, 2026
- A.A. CARDANI, I. GIRARDI (2024), *Impresa bancaria ed esternalizzazione di servizi tecnologici*, in “Orizzonti del Diritto Commerciale”, 2024, n. 2
- S. CARREA (2017), *L’individuazione del forum commissi delicti in caso di illeciti cibernetici: alcune riflessioni a margine della sentenza Concurrence Sàrl*, in “Diritto del commercio internazionale”, 2017, n. 3
- E. CHIOCCHIO (2022), *Una nuova centralità per la cyber security nel settore finanziario*, in bancaforte.it, 28 luglio 2022
- G. CORASANTI (2025), *Strategie di contrasto al ransomware e nuove frontiere della criminalità informatica*, in “Il diritto dell’informazione e dell’informatica”, 2025, n. 1
- F. CORONA (2023), *I reati informatici*, in M. Iasselli, G.B. Caria (a cura di), “Cybersecurity & Cyberwarfare, Diritto tecnologia e sicurezza”, EPC Editore, 2023
- F. CORONA (2021), *Il cybercrime: soggetto, oggetto e condotta*, in Id. (a cura di), “Reati informatici e investigazioni digitali”, Pacini Giuridica, 2021
- L. CUOMO (2000), *La tutela dei beni informatici*, in L. Cuomo, G. Di Giandomenico (a cura di), “Profili giuridici dell’informatica”, Edizioni Scientifiche Italiane, 2000
- L. CUOMO, B. IZZI (2002), *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in “Cassazione penale”, 2002, n. 3
- L. CUOMO, R. RAZZANTE (2009), *La nuova disciplina dei reati informatici*, Giappichelli, 2009
- M. DI CUIA (2025), *Cyber attacco, produzione bloccata: l’INPS può concedere la CIGO?*, in “Altalex”, 19 marzo 2025
- M. DONINI (2013), *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in “Diritto penale contemporaneo”, 2013, n. 4
- M. DONINI (2003), *Alla ricerca di un disegno. Scritti sulle riforme penali in Italia*, Cedam, 2003
- M. DONINI (1999), *Teoria del reato*, in “Digesto discipline penalistiche”, vol. XIV, Utet, 1999
- D. FADDA (2025), *In cassa integrazione per colpa del ransomware: sempre più casi in Italia*, in cybersecurity360.it, 20 febbraio 2025
- N.M.F. FARAONE (2024), *IA e vigilanza prudenziale: alla ricerca di un nuovo equilibrio tra presidio dei rischi e trasformazione digitale dell’impresa bancaria*, in “Rivista di Diritto Bancario”, 2024, n. 4
- G. FIANDACA (1982), *Il bene giuridico come problema teorico e come criterio di politica criminale*, in “Rivista italiana di diritto e procedura penale”, 1982, n. 1
- A. FIORELLA (1987), *Reato in generale*, in “Enciclopedia del diritto”, vol. XXXVIII, Giuffrè, 1987
- 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

- R. FLOR (2023), *Lawful hacking, vulnerabilità tecnologica e diritto penale, fra esigenze di accertamento dei reati e tutela di beni giuridici di nuova generazione*, in L. Picotti (a cura di), "Automazione, diritto e responsabilità", Edizioni Scientifiche Italiane, 2023
- R. FLOR (2022), *Le indagini ad alto contenuto tecnologico fra esigenze di accertamento e repressione dei reati e tutela penale di tradizionali e nuovi beni giuridici nell'era digitale*, in R. Flor, S. Marcolini (a cura di), "Dalla data retention alle indagini ad alto contenuto tecnologico", Giappichelli, 2022
- R. FLOR (2019-A), *Cybersecurity e il contrasto ai cyberattacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in "Diritto di internet", 2019, n. 3
- R. FLOR (2019-B), *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), "Cybercrime. Diritto e procedura penale dell'informatica", Utet Giuridica, 2019
- D. FRACCHIOLLA (2022), *La cyber-diplomacy, la nuova frontiera delle relazioni internazionali*, in "Digital Politics", vol. 2, 2022, n. 3
- GARANTEE PER LA PROTEZIONE DEI DATI PERSONALI (2020), *Tecnologia e diritto devono allearsi per una corretta governance digitale. Intervista ad Antonello Soro*, in garanteprivacy.it, 2020
- P. GHIGNATTI (2024), *DORA, inizia il conto alla rovescia per le aziende: i cinque pilastri per la compliance*, in cybersecurity360.it, 23 febbraio 2024
- G. GONZÁLEZ FUSTER, L. JASMONTAITE (2020), *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. Christen, B. Gordijn, M. Loi (eds.), "The Ethics of Cybersecurity", Springer, 2020
- L. LESSIG (1999), *Code And Other Laws of Cyberspace*, Basic Books, 1999
- A. LICASTRO (2025), *La configurazione dei mercati digitali a partire dal Digital Markets Act*, in "Rivista della Regolazione dei Mercati", 2025, n. 1
- F. LORÈ, P. MUSACCHIO (2021), *Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva?*, in "Amministrativamente", 2021, n. 1
- F. MANTOVANI (1977), *Il principio di offensività del reato nella Costituzione*, in "Aspetti e tendenze del diritto costituzionale. Scritti in onore di Costantino Mortati", Giuffrè, 1977
- G.L. MARCIALIS (2023), *La sicurezza informatica di frontiera: il modello "secure by design" nei sistemi biometrici*, in G. Colaiaicovo (a cura di), "Sicurezza, informazioni e giustizia penale", Pacini Giuridica, 2023
- L. MARTINO (2018), *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in "Politica&Società", 2018, n. 3
- A. MATTARELLA (2022), *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in "Diritto penale e processo", 2022, n. 6
- L. MENELLY (1985), *Prosecuting Computer-Related Crime in the United States, Canada and England: New Laws for Old Offenses?*, in "Boston College International & Comparative Law Review", vol. 8, 1985
- N. MICIELI (2024), *Cybersecurity e gestione del rischio ICT: l'impatto sulla corporate governance*, in "Banca Impresa Società", 2024, n. 2
- G.P. MILLER (2014), *Compliance function: an overview*, New York University School of Law, Law & Economics Research Paper Series, Working Paper n. 14-36, November 2014
- V. MONGILLO (2022), *Presente e futuro della compliance penale*, in sistemapenale.it, 2022
- G. MORGANTE (2025), *Transizione digitale e diritto penale. Dall'evoluzione delle categorie sostanziali al "nuovo volto" del law enforcement*, in "Rivista italiana di informatica e diritto", 2025, n. 2

- G.N. NEPPI MODONA (1965), *Il reato impossibile*, Giuffrè, 1965
- D. PADOVAN (2023), *La sicurezza informatica*, in M. Iasselli, G.B. Caria (a cura di), "Cybersecurity & Cyberwarfare. Diritto, tecnologia e sicurezza", EPC Editore, 2023
- A. PAGLIARO (1965), *Bene giuridico e interpretazione della legge penale*, in "Studi in onore di Francesco Antolisei", vol. II, Milano, 1965
- V. PAPAKONSTANTINO (2022), *Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?*, in "Computer Law & Security Review", vol. 44, 2022
- D.B. PARKER (1974), *Computer-related crime*, in "Journal of Forensic Sciences", vol. 19, 1974, n. 2
- C. PECORELLA (2006), *Diritto penale dell'informatica*, Cedam, 2006
- E.F. PÉREZ CARRILLO (2023), *Cybersecurity in European Financial Institutions: new grounds for corporate governance reform*, in "European Business Law Review", vol. 34, 2023, n. 7
- L. PICOTTI (2011), *Sicurezza informatica e diritto penale*, in M. Donini, M. Pavarini (a cura di), "Sicurezza e diritto penale", Bononia University Press, 2011
- L. PICOTTI (2000), *Reati informatici*, in "Enciclopedia giuridica Treccani", vol. aggiorn. VIII, 2000
- S. PIETROPAOLI (2019), *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in "Rivista di filosofia del diritto", 2019, n. 2
- M. PIGNATTI (2024), *La resilienza operativa digitale per il settore finanziario tra vincoli contrattuali e responsabilità*, in "Diritto ed economia dell'impresa", 2024, n. 4
- G.D. PISAPIA (1948), *Introduzione alla parte speciale del diritto penale*, Giuffrè, 1948
- D. PIVA (2022), *Cybersecurity e corporate governance tra valutazioni top-down e tecniche bottom-up*, in "Corporate Governance", 2022, n. 4
- A. PORTOLANO, J. MAZZA (2023), *Regolamento DORA: novità in arrivo per i contratti di fornitura dei servizi ICT*, in "Agenda Digitale", 28 giugno 2023
- D. PULITANÒ (1981), *La teoria del bene giuridico fra codice e Costituzione*, in "La Questione criminale", 1981, n. 1
- F. RAFFAELE (2024), *Appunti sul c.d. Cybersecurity Risk Management tra disclosure statunitense e approccio regolatorio europeo*, in "Il Nuovo Diritto delle Società", 2024
- I. RAMADHAN (2021), *The Implication of Cyberspace Towards State Geopolitics*, in "Politicon: Jurnal Ilmu Politik", vol. 3, 2021, n. 2
- R. RAZZANTE (2023), *L'attribuzione degli attacchi informatici e il cyberterrorismo*, in Id. (a cura di), "Manuale di cybersicurezza", Pacini Giuridica, 2023
- R. RAZZANTE (2022), *Cybersecurity e 231: il raccordo tra norme ed eventi*, in "La responsabilità amministrativa delle società e degli enti", 2022, n. 1
- A. ROCCO (1913), *L'oggetto del reato e la tutela giuridica penale*, Fratelli Bocca, 1913
- T.E. ROMOLOTTI (2019), *Cybersecurity: un ponte tra GDPR e d.lgs. 231/2001 alla luce del d.lgs. 101/2018*, in "Responsabilità amministrativa delle società e degli enti", 2019, n. 2
- G. SCHNEIDER (2022), *La resilienza operativa digitale come materia di corporate governance: prime riflessioni a partire dal DORA*, in "Corporate Governance", 2022, n. 4
- R. SHARMA (2022), *Cyber Security to Safeguard Cyber Attacks*, in "International Journal of Information Security and Cybercrime (IJISC)", vol. 11, 2022, n. 2
- F. STELLA (1973), *La teoria del bene giuridico e i c.d. fatti inoffensivi conformi tipo*, Giuffrè, 1973

- A. STILE (1985), *Bene giuridico e riforma della parte speciale*, Jovene, 1985
- W.G. URGESSA (2020), *Multilateral cybersecurity governance: Divergent conceptualizations and its origin*, in “Computer Law & Security Review”, vol. 36, 2020
- R.M. VADALÀ (2025), *La fattispecie penale tra economia digitale e diritto europeo*, Giappichelli, 2025
- G. VASSALLI (1982), *Considerazioni sul principio di offensività*, in “Studi in onore di Pietro Pioletti”, Giuffrè, 1982



ROBERTO FLOR – BEATRICE PANATTONI

Il concetto di criminalità grave e la sfida della proporzionalità nelle indagini digitali

Il contributo analizza il ruolo del principio di proporzionalità nelle indagini penali digitali, con particolare attenzione alla nozione di “criminalità grave” quale criterio di delimitazione dell’impiego degli strumenti investigativi maggiormente invasivi. Muovendo dalla giurisprudenza della Corte di giustizia dell’Unione europea, l’analisi si concentra su due *case studies* emblematici: la *data retention* e l’accesso alle comunicazioni cifrate. Mentre nel primo ambito la Corte ha progressivamente elaborato un modello di bilanciamento fondato sul rapporto tra gravità dell’ingerenza e gravità del reato perseguito, nel secondo la riflessione si è concentrata prevalentemente sulle garanzie procedurali e sull’utilizzabilità della prova. Il contributo propone una lettura integrata del principio di proporzionalità che tenga insieme diritto processuale penale, diritto della protezione dei dati personali e diritto penale sostanziale, evidenziando come la nozione di “criminalità grave” possa fungere da parametro sostanziale per orientare tanto le scelte legislative quanto il controllo giudiziale sulle investigazioni digitali.

Proporzionalità – Data Retention – Criminalità grave – Indagini digitali – Diritti fondamentali

The concept of serious crime and the challenge of proportionality in digital investigations

This paper examines the role of the principle of proportionality in digital criminal investigations, focusing on the notion of “serious crime” as a criterion for limiting the use of the most intrusive investigative powers. Drawing on the case law of the Court of Justice of the European Union, the analysis addresses two key case studies: data retention and access to encrypted communications. While the Court has progressively developed, in the field of data retention, a framework based on the relationship between the seriousness of the interference and the seriousness of the offence investigated, the debate concerning encrypted communications has mainly focused on procedural safeguards and admissibility of evidence. The article proposes an integrated understanding of proportionality combining criminal procedure, data protection law, and substantive criminal law, arguing that the notion of “serious crime” should serve as a substantive benchmark for both legislative choices and judicial review in the regulation of digital investigations.

Proportionality – Data Retention – Serious Crimes – Digital investigations – Fundamental rights

Roberto Flor è professore ordinario in diritto penale presso il Dipartimento di Scienze Giuridiche dell’Università degli Studi di Verona (autore dei par. 1 e 3)

Beatrice Panattoni è ricercatrice post doc in diritto penale presso la Faculty of Law, Economics and Finance dell’Università del Lussemburgo e docente a contratto presso il Dipartimento di Scienze Giuridiche dell’Università degli Studi di Verona (autrice dei par. 2 e 4)

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli

SOMMARIO: 1. Investigazioni digitali: bilanciamento tra lotta al crimine e tutela dei diritti fondamentali. – 2. Il *case study* della *data retention*. – 3. *Encryption, lawful hacking* e accesso alle comunicazioni cifrate: la proporzionalità nelle investigazioni su larga scala. – 4. Proporzionalità e “criminalità grave”.

1. Investigazioni digitali: bilanciamento tra lotta al crimine e tutela dei diritti fondamentali

La progressiva digitalizzazione della società ha prodotto una trasformazione profonda del panorama investigativo, imponendo una riconsiderazione dei mezzi tradizionalmente impiegati nella ricerca della prova. L'aumento esponenziale dei flussi di comunicazione elettronica, la pervasività dei dispositivi digitali nella vita quotidiana e la conseguente disponibilità di enormi masse di dati hanno radicalmente mutato le modalità attraverso cui le autorità accedono alle informazioni rilevanti ai fini investigativi¹, dovendo fronteggiare forme di criminalità altrettanto segnate da una marcata digitalizzazione. Di fronte a tale scenario, è ormai indispensabile confrontarsi con una duplice esigenza: da un lato, dotare gli organi investigativi di strumenti adeguati per contrastare fenomeni criminali sempre più complessi e tecnologicamente sofisticati; dall'altro, garantire che l'esercizio di tali “poteri investigativi” avvenga nel rispetto dei diritti fondamentali e delle garanzie individuali².

L'impatto della trasformazione digitale sulle investigazioni penali non si esaurisce tuttavia nell'introduzione di nuovi strumenti tecnici. Più profondamente, esso investe la stessa struttura epistemica dell'accertamento penale. Il crescente patrimonio informazionale derivante dalla disponibilità di dati generati dalle attività quotidiane degli individui, ossia dai diversi processi di *datafication*, ha infatti favorito l'emersione di un nuovo paradigma investigativo, frequentemente descritto attraverso l'espressione *data-driven investigations*³; formula che racchiude in sé un duplice mutamento.

Da un lato, essa evidenzia come nell'ambiente digitale “*evidence is all about data*”⁴. Le attività investigative si traducono in operazioni di raccolta, conservazione, selezione, elaborazione e correlazione di informazioni digitali provenienti dalle fonti più disparate: comunicazioni elettroniche, dispositivi personali, servizi online, piattaforme sociali, sistemi di geolocalizzazione, infrastrutture cloud e banche dati pubbliche e private.

Dall'altro lato, il paradigma *data-driven* introduce una trasformazione qualitativa ancora più significativa. Le caratteristiche dell'ecosistema

1. La letteratura sul punto è ormai alquanto ampia e difficilmente riassumibile. Tra i principali riferimenti nel contesto domestico cfr. CAIANIELLO 2025; DI PAOLO–PRESSACCO 2025; FLOR–MARCOLINI 2022; CAIANIELLO 2019; LASAGNI 2018. A livello europeo cfr. VAVOULA 2026; OERLEMANS–ROYER 2023; BACHMAIER WINTER 2022. Tra le ricerche empiriche cfr. LAVORGNA–UGWUDIKE 2021.

2. SACHOULIDOU 2026; LASAGNI 2018.

3. In particolare, le ultime frontiere del tema hanno portato la comunità scientifica ad interrogarsi sull'impatto dell'impiego dei sistemi di intelligenza artificiale nel contesto delle indagini penali. Anche su questo la letteratura è ormai numerosa. Tra i più recenti si vedano i contributi raccolti in LIGETI 2026.

4. Cfr. l'editoriale di GALIČ–STEVENS–KOOPS 2023, e i contributi raccolti nella *special issue* di “New Journal of European Criminal Law”, 14(4), 2023.

digitale rendono infatti meno centrale, o addirittura ostacolano, la ricerca mirata di informazioni relative a fatti e soggetti determinati e favoriscono, invece, la raccolta preventiva e generalizzata di enormi quantità di dati, da analizzare successivamente attraverso tecniche automatizzate. La logica dell'investigazione tende così a spostarsi dall'individuazione reattiva di prove riferibili a un reato commesso e ad un sospettato già identificato verso la costruzione preventiva di una più ampia *information position* – quale tecnica derivante propriamente dalle attività di *intelligence*⁵ – funzionale non soltanto all'accertamento di reati già realizzati, ma anche all'individuazione preventiva di rischi e minacce⁶. La trasformazione in atto implica quindi un parziale mutamento della razionalità investigativa. Nelle investigazioni digitali contemporanee, la disponibilità di grandi quantità di dati consente spesso di individuare correlazioni, schemi comportamentali e profili di rischio. L'attenzione tende così a spostarsi dalla ricostruzione di eventi già verificatisi alla costruzione di una conoscenza preventiva del fenomeno criminale. In tale prospettiva, le investigazioni digitali acquisiscono sempre più frequentemente, per l'appunto, la veste di attività di *intelligence*, in un contesto che si caratterizza per una imprescindibile vocazione transnazionale.

La possibilità di raccogliere e conservare preventivamente enormi quantità di dati di traffico, dati di localizzazione e, in alcuni casi, persino dati relativi al contenuto delle comunicazioni, accentua ulteriormente tale tendenza. Il modello della sorveglianza mirata (*targeted surveillance*), costruito attorno a uno specifico soggetto o a uno specifico fatto di reato, tende progressivamente a confrontarsi con pratiche di raccolta generalizzata delle informazioni che, pur perseguendo finalità

investigative legittime, presentano tratti riconducibili a una c.d. *mass surveillance*. La distinzione tra raccolta selettiva e raccolta indiscriminata dei dati diviene pertanto meno netta rispetto al passato, con conseguenze particolarmente rilevanti sul piano delle garanzie individuali⁷.

Il grado di invasività delle investigazioni digitali risulta infatti strutturalmente più incisivo rispetto a quello delle tecniche investigative “convenzionali”. Come ha chiarito la Corte di giustizia dell'Unione europea (CGUE) in diverse occasioni, la raccolta massiva di dati di traffico e localizzazione – anche a prescindere dall'accesso al contenuto delle comunicazioni – può consentire di trarre conclusioni assai precise sulla vita privata delle persone interessate, incluse le loro abitudini, i loro luoghi di residenza, gli spostamenti quotidiani, le attività svolte, nonché le relazioni personali e l'ambiente sociale⁸. In questo contesto assume particolare rilievo il quadro di tutela offerto dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza), considerato come le investigazioni digitali incidano dunque sulla tutela del diritto al rispetto della vita privata e familiare e sul diritto alla protezione dei dati personali, rendendo necessario un sistema di garanzie che tenga conto della specifica capacità informativa delle tracce digitali generate dagli individui.

Le investigazioni digitali pongono pertanto un problema di “traduzione”⁹ delle regole tradizionali. Come è stato osservato, l'avvento delle tecnologie digitali impone di ripensare le basi teoriche dei diritti e delle libertà protette dalle Carte europee, al fine di elaborare regole procedurali capaci di garantire un adeguato livello di tutela nell'ambiente digitale¹⁰. Si tratta, peraltro, di una questione che coinvolge la maggior parte degli ordinamenti,

5. Si parla infatti di “intelligence-led policing”. Cfr. GOLDSTEIN 1990.

6. Cfr. DE JONGE–DE VRIES 2024.

7. Su questo cfr. MITSILEGAS–GUILD–KUSKONMAZ–VAVOULA 2023.

8. Si vedano riferimenti in par. 2 e 3.

9. Come evidenzia CAIANIELLO 2019, richiamando WASHINGTON–RICHARDS 2019: la rivoluzione digitale “squarely presents the problem of translation for constitutional rules. It requires courts to answer the question how (or if) we will translate our hard-won protections of civil liberties into the digital environment [...] Translating ancient principles and doctrines to emerging technologies such as the cloud, location tracking, and encryption has proven so difficult as to threaten civil liberties themselves. One way or another, our response to this challenge will become our generation's defining legacy of civil liberties”.

10. LASAGNI 2018.

compresi quelli oltreoceano, come l'ordinamento statunitense, in cui da tempo sono emerse analoghe riflessioni, che hanno evidenziato come la crescente difficoltà di applicare categorie elaborate per il mondo analogico a fenomeni caratterizzati dalla continua produzione e circolazione di informazioni digitali debba condurre al ripensamento di alcuni istituti e diritti¹¹.

In questo tentativo di “traduzione”, quindi, vi sono due questioni particolarmente rilevanti con cui occorre interfacciarsi: quella dell'atipicità e quella della proporzionalità.

Per quanto riguarda la prima, ossia l'atipicità che può connotare questi mezzi investigativi, si osserva come gli strumenti investigativi vigenti – *rectius* i mezzi di ricerca della prova – pensati in un'epoca in cui le comunicazioni assumevano forme ben definite e le tracce dell'attività umana erano prevalentemente materiali, possano rivelarsi inadeguati a disciplinare la complessità e la varietà delle tecniche investigative digitali attualmente disponibili. Ne risultano significativi deficit in punto di legalità, che si manifestano non soltanto nell'assenza di un quadro normativo organico, ma anche nell'inadeguatezza delle categorie concettuali tradizionali a cogliere la specificità dell'atto digitale¹². Questa circostanza pone questioni non solamente in relazione alle modalità d'acquisizione, ma anche in relazione alla quantità e alla qualità delle informazioni che possono essere ricavate da tali attività. Un ulteriore elemento distintivo consiste, infatti, nel potenziale coinvolgimento di una pluralità di soggetti estranei al procedimento. Le tecniche di raccolta massiva di dati incidono frequentemente su persone che non rivestono la qualità di indagati e che non risultano in alcun modo collegate ai fatti oggetto di accertamento. Le informazioni raccolte possono riguardare interlocutori occasionali, utenti appartenenti alla medesima piattaforma digitale, soggetti geograficamente prossimi alla persona investigata o, più in generale, individui i cui dati vengono acquisiti incidentalmente nel corso delle operazioni investigative¹³.

Il panorama delle investigazioni digitali appare inoltre estremamente eterogeneo. Risulta alquanto

complesso ricomprendere in un quadro sistematico il ricco insieme di attività che possono essere ricondotte entro il cappello di “indagini digitali”, considerato che ognuna di esse pone poi questioni assai tecniche e specifiche. Volendo fare uno sforzo di sintesi, rientrano in questo insieme attività d'indagine digitale occulte (come è il caso del controllo occulto dei dispositivi, ossia il c.d. *lawful hacking*), palesi (come sono i sequestri informatici), attività di *open source intelligence* (come le stesse *social network analysis*), attività d'indagine che si servono di sistemi di intelligenza artificiale, così come attività di cooperazione con attori privati, e in particolare, con *online service providers*, a cui possono essere rivolti ordini di produzione di dati in loro possesso. A ciò si aggiunge la dimensione frequentemente transnazionale che caratterizza tali operazioni, con le conseguenti trasmissioni e scambi di ingenti dataset tra autorità appartenenti a ordinamenti diversi.

Non è tuttavia su queste specifiche attività, e sull'atipicità che le può connotare in relazione ai mezzi di ricerca della prova disciplinati dal codice di procedura penale, che si soffermerà l'analisi. Adottando una prospettiva interdisciplinare, che tenga conto non soltanto del diritto processuale penale ma anche del diritto della protezione dei dati personali e del diritto penale sostanziale, l'attenzione sarà rivolta alla seconda questione appena richiamata, ossia quella attinente alla proporzionalità quale parametro di legittimità dell'azione investigativa digitale. Studi recenti hanno iniziato a valorizzare la necessità di creare un dialogo interdisciplinare sul punto tra diritto processuale penale e diritto della protezione dei dati personali, valorizzando il contributo che quest'ultimo può offrire nella definizione dei limiti all'esercizio dei poteri investigativi¹⁴. A tale prospettiva può essere affiancata una terza dimensione, rappresentata dal diritto penale sostanziale, poiché la delimitazione dei poteri investigativi più invasivi presuppone inevitabilmente una scelta circa i fenomeni criminali che giustificano il sacrificio dei diritti fondamentali coinvolti, assicurando al contempo l'*habeas data*, inteso quale

11. KERR 2024.

12. Cfr. NICOLICCHIA 2024; ŠKORVÁNEK-KOOPS-NEWELL-ROBERTS 2019; NEWELL-TIMAN-KOOPS 2018.

13. Cfr. par. 3.

14. GALIČ-STEVENSON-KOOPS 2023.

base fondativa dei diritti di libertà della persona nella dimensione immateriale dell'infosfera¹⁵.

Il principio di proporzionalità, quale concetto e categoria polimorfica che esprime un approccio relazionale volto al bilanciamento armonioso tra punti contrapposti¹⁶, nel contesto che qui interessa svolge una funzione di bilanciamento tra l'efficienza dell'accertamento penale e la tutela dei diritti individuali¹⁷. Esso viene definito, nell'ordinamento multilivello, attraverso il riferimento all'art. 52 della Carta di Nizza, il quale richiede che limitazioni all'esercizio di diritti e libertà siano previste dalla legge, necessarie, rispondano effettivamente a finalità di interesse generale (come è la lotta al crimine)¹⁸. Viene poi articolato, più nello specifico nell'ambito della procedura penale, nei sub-criteri della idoneità, necessità e proporzionalità in senso stretto¹⁹.

Tale parametro non opera tuttavia soltanto come criterio applicativo, ma assume anche forti declinazioni politico criminali. Esso presuppone una scelta di fondo circa le forme di criminalità rispetto alle quali le ingerenze investigative più penetranti possono essere considerate tollerabili in una società democratica, con conseguenti ricadute sul concetto, indeterminato e controverso, di ciò che intendiamo con "criminalità grave".

Come si vedrà, infatti, la progressiva emersione della nozione di "criminalità grave" nella giurisprudenza europea appare, sotto questo profilo, particolarmente significativa. Quanto maggiore è la capacità intrusiva dello strumento investigativo, tanto più forte diviene l'esigenza di circoscriverne l'utilizzo a fenomeni criminali ritenuti particolarmente lesivi degli interessi fondamentali della collettività. Il problema si sposta così dall'individuazione della misura investigativa alla definizione dell'obiettivo che può giustificarla.

Entro questa cornice, il presente contributo si propone di analizzare, muovendo dalla giurisprudenza europea, le recenti linee evolutive che

caratterizzano la proporzionalità nelle investigazioni digitali, con particolare riguardo al ruolo assunto dalla nozione di "criminalità grave" quale criterio selettivo dell'intensità dell'interferenza investigativa ammissibile. A tal fine, dopo aver esaminato i *case studies* dati da due ambiti particolarmente rilevanti nel contesto delle indagini digitali, ossia quello della *data retention* e quello delle comunicazioni *encrypted* (par. 2 e 3), si procederà a una valutazione della funzione della nozione di criminalità grave all'interno del test di proporzionalità (par. 4).

2. Il case study della data retention

Un primo osservatorio privilegiato per analizzare il rapporto tra investigazioni digitali, tutela dei diritti fondamentali e principio di proporzionalità è rappresentato da un settore particolare della cooperazione tra pubblico e privato e, nello specifico, dagli ordini di produzione di dati che possono essere inviati a fornitori di servizi telematici e dalla disciplina della conservazione dei dati di traffico delle comunicazioni elettroniche, comunemente nota come *data retention*. Tale ambito assume particolare rilevanza non soltanto per il ruolo centrale che i dati di traffico svolgono nelle indagini, ma anche perché è proprio in questo settore che la CGUE ha elaborato, nel corso dell'ultimo decennio, una ricca giurisprudenza.

Come noto, si tratta di una materia segnata da una movimentata evoluzione. Il punto d'inizio è stato segnato dalla disciplina originariamente prevista dalla direttiva 2006/24/CE (c.d. Data Retention Directive), poi invalidata dalla famosa sentenza *Digital Rights*, dove si è affermato che la conservazione generalizzata dei dati di traffico e localizzazione relativi alle comunicazioni effettuate dagli utenti sia contraria al principio di proporzionalità²⁰. Si è infatti inizialmente chiarito come non sia sufficiente che una misura limitativa dei diritti fondamentali sia prevista dalla legge e che

15. Cfr. DI PAOLO 2024.

16. BILLIS-KNUST-RUI 2021; LACEY 2016; COGNETTI, 2011; HICKMAN 2008.

17. Cfr. CAIANIELLO 2025; CAIANIELLO 2014.

18. Si tornerà più diffusamente sul punto nel par. 4.

19. CAIANIELLO 2014.

20. C. giust. UE, 8 aprile 2014, *Digital Rights Ireland Ltd*, C-293/12 e C-594/12, par. 34, 36, 42, 38, 54. Cfr. FLOR-MARCOLINI 2022; FORMICI 2021; MARCOLINI 2019; FABBRINI 2015; FLOR 2014.

persegua un obiettivo legittimo di interesse generale, ma occorra altresì verificare se il legislatore abbia predisposto un sistema sufficientemente preciso e dettagliato di garanzie idonee a circoscrivere l'ingerenza entro quanto strettamente necessario al perseguimento delle finalità perseguite.

A partire da tale sentenza è poi iniziato un lungo percorso giurisprudenziale nel quale la CGUE ha progressivamente affinato i criteri di legittimazione del regime della *data retention*²¹, con numerose ricadute nei diversi ordinamenti europei, i quali hanno portato a recenti dettagliati studi comparati sul punto²².

Dalla giurisprudenza europea emerge come il collegamento tra gravità dell'ingerenza derivante dal regime di *data retention* e gravità del reato perseguito assuma una formulazione particolarmente esplicita. La Corte afferma infatti in diverse occasioni che una grave interferenza nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta può essere giustificata soltanto da obiettivi di lotta contro forme gravi di criminalità, dove quindi il principio della “minima interferenza” nei diritti fondamentali violati nel raggiungimento dello scopo può e deve dirsi “contenutistico”, nel senso che per rispettarlo non è sufficiente che trovi una cornice formale nel diritto positivo, ma occorre investigare come il legislatore abbia esercitato la riserva di legge formale²³.

Dalle critiche volte alla Data Retention Directive, che consentiva l'esercizio del diritto di accesso delle autorità pubbliche per reati genericamente definiti come “gravi”, con inaccettabile rinvio per la specificazione di tale concetto ai legislatori nazionali²⁴, si è iniziato a raffinare questa categoria in sentenze successive. Si è affermato che “in conformità al principio di proporzionalità, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come ‘grave’”²⁵. Nel caso *La Quadrature du Net T* si è delineata una gerarchia tra gli obiettivi di interesse pubblico che possono giustificare una restrizione nella protezione dei diritti, distinguendo tra esigenze di sicurezza nazionale, ordine pubblico e lotta contro il “*serious crime*”, evidenziando come quest'ultimo non possa essere equiparato a minacce alla sicurezza nazionale, che tradizionalmente legittimano forme più intense d'attività di *intelligence*²⁶.

All'interno di questo percorso evolutivo si arriva così alla recente sentenza della CGUE del 30 aprile 2024²⁷, che ha coinvolto in particolare l'ordinamento italiano e la disciplina interna in materia di *data retention*²⁸. La pronuncia trae infatti origine da un rinvio pregiudiziale promosso dalla Procura di Bolzano nell'ambito di un procedimento riguardante alcuni episodi di furto di telefoni cellulari, in

21. Sulle vicissitudini che hanno caratterizzato l'ambito e l'interpretazione dell'obbligo di *data retention* e, in particolare, la copiosa giurisprudenza europea che si è pronunciata in punto, si è già dedicato un altro contributo nel presente fascicolo, cfr. BONETTI 2026, a cui si rimanda, il quale approfondisce in particolare il tema da una prospettiva privatistica, confermando così la necessità di un approccio interdisciplinare al tema, che consideri le specificità della materia della protezione dei dati personali.

22. KOSTA-KAMARA 2025.

23. FLOR-MARCOLINI 2022.

24. C-293/12 e C-594/12, cit., par. 60: “la suddetta mancanza generale di limiti si aggiunge il fatto che la direttiva 2006/24 non prevede alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la direttiva 2006/24 si limita a rinviare, all'articolo 1, paragrafo 1, in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno”.

25. C. giust. UE, 18 gennaio 2018, *Ministerio Fiscal*, C-270/16, par. 56.

26. C. giust. UE, 6 ottobre 2020, *La Quadrature du Net et al.*, C-511/18, C-512/18, C-520/18, par. 61-63. Cfr. MITSILEGAS 2026.

27. C. giust. UE, 30 aprile 2024, *Ignoti c. Italia*, C-178/22.

28. Cfr. i commenti alla sentenza: PARODI 2025; DALLA TORRE 2024; ALBANESE 2024; GRISONICH 2024; MARINO 2024.

cui, nel corso delle indagini, il PM aveva richiesto l'autorizzazione all'acquisizione dei dati conservati dagli operatori telefonici ai sensi dell'art. 132, comma 3, del d.lgs. n. 196/2003 (codice privacy). Nello specifico si era richiesto di acquisire "tutti i dati in possesso delle compagnie, con metodo di tracciamento e localizzazione, chiamati/chiamanti, siti visitati/raggiunti, orario e durata della chiamata/connessione (...)"²⁹, quindi, sia dati relativi al traffico, sia dati relativi all'ubicazione, i quali permettono evidentemente di trarre precise conclusioni sulla vita privata dei titolari, qualificandosi come ingerenza grave nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta.

La possibilità di procedere in tal senso è dovuta al fatto che la disciplina italiana dell'art. 132 comma 3 prevede che le autorità possano procedere con la richiesta di acquisizione dei dati conservati dai *provider* nel caso in cui le indagini riguardino reati per i quali si prevede la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, così come per i reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, nel caso in cui la minaccia, la molestia e il disturbo siano gravi, nel caso in cui tali dati siano rilevanti per l'accertamento dei fatti o per le ricerche di un latitante.

La soglia dei tre anni dunque permette che rientrino nell'ambito di applicazione di questo strumento investigativo anche "reati che destano solo scarso allarme sociale e che sono punitivi solo a querela di parte"³⁰, come i furti di scarso valore (ossia quelli che interessavano il caso di specie), senza che il giudice italiano disponga di un sufficiente margine di discrezionalità per negare l'autorizzazione in questi casi, dal momento che è sufficiente, affinché venga rilasciata, essere in presenza di "sufficienti indizi", e che i dati richiesti "siano rilevanti ai fini dell'accertamento del reato". Attraverso il rinvio alla CGUE si è dunque sollevata la conformità al diritto europeo della disciplina italiana, e in particolare il fatto che la formulazione adottata non lasci ai giudici

un margine di valutazione in ordine alla concreta gravità del reato oggetto d'indagine.

Nella sua decisione, la CGUE ribadisce anzitutto il proprio orientamento, ormai consolidato, secondo cui l'accesso ai dati di traffico e localizzazione costituisce una grave ingerenza nei diritti garantiti dagli artt. 7 e 8 della Carta e può pertanto essere giustificato soltanto da obiettivi di lotta contro forme gravi di criminalità o di prevenzione di gravi minacce alla sicurezza pubblica³¹. Tuttavia, la parte più interessante della pronuncia riguarda il tentativo di precisare il contenuto della nozione di "*serious crime*".

La CGUE prende parzialmente posizione sul punto. Coscienziosamente, viene ribadito che la competenza sul punto spetta e rimane in capo agli Stati membri, ma si specifica che essa deve essere esercitata nel rispetto del diritto dell'Unione. Nello specifico, si afferma che gli ordinamenti nazionali non possono "snaturare" la nozione di 'reato grave', e, per estensione, quella di 'grave criminalità', includendovi reati che manifestamente non sono gravi, alla luce delle condizioni sociali esistenti nello Stato membro interessato, sebbene il legislatore di tale Stato abbia previsto di punirlo con la pena della reclusione non inferiore nel massimo a tre anni"³².

È proprio su questo punto che emerge con particolare evidenza la duplice dimensione del giudizio di proporzionalità. Da un lato, vi è una dimensione astratta, affidata al legislatore, il quale individua *ex ante* le categorie di reati ritenute sufficientemente gravi da giustificare determinate forme di interferenza investigativa. Dall'altro lato, permane una dimensione concreta, che richiede una valutazione della specifica fattispecie oggetto di indagine e dell'effettiva gravità del fatto rispetto all'ingerenza richiesta. La sentenza sembra dunque suggerire che il rispetto del principio di proporzionalità non possa essere assicurato esclusivamente mediante il ricorso a soglie legislative fondate sulla pena edittale, per quanto venga allo stesso tempo affermato che la tecnica di fissazione di soglie a partire dalla pena massima per giustificare che il reato sia qualificato come grave "non è necessariamente

29. C-178/22, cit., par. 17.

30. *Ivi*, par. 21.

31. *Ivi*, par. 42.

32. *Ivi*, par. 50.

contraria al principio di proporzionalità³³ (anche se rimane la criticità della mancata considerazione del limite della pena minima)³⁴.

Seppur, dunque, un criterio oggettivo rimanga imprescindibile, in quanto capace garantire un minimo livello di prevedibilità e certezza del diritto, viene evidenziato come, da solo, rischi di risultare eccessivamente rigido, ove non accompagnato dalla possibilità di una valutazione in concreto della gravità della fattispecie – come peraltro ritroviamo espresso anche nella giurisprudenza domestica³⁵.

La difficoltà principale risiede tuttavia nel parametro individuato dalla Corte per orientare tale valutazione. Il riferimento a reati “manifestamente non gravi alla luce delle *condizioni sociali* esistenti nello Stato membro interessato” appare infatti caratterizzato da un elevato grado di indeterminatezza. Non risulta immediatamente chiaro quali siano le “condizioni sociali” rilevanti, né quali criteri il giudice debba utilizzare. Osservazioni interessanti si possono invece ricavare dalle conclusioni dell’Avvocato generale, che suggeriva di utilizzare un criterio meglio definito, quale quello delle “circostanze che caratterizzano lo specifico caso di cui trattasi”, compresi i danni causati alle vittime di reato e i rischi per i terzi coinvolti³⁶. Il rischio derivante da una simile formulazione è dunque quello di attribuire al giudice un margine di discrezionalità particolarmente ampio, suscettibile di incidere sulle stesse scelte di politica criminale compiute dal legislatore³⁷.

Le ricadute che questa pronuncia della CGUE avranno nel contesto interno riguarderanno infatti la possibilità per i giudici interni di compiere un autonomo sindacato di proporzionalità in concreto sulla gravità del reato seguendo un criterio così indeterminato; possibilità che secondo alcuni commenti dovrebbe essere negata, preferendo piuttosto attendere un intervento chiarificatore del legislatore o un coinvolgimento della Corte

Costituzionale, anche attraverso un ulteriore rinvio alla CGUE che chieda di esplicitare in modo più preciso tale criterio³⁸, mentre altre voci lasciano aperta tale possibilità per i giudici nazionali³⁹.

Nonostante le criticità rilevate, la pronuncia della CGUE mette bene in luce la centralità della delimitazione di ciò che può definirsi “criminalità grave”, con evidenti ricadute sia in sede di politica criminale, in relazione alla disciplina di mezzi investigativi tecnologicamente connotati e altamente intrusivi, sia in sede giudiziale, in relazione alla applicazione del c.d. test di proporzionalità. Il caso della *data retention* mostra dunque con particolare chiarezza come la proporzionalità operi attraverso l’individuazione di criteri sufficientemente rigorosi per stabilire quali forme di criminalità siano in grado di giustificare il sacrificio dei diritti fondamentali coinvolti. È proprio quest’ultimo profilo a costituire il punto di collegamento con il successivo ambito di analisi, relativo all’accesso alle comunicazioni cifrate, nel quale il rapporto tra gravità dell’ingerenza e gravità del reato appare assai meno definito rispetto a quanto avvenuto nel settore appena richiamato.

3. *Encryption, lawful hacking e accesso alle comunicazioni cifrate: la proporzionalità nelle investigazioni su larga scala*

Se il settore della *data retention* costituisce il principale laboratorio entro cui la CGUE ha progressivamente elaborato il rapporto tra gravità dell’ingerenza investigativa e gravità del reato perseguito, un secondo osservatorio particolarmente significativo è rappresentato dalle investigazioni aventi ad oggetto comunicazioni protette da sistemi di cifratura (*encryption*). Anche in questo ambito emerge con forza la tensione tra esigenze investigative e tutela dei diritti fondamentali. Diversamente da quanto avviene nel caso della

33. *Ivi*, par. 58.

34. *Ivi*, par. 57.

35. Cfr. Cass. pen., sez. III, 25 settembre 2019, n. 48737, in “OneLegale”, dove si evidenzia che tale principio “mal si presta ad una preventiva, rigida codificazione”.

36. Cfr. Conclusioni dell’avvocato generale A.M. Collins, presentate l’8 giugno 2023.

37. DALLA TORRE 2024.

38. *Ibidem*.

39. ALBANESE 2024; TODARO 2024.

conservazione dei dati di traffico, tuttavia, la questione si presenta in termini in parte differenti, poiché il problema non riguarda soltanto l'accesso a informazioni già detenute da soggetti privati, ma investe la possibilità stessa di superare le barriere tecnologiche predisposte a tutela della riservatezza delle comunicazioni direttamente da parte delle autorità pubbliche.

La cifratura costituisce oggi una delle principali infrastrutture tecnologiche della sicurezza digitale. Attraverso la trasformazione delle informazioni in dati intelligibili esclusivamente ai soggetti autorizzati, essa garantisce la riservatezza delle comunicazioni, la protezione dei dati personali, la sicurezza delle transazioni economiche e, più in generale, l'affidabilità dell'ambiente digitale. Essa rappresenta uno strumento essenziale per la protezione della vita privata nell'ambiente digitale. Come è stato osservato, la cifratura contribuisce alla creazione di una vera e propria "zona di privacy", funzionale all'esercizio di diritti fondamentali quali la libertà di opinione e di espressione⁴⁰.

Proprio perché svolge una funzione cruciale nella tutela dei diritti individuali, l'*encryption* pone questioni particolarmente delicate sotto il profilo investigativo. Le autorità di contrasto si confrontano infatti con una crescente diffusione di servizi e dispositivi caratterizzati da elevati livelli di protezione crittografica, che possono rendere estremamente complesso l'accesso alle comunicazioni rilevanti ai fini probatori. Tale fenomeno emerge con evidenza nei noti casi di *EncroChat*⁴¹ e *Sky ECC*⁴², che hanno rappresentato alcune delle più vaste operazioni investigative digitali realizzate in Europa negli ultimi anni. Entrambe le piattaforme offrivano servizi

di comunicazione fortemente protetti mediante cifratura end-to-end e ulteriori funzionalità volte a rafforzare l'anonimato degli utenti. Pur essendo formalmente accessibili a chiunque, esse risultavano frequentemente utilizzate nell'ambito di attività riconducibili alla criminalità organizzata transnazionale e al traffico internazionale di stupefacenti.

Le indagini condotte dalle autorità francesi hanno consentito di acquisire l'accesso alle infrastrutture tecnologiche di tali servizi mediante tecniche di *lawful hacking*, permettendo la raccolta di enormi quantità di comunicazioni successivamente condivise con numerose autorità investigative europee. Nel caso *EncroChat*, le autorità sono riuscite ad acquisire centinaia di milioni di messaggi; nel caso *Sky ECC*, il numero delle comunicazioni raccolte ha superato il miliardo. I dati ottenuti sono stati successivamente oggetto di processi di selezione e analisi automatizzata attraverso ricerche per parole chiave, sistemi di correlazione e altre tecniche tipiche delle investigazioni *data-driven*.

Tali casi si inseriscono dunque appieno nel quadro appena delineato sollevando la questione attinente al bilanciamento tra l'esigenza di accesso ai dati da parte delle autorità pubbliche e la tutela di infrastrutture digitali progettate per garantire la riservatezza delle comunicazioni e quindi la sicurezza dell'ecosistema digitale, senza considerare le problematiche relative ai modelli di "trasferimento probatorio" e di "raccolta transnazionale della prova" (che non sono oggetto specifico del presente studio).⁴³

A differenza delle tradizionali intercettazioni, l'oggetto dell'intervento investigativo non coincide con una singola comunicazione o con uno specifico soggetto previamente individuato. L'operazione

40. KAYE 2015.

41. C. giust. UE, 30 aprile 2024, *M.N. (EncroChat)*, C-670/22; C. giust. UE, 4 luglio 2024, *M.R.*, C-288/24; Corte EDU, 17 ottobre 2024, *A.L. e E.J. c. Francia*, ric. nn. 44715/20 e 47930/21. Cfr. BAJOVIĆ-ĆORIĆ 2025; LASSALLE-LANNIER 2025.

42. OERLEMANS-ROYER 2023.

43. Si rinvia a DI PAOLO 2024. L'Autrice evidenzia "l'eterno problema – dovuto al fatto che manca a tutt'oggi un'armonizzazione, seppur minima, delle discipline probatorie nazionali – è quello della utilizzabilità della prova allogena e, a monte, quello della disciplina applicabile per la sua raccolta (*lex loci* o *lex fori*). Si tratta di una criticità in parte affievolita dall'ibridismo che connota il sistema dell'ordine europeo di indagine penale (O.E.I.), nell'ambito del quale, per assicurare la spendita del 'risultato' probatorio raccolto *ultra fines*, si prevede espressamente la possibilità che la prova sia confezionata dall'autorità di esecuzione secondo le "indicazioni" formali e procedurali richieste dall'autorità emittente, con sostanziale prevalenza della *lex fori*. Altro aspetto degno di nota è l'espresso riferimento, nella direttiva relativa all'O.E.I., al principio di proporzionalità, elevato a parametro di controllo sulla legittimità dell'attività probatoria richiesta, sia per l'autorità di emissione che per l'autorità di esecuzione".

investe invece un'intera infrastruttura comunicativa – si parla infatti di *bulk interception* – consentendo l'acquisizione simultanea delle comunicazioni generate da migliaia di utenti⁴⁴. Diviene così sempre più complesso distinguere tra singole acquisizioni investigative e formazione progressiva di grandi patrimoni informativi suscettibili di impieghi successivi. Il rischio è che la nozione stessa di raccolta massiva finisca per perdere capacità selettiva, dal momento che quasi ogni indagine digitale produce oggi dataset potenzialmente riutilizzabili per ulteriori finalità investigative.

Questi casi hanno suscitato lunghe e complesse vicende giudiziali nell'ambito di diversi ordinamenti europei, dal momento che i dati collezionati dalle autorità francesi sono poi stati oggetti di trasferimenti transfrontalieri in diversi ordinamenti, come quello tedesco, olandese, inglese e anche italiano, fino poi ad arrivare, in alcuni casi, anche alle corti europee⁴⁵. Molto clamore queste vicende hanno suscitato in relazione alla questione delle salvaguardie procedurali e i diritti di difesa che dovrebbero essere garantiti durante queste investigazioni, nonché al nodoso problema dell'ammissibilità della prova in un contesto di investigazioni *cross-border*.

In tale contesto, il principio di proporzionalità assume dunque una funzione centrale, anche e soprattutto in relazione alla protezione dei terzi che risultano coinvolti nelle attività investigative, imponendo di valutare non solo l'impatto delle misure adottate sui diritti degli utenti e sulle caratteristiche del servizio oggetto dell'intervento, ma anche la gravità dei reati perseguiti. In questo contesto particolare rilievo assumono quindi non solo il momento dell'acquisizione dei dati, ma soprattutto le lavorazioni eseguite a posteriori, ossia i criteri con i quali l'accusa seleziona progressivamente i dati rilevanti per le indagini, evidenziando come la proporzionalità debba essere garantita sempre non solo *ab initio*, ma anche *in itinere*: prospettiva che, come è stato evidenziato, sembra essere stata messa in secondo piano dalle difese nelle sentenze

domestiche sul caso *Sky ECC*, dove ci si è prevalentemente concentrati sull'utilizzo dell'algoritmo di decrittazione⁴⁶.

Il dibattito sviluppatosi attorno a tali vicende si è naturalmente concentrato prevalentemente sulle garanzie procedurali. Le principali questioni affrontate hanno riguardato la qualificazione giuridica delle attività compiute dalle autorità straniere, i presupposti per il trasferimento transfrontaliero dei dati, i diritti della difesa e le condizioni di utilizzabilità delle informazioni raccolte; mentre limitata attenzione è stata invece dedicata al tema delle condizioni sostanziali che dovrebbero giustificare il ricorso a forme investigative caratterizzate da un livello di intrusività così elevato. La CGUE ricorre alla proporzione solamente per minacciare la conseguente esclusione della prova nel caso in cui sia stata preclusa alla difesa la possibilità di commentare le prove digitali prodotte dall'accusa⁴⁷.

Sotto questo profilo emerge una significativa differenza rispetto all'evoluzione registrata nel settore della *data retention*. Come si è visto, in quel contesto la giurisprudenza europea sta progressivamente costruendo un sistema di garanzie fondato anche sul rapporto tra gravità dell'ingerenza e gravità della criminalità perseguita. Nei casi relativi alle comunicazioni cifrate, invece, la nozione di "criminalità grave" è rimasta sostanzialmente sullo sfondo del dibattito giuridico. La circostanza appare particolarmente significativa se si considera che le operazioni *EncroChat* e *Sky ECC* sono state giustificate proprio in ragione del coinvolgimento di fenomeni riconducibili alla criminalità organizzata transnazionale e al traffico internazionale di stupefacenti. In altri termini, le autorità investigative hanno operato all'interno di un contesto caratterizzato dalla presenza di forme di criminalità unanimemente considerate particolarmente gravi. Tale dato fattuale ha probabilmente contribuito a ridurre l'attenzione verso la necessità di elaborare criteri generali idonei a delimitare il ricorso a tali strumenti investigativi.

44. OERLEMAS–VAN TOOR 2022. Interessante in questo senso anche il caso *Podchasov v. Russia*, Cfr. Corte EDU, 13 febbraio 2024, appl. 33696/19; nonché il caso *Big Brother Watch and Others v. the United Kingdom*, Corte EDU, 25 maggio 2021, appl. 58170/13, 62322/14, 24960/15.

45. LASSALLE–LANNIER 2025.

46. CAIANIELLO 2025.

47. C-670/22, cit. Cfr. PANZAVOLTA–MAES 2022.

Tuttavia, proprio la straordinaria capacità intrusiva di queste tecniche suggerirebbe la necessità di una riflessione più approfondita sul rapporto tra gravità dell'ingerenza e gravità del reato perseguito. Quanto maggiore è la capacità di uno strumento investigativo di incidere simultaneamente sui diritti di un elevato numero di soggetti, tanto più forte dovrebbe essere l'esigenza di circoscriverne l'utilizzo a fenomeni criminali dotati di particolare offensività.

Il rischio che si rimanga silenti a livello europeo sul punto è che tale questione sia affrontata in modo frammentato dai diversi ordinamenti nazionali. In questa prospettiva, alcuni spunti possono essere ricavati dalle discipline nazionali che regolano il ricorso ai captatori informatici⁴⁸. Anche nell'ordinamento italiano, infatti, l'utilizzo delle forme investigative tecnologicamente più invasive è generalmente subordinato alla presenza di specifiche categorie di reati considerate particolarmente gravi dal legislatore. Pur trattandosi di contesti normativi differenti, tale modello evidenzia come la delimitazione sostanziale delle finalità investigative costituisca uno strumento essenziale per garantire il rispetto del principio di proporzionalità.

Le vicende relative alle comunicazioni cifrate mostrano dunque un quadro per molti aspetti ancora incompleto. Se la giurisprudenza europea ha sviluppato una teoria relativamente articolata della proporzionalità nell'ambito della *data retention*, analoga elaborazione non sembra essersi ancora consolidata con riguardo alle tecniche di accesso a comunicazioni protette da sistemi di cifratura⁴⁹. Il dibattito continua a concentrarsi prevalentemente sulle garanzie procedurali e sull'utilizzabilità delle prove raccolte, mentre rimane in larga misura aperta la questione relativa alle condizioni sostanziali che possono giustificare il ricorso a forme di acquisizione massiva delle comunicazioni digitali.

Il confronto tra i due *case studies* evidenzia così una significativa asimmetria. È proprio questa asimmetria che conduce alla questione conclusiva del presente contributo: quale funzione debba assumere la nozione di "criminalità grave" all'interno del test di proporzionalità nelle investigazioni digitali e quali criteri possano orientarne una definizione sufficientemente determinata e compatibile con le esigenze di tutela dei diritti fondamentali.

4. Proporzionalità e "criminalità grave"

Le considerazioni svolte nei paragrafi precedenti mostrano come il principio di proporzionalità rappresenti oggi il principale criterio di legittimazione delle investigazioni digitali. La crescente capacità delle tecnologie investigative di incidere sulla sfera privata degli individui rende infatti insufficiente una prospettiva fondata esclusivamente sul principio di legalità formale, imponendo una valutazione ulteriore relativa alla giustificazione sostanziale dell'ingerenza.

Sebbene il codice di procedura penale non contenga una disciplina generale del principio di proporzionalità in materia probatoria, tale criterio ha progressivamente assunto una fisionomia autonoma all'interno del sistema⁵⁰, anche grazie all'influenza esercitata dal diritto europeo e dalla giurisprudenza sovranazionale. Tanto la Convenzione europea dei diritti dell'uomo quanto la Carta dei diritti fondamentali dell'Unione europea subordinano infatti la legittimità delle limitazioni ai diritti fondamentali a tale principio, costruito attorno alla presenza di una base legale adeguata, al perseguimento di un obiettivo legittimo di interesse generale e al rispetto del principio di necessità⁵¹.

Nel contesto delle investigazioni digitali, tuttavia, il test di proporzionalità non può essere ricostruito esclusivamente a partire dalle categorie del

48. FLOR-MARCOLINI 2022.

49. LASSALLE-LANNIER 2025. Come evidenziano gli autori, anche se "undoubtedly being the most intrusive [steps] in the process (...), At the European level, neither the ECJ nor the ECtHR has yet addressed the substance of the proportionality of the legal hacking carried out in France. They also have not dealt with the implications of these measures for criminal proceedings abroad. Several applications are pending before the ECtHR, which will likely offer the opportunity to revisit the matter. However, as these applications are not directed against France as the 'collecting country', the Court in Strasbourg is not going to discuss the proportionality of legal hacking".

50. CAIANELLO 2025.

51. Espressamente previsto dall'art. 52 par. 1 della Carta di Nizza, ma rinvenibile anche nel sistema CEDU anche se non espressamente richiamato. Su questo cfr. GALETTA 1999.

diritto processuale penale. La particolare natura dell'oggetto dell'attività investigativa, costituito da dati personali, comunicazioni elettroniche e informazioni digitali, impone infatti di integrare tale prospettiva con ulteriori coordinate.

Una prima integrazione deriva dal diritto della protezione dei dati personali. Tanto il Regolamento (UE) 2016/679 (GDPR), quanto la direttiva (UE) 2016/680 (Law Enforcement Directive), pur operando in contesti differenti, richiedono che ogni trattamento di dati personali sia necessario e proporzionato rispetto alle finalità perseguite⁵². La proporzionalità assume quindi una dimensione specificamente informazionale, imponendo di considerare non soltanto le modalità di acquisizione dei dati, ma anche la loro qualità, quantità, durata della conservazione, possibilità di riutilizzo e circolazione tra soggetti pubblici e privati⁵³. Si tratta di una prospettiva che appare particolarmente rilevante nelle investigazioni digitali. Una lettura esclusivamente processualistica rischia infatti di concentrarsi prevalentemente sul "contenitore" dell'attività investigativa (il *device*, ad esempio), senza considerare adeguatamente il "contenuto" rappresentato dai dati concretamente accessibili attraverso tali strumenti.

In letteratura⁵⁴, seppur in un contesto diverso da quello delle indagini digitali, ci si è già confrontati con l'integrazione di questi due livelli, da cui deriva un test di proporzionalità che si articola in scanditi passaggi, ossia quelli della disciplina positiva della misura, della finalità legittima perseguita, della necessità della misura in una società democratica. Il terzo step poi racchiude a sua volta diversi sotto-criteri, ossia che la misura sia: genuinamente effettiva, la minor intrusiva possibile, che vi sia un equo bilanciamento tra diritti contrapposti, che vi siano adeguate salvaguardie.

Accanto alla dimensione processuale e a quella della protezione dei dati personali deve poi essere valorizzata una terza prospettiva, rappresentata dal diritto penale sostanziale. È infatti proprio sul terreno della proporzionalità in senso stretto che emerge la necessità di considerare non soltanto

l'intensità dell'ingerenza investigativa, ma anche il valore degli interessi pubblici perseguiti attraverso tale ingerenza. In altri termini, il giudizio di proporzionalità non può limitarsi a verificare se una determinata misura sia astrattamente idonea e necessaria all'accertamento dei fatti, ma deve altresì interrogarsi sulla gravità del fenomeno criminale che ne giustifica l'utilizzo.

Da questo punto di vista, il tradizionale test tripartito elaborato nella cultura giuridica tedesca, articolato nei criteri della idoneità (ossia capacità della misura in astratto a perseguire l'obiettivo prefissato, in questo caso le esigenze probatorie), necessità (ossia assenza di alternative meno intrusive) e proporzionalità in senso stretto (ossia adeguatezza nel bilanciamento tra esigenze contrapposte, in questo caso in relazione al fine perseguito, e quindi alla gravità del reato perseguito), e progressivamente valorizzato anche nel sistema domestico⁵⁵ appare perfettamente compatibile con la struttura del controllo di proporzionalità elaborata dalla giurisprudenza europea e ricavabile dalla disciplina della protezione dei dati personali. I modelli, più che alternativi, risultano complementari.

È proprio all'interno dei diversi livelli che compongono il test di proporzionalità che assume rilievo la nozione di "criminalità grave". Come mostrano le vicende della *data retention* sopra esaminate, la gravità del reato non costituisce un elemento esterno al giudizio di proporzionalità, bensì uno dei suoi fattori costitutivi. Quanto maggiore è la capacità intrusiva dello strumento investigativo, tanto più elevato deve essere il livello di offensività del fenomeno criminale che ne giustifica l'impiego.

La nozione di criminalità grave assume pertanto una duplice funzione. In primo luogo, essa opera sul piano legislativo, orientando le scelte di politica criminale relative alla delimitazione dei presupposti applicativi dei mezzi investigativi maggiormente invasivi. In secondo luogo, essa rileva sul piano applicativo, consentendo al giudice di verificare in concreto se il sacrificio imposto ai

52. Cfr. artt. 6 par. 4, 23, 9, 10, 22 GDPR e art. 4 LED.

53. Cfr. DE JONGE-DE VRIES 2024.

54. BERTRAND-MAXWELL-VAMPARYS 2020.

55. Si veda la ricostruzione del principio fatta da CAIANELLO 2014, compresi i riferimenti relativi alla dottrina tedesca sul punto.

diritti fondamentali risulti giustificato rispetto alle caratteristiche del caso sottoposto al suo esame.

Questa duplice dimensione emerge chiaramente anche dalla recente giurisprudenza della Corte di giustizia relativa alla disciplina italiana della *data retention*. La sentenza della Procura di Bolzano mostra infatti come il rispetto del principio di proporzionalità non possa essere assicurato esclusivamente attraverso criteri legislativi astratti fondati sui limiti edittali di pena, ma richieda altresì una verifica concreta della gravità del fatto oggetto di accertamento. Al tempo stesso, tuttavia, una valutazione interamente rimessa alla discrezionalità giudiziale rischierebbe di compromettere le esigenze di prevedibilità e certezza del diritto.

La soluzione sembra dunque risiedere in un modello integrato, nel quale il legislatore individui *ex ante* le categorie di reati sufficientemente gravi da giustificare il ricorso a determinati strumenti investigativi, lasciando al giudice il compito di verificare, nel caso concreto, se l'ingerenza richiesta risulti effettivamente proporzionata rispetto alle caratteristiche della fattispecie. Occorre, in altri termini, considerare, da un lato, la tipologia del reato (seguendo, ad esempio, le aree di criminalità grave individuate dallo stesso diritto penale europeo)⁵⁶, e, dall'altro, la gravità del fatto.

Anche la giurisprudenza della CGUE sembra muoversi nella medesima direzione. In materia di *data retention*, la Corte ha progressivamente elaborato una vera e propria gerarchia degli interessi pubblici suscettibili di giustificare limitazioni ai diritti fondamentali⁵⁷. Al vertice si colloca la tutela della sicurezza nazionale⁵⁸, seguita dalla prevenzione delle minacce gravi alla sicurezza pubblica e dalla lotta contro forme gravi di

criminalità. Solo in posizione subordinata si collocano, invece, la lotta contro la criminalità ordinaria e gli obiettivi generali di prevenzione.

Le indagini digitali rappresentano, dunque, un terreno particolarmente fertile per sviluppare un dialogo interdisciplinare tra diritto processuale penale, protezione dei dati personali e diritto penale sostanziale. Proprio la crescente centralità del dato quale oggetto dell'attività investigativa impone infatti di superare una visione frammentata delle garanzie, favorendo una lettura integrata delle diverse dimensioni coinvolte.

Anche se rimane il piano applicativo, in ultima istanza, il contesto in cui la proporzionalità assume concretezza e in cui devono quindi raccogliersi in modo equilibrato l'esercizio di un margine di discrezionalità e la sua applicazione rigorosa, attraverso un'adeguata "proceduralità argomentativa"⁵⁹ orientata ai criteri derivanti dal quadro (normativo e giurisprudenziale) europeo, tale impostazione conferma come la proporzionalità non possa essere ridotta a un mero criterio applicativo rimesso alla valutazione del giudice, ma debba essere considerata anche quale salvaguardia metodologica nelle scelte di politica legislativa (eventualmente sindacabile dalla sola Corte Costituzionale). La selezione delle forme di criminalità che giustificano il ricorso agli strumenti investigativi più invasivi costituisce infatti una scelta normativa preliminare, destinata a incidere profondamente sull'equilibrio tra sicurezza e libertà all'interno dell'ordinamento. Ed è proprio la crescente diffusione delle investigazioni digitali a rendere sempre più urgente la costruzione di una disciplina sistematica che assuma il principio di proporzionalità e la nozione di criminalità grave quali parametri centrali nella regolazione dei poteri investigativi tecnologicamente avanzati.

Riferimenti bibliografici

D. ALBANESE (2024), *Dalla Corte di Giustizia dell'Unione europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*, in "Sistema penale", 2024, n. 5

56. Ci si riferisce alle aree di cui all'art. 83 par. 1 TFUE. Evidenzia il problema di lasciare una discrezionalità troppo ampia agli Stati membri MARINO 2024.

57. Cfr. C. giust. UE, 5 aprile 2022, *Commissioner of An Garda Síochána*, C-140/20, par. 56.

58. Cfr. C-511/18, C-512/18, C-520/18, cit.

59. CAIANIELLO 2025.

- L. BACHMAIER WINTER (2022), *Criminal Investigation, Technological Development, and Digital Tools: Where Are We Heading?*, in L. Bachmaier Winter, S. Ruggeri (Eds.), "Investigating and Preventing Crime in the Digital Era", Springer, 2022
- V. BAJOVIĆ, V. ĆORIĆ (2025), *Encrochat and SkyECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 33, 2025
- A. BERTRAND, W. MAXWELL, X. VAMPARYS (2020), *Are AI-Based Anti-Money Laundering Systems Compatible with Fundamental Rights?*, in SSRN, 2020
- E. BILLIS, N. KNUST, J.P. RUI (Eds.) (2021), *Proportionality in Crime Control and Criminal Justice*, Bloomsbury, 2021
- S. BONETTI (2026), *La data retention: alcune riflessioni nella prospettiva del diritto privato della protezione dei dati personali*, in "Rivista italiana di informatica e diritto", 2026, n. 1
- M. CAIANIELLO (2025), *Il principio di proporzionalità nel diritto penale*, in "Rivista italiana di diritto e procedura penale", 2025, n. 3
- M. CAIANIELLO (2019), *Criminal Process Faced with the Challenges of Scientific and Technological Development*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 27, 2019
- M. CAIANIELLO (2014), *Il principio di proporzionalità nel procedimento penale*, in "Diritto Penale Contemporaneo", 2014, n. 3-4
- S. COGNETTI (2011), *Principio di proporzionalità. Profili di teoria generale e di analisi sistematica*, Giappichelli, 2011
- J. DALLA TORRE (2024), *Proporzionalità va cercandosi: la Corte di giustizia sul concetto di criminalità grave nella data retention*, in "Rivista italiana di diritto e procedura penale", 2024, n. 2
- B. DE JONGE, B. DE VRIES (2024), *Data-Driven Investigations in a Cross-Border Setting*, in "eucrim", vol. 19, 2024, n. 3
- G. DI PAOLO (2024), *La circolazione transfrontaliera delle prove elettroniche*, in "Penale. Diritto e Procedura", 2024, n. 2
- G. DI PAOLO, L. PRESSACCO (a cura di) (2025), *Indagini e prove nella società digitale. Questioni attuali e prospettive future*, Editoriale Scientifica, 2025
- F. FABBRINI (2015), *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in "Harvard Human Rights Journal", 2015
- R. FLOR (2014), *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in "Diritto Penale Contemporaneo", 2014, n. 2
- R. FLOR, S. MARCOLINI (2022), *Dalla data retention alle indagini ad alto contenuto tecnologico*, Giappichelli, 2022
- G. FORMICI (2021), *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Giappichelli, 2021
- D.U. GALETTA (1999), *Il principio di proporzionalità nella Convenzione europea dei diritti dell'uomo, fra principio di necessità e dottrina del margine di apprezzamento statale: riflessioni generali su contenuti e rilevanza effettiva del principio*, in "Rivista italiana di diritto pubblico comunitario", vol. 9, 1999, n. 3-4
- M. GALIČ, L. STEVENS, B.-J. KOOPS (2023), *Editorial: A Trialogue on Regulating Data-Driven Criminal Procedure*, in "New Journal of European Criminal Law", vol. 14, 2023, n. 4

- H. GOLDSTEIN (1990), *Problem-Oriented Policing*, McGraw-Hill, 1990
- E. GRISONICH (2024), *Al vaglio della Corte di giustizia la riforma italiana in materia di acquisizione dei tabulati telefonici*, in “Processo Penale e Giustizia”, 2024
- T. HICKMAN (2008), *The Substance and Structure of Proportionality*, in “Public Law”, 2008
- D. KAYE (2015), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/29/32, 22 maggio 2015
- O. KERR (2024), *The Digital Fourth Amendment*, Oxford University Press, 2024
- E. KOSTA, I. KAMARA (Eds.) (2025), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive*, Oxford University Press, 2025
- N. LACEY (2016), *The Metaphor of Proportionality*, in “Journal of Law and Society”, vol. 43, 2016
- G. LASAGNI (2018), *Tackling Phone Searches in Italy and in the US. Proposals for a Technological Re-Thinking of Procedural Rights and Freedoms*, in “New Journal of European Criminal Law”, vol. 9, 2018
- M. LASSALLE, S. LANNIER (2025), *EncroChat – A Judicial Chronology*, in “eucrim”, vol. 20, 2025, n. 4
- A. LAVORGNA, P. UGWUDIKE (2021), *The Datafication Revolution in Criminal Justice: An Empirical Exploration of Frames Portraying Data-Driven Technologies for Crime Prevention and Control*, in “Big Data & Society”, 2021
- K. LIGETI (Ed.) (2026), *AI Evidence and Criminal Proceedings*, Hart Publishing, 2026
- S. MARCOLINI (2019), *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), “Cybercrime”, Utet-WKI, 2019
- F. MARINO (2024), *Comunicazioni elettroniche, perseguimento di reati gravi e rispetto della vita privata*, in “Giurisprudenza Italiana”, 2024
- V. MITSILEGAS (2025), *Data Retention and the Judicial Parameters of Mass Surveillance in EU Law*, in E. Kosta, I. Kamara (Eds.), “Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive”, Oxford University Press, 2025
- V. MITSILEGAS, E. GUILD, E. KUSKONMAZ, N. VAVOULA (2023), *Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks*, in “European Law Journal”, vol. 29, 2023, n. 1-2
- B.C. NEWELL, T. TIMAN, B.-J. KOOPS (Eds.) (2018), *Surveillance, Privacy, and Public Space*, Routledge, 2018
- F. NICOLICCHIA (2024), *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata dall'estero*, in “Sistema penale”, 2024, n. 2
- J.-J. OERLEMANS, S. ROYER (2023), *The Future of Data Driven Investigations in Light of the Sky ECC Operation*, in “New Journal of European Criminal Law”, vol. 14, 2023, n. 4
- J.-J. OERLEMANS, D.A.G. VAN TOOR (2022), *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in “European Journal of Crime, Criminal Law and Criminal Justice”, vol. 30, 2022, n. 3-4
- M. PANZAVOLTA, E. MAES (2022), *Exclusion of Evidence in Times of Mass Surveillance. In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence in Criminal Cases in the European Union*, in “The International Journal of Evidence & Proof”, vol. 26, 2022
- L. PARODI (2025), *La “gravità dell'ingerenza” nel prisma della proporzionalità: nuovi equilibri in tema di data retention*, in “Sistema penale”, 2025

- A. SACHOULIDOU (2026), *A Typology of Automated Law Enforcement Systems Under EU Law: What Standards for Defence Rights?*, in N. Vavoula (Ed.), “The Future of Digitalisation in EU Law Enforcement”, in “European Papers – A Journal on Law and Integration,” vol. 11, 2026, n. 1
- I. ŠKORVÁNEK, B.-J. KOOPS, B.C. NEWELL, A. ROBERTS (2019), “*My Computer Is My Castle*”: *New Privacy Frameworks to Regulate Police Hacking*, in “Brigham Young University law review”, 2019, n. 4
- G. TODARO (2024), *L'evoluzione delle fonti del diritto nella «società algoritmica»: data retention e diritti fondamentali della persona*, in “Cassazione Penale”, 2024, n. 6
- N. VAVOULA (Ed.) (2026), *The Future of Digitalisation in EU Law Enforcement*, in “European Papers – A Journal on Law and Integration”, vol. 11, 2026, n. 1
- M. WASHINGTON, N. RICHARDS (2019), *Digital Civil Liberties and the Translation Problem*, in D.K. Brown, J.I. Turner, B. Weisser (Eds.), “The Oxford Handbook of Criminal Process”, Oxford University Press, 2019



PIETRO SCHIRÒ

La lunga storia delle intercettazioni nel processo penale: dal confidente al captatore informatico

Il contributo ricostruisce, in prospettiva storico-giuridica, l'evoluzione delle tecniche di captazione delle comunicazioni nel processo penale, dalle pratiche informative dell'età inquisitoria fino all'attuale utilizzo del captatore informatico. A partire dall'analisi delle forme di raccolta occulta delle informazioni nel processo inquisitorio – quali delazioni, infiltrazione di confidenti, anonimato delle fonti e segretezza dell'istruttoria – il saggio prova a mostrare come tali pratiche costituissero già nella giurisdizione premoderna un ordinario strumento di accertamento giudiziario. Con l'emergere del costituzionalismo moderno esse non scompaiono, ma vengono progressivamente sottoposte a limiti e garanzie giuridiche. L'articolo segue quindi la trasformazione del concetto di intercettazione tra età delle codificazioni, Novecento e stagione costituzionale. Lo sviluppo delle tecnologie digitali e l'introduzione del captatore informatico ripropongono oggi, in forme nuove, la tensione tra esigenze investigative e tutela dei diritti fondamentali nelle comunicazioni.

*Intercettazioni – Processo inquisitorio – Segretezza delle comunicazioni – Captatore informatico
Diritti fondamentali e processo penale*

The Long History of the Interception of Communications in Criminal Procedure: From Informers to State Trojans

The article reconstructs, from a historical-legal perspective, the evolution of techniques for intercepting communications in criminal proceedings, from the information-gathering practices of the inquisitorial age to the contemporary use of the so-called investigative malware (state trojan). Starting from an analysis of covert information-gathering practices within the inquisitorial process, the study shows how such techniques already constituted an ordinary instrument of fact-finding in pre-modern jurisdiction. With the emergence of modern constitutionalism, these practices did not disappear but were progressively subjected to legal limits and procedural safeguards. The analysis then traces the transformation of the institution through the age of codifications, the twentieth century, and the constitutional era. The development of digital technologies and the introduction of investigative malware today revive, in new forms, the enduring tension between investigative powers and the protection of fundamental rights in the sphere of communications.

*Surveillance – Interception of communications – Inquisitorial procedure – Digital investigations
Fundamental rights*

L'Autore è Ricercatore in Storia del diritto medievale e moderno presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Verona

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli

SOMMARIO: 1. Introduzione. Il captatore informatico: l'eterno ritorno dell'uguale. – 2. Una questione di sicurezza: l'intercettazione durante l'*ancien régime*. – 3. Ordine, sicurezza e limite: la captazione delle informazioni nell'età delle codificazioni. – 4. Ascoltare per prevenire. Le intercettazioni nel primo Novecento. – 5. Dalla costituzionalizzazione delle intercettazioni alla ricerca di una nuova *connessione giuridica*.

1. Introduzione. Il captatore informatico: l'eterno ritorno dell'uguale

Roma, 17 febbraio 1600.

Nel freddo dell'alba le ruote di un carro scivolavano sul selciato umido di Campo de' Fiori. Un uomo incappucciato, accompagnato da alcuni membri dell'Arciconfraternita di San Giovanni Decollato, veniva fatto scendere e consegnato al boia. Nel corso della notte il condannato era stato prelevato dalle carceri di Tor di Nona; dopo le preghiere, le litanie e gli ultimi tentativi di indurlo al pentimento, era stato preparato per l'estremo supplizio¹. L'uomo indossava una mordacchia di ferro che gli serrava la lingua, impedendo qualsiasi parola. Legato completamente nudo al palo mediante un borello, fu circondato dalle fascine accatastate ai suoi piedi. Quando il fuoco attecchì alla paglia, le fiamme si levarono dal basso, avvolgendone progressivamente il corpo. Il legno crepitava, il fumo si addensava nell'aria fredda del mattino. La carne si fece brace, la brace cenere, la cenere polvere sottile che il vento disperse nell'atmosfera. Quella

polvere, residuo ultimo del corpo, tornava a confondersi con la stessa materia di cui è intessuto il cosmo²: con gli elementi prodotti dalle stelle, con la sostanza elementare che compone i mondi senza numero che egli aveva osato pensare nelle sue teorie.

Il rogo pone fine a un processo durato ben sette anni, ma soprattutto conclude un'opera sistematica di captazione delle informazioni organizzate ad arte dall'autorità giudiziaria al fine di condannare Giordano Bruno³. Il procedimento inquisitorio contro il filosofo si sviluppa infatti attraverso una rete articolata di confidenti e informatori che consentono, con le loro attività di registrazione delle dichiarazioni dell'imputato, di far proseguire un processo che in più momenti era arrivato ad una fase di stallo. Lo strumento principale per la *captazione* è, come d'abitudine del Santo Uffizio, l'utilizzo di tre delatori confidenti: Francesco Maria Vilardi, Francesco Graziano e soprattutto Celestino da Verona. La storiografia ricostruisce ormai con una certa sicurezza⁴ il ruolo di spia di Celestino, il cui scopo, come ben si comprende dalle

1. È possibile leggere la descrizione dell'esecuzione e dell'assistenza prestata a Giordano Bruno nell'Archivio di Stato di Roma, Fondo San Giovanni Decollato, vol. XVI, c. 87r.

2. Per una suggestiva riflessione contemporanea sulla comune origine cosmica della materia si confronti ROVELLI 2014, ove si sottolinea come gli atomi di cui siamo composti abbiano avuto origine nei processi stellari e come la fisica moderna dissolva ogni pretesa di separatezza ontologica tra l'umano e il cosmo.

3. Per la ricostruzione documentaria del processo e delle sue fasi si vedano: DEI 2000 e GHEZZI 2011. Mentre per una lettura critica aggiornata del procedimento e delle sue implicazioni teologiche, giuridiche e politiche: MAIFREDA 2018.

4. Si veda MAIFREDA 2016.

notizie sulla sua incarcerazione⁵ nello stesso luogo del filosofo, era proprio quello di captare e annotare tutte le dichiarazioni, le confidenze, i pensieri che Bruno faceva durante la detenzione. Effettivamente, senza le informazioni captate dal frate i giudici non sarebbero mai riusciti a condannare Giordano Bruno. Del resto il processo era iniziato a seguito di denunce segrete, sicché l'iniziativa inquisitoria non nasce da un fatto colto nell'immediatezza, bensì dalla delazione e dalla trattazione di informazioni riferite.

La vicenda di Bruno, lungi dall'essere un episodio isolato, esprime un paradigma più ampio: la captazione occulta di informazioni risulta essere una tecnica ordinaria della giurisdizione premoderna. In questi procedimenti l'*inquisitio* agisce d'ufficio, raccoglie deposizioni, interroga, seleziona elementi. La verità processuale prende forma attraverso una progressiva accumulazione di informazioni captate in modo sproporzionato e segreto, che vengono poi opposte all'indagato spingendolo, utilizzando anche la tortura, alla confessione. In questo quadro, la confessione non è che l'esito finale di una asimmetria cognitiva. Il sospetto legittima l'indagine; l'indagine alimenta la raccolta segreta delle informazioni; la raccolta segreta orienta l'interrogatorio; l'interrogatorio produce la confessione. Il processo, così strutturato, non tende a scoprire la verità; al contrario, la crea.

Prima ancora che l'illuminismo giuridico producesse i diritti inviolabili, prima che si affermasse un diritto soggettivo alla riservatezza delle comunicazioni, l'autorità procedente disponeva di strumenti legittimati, sia dalla prassi che dalla dottrina, per penetrare la sfera privata dell'indagato attraverso delazione, infiltrazione, lettura della corrispondenza, protezione delle fonti.

Se si guarda a questo quadro con la distanza storica necessaria, l'impressione di radicale novità che

accompagna oggi il dibattito sul captatore informatico appare meno netta. Il c.d. trojan di Stato⁶ consente all'autorità giudiziaria di accedere da remoto al dispositivo elettronico dell'indagato, di attivarne microfoni e telecamere, di acquisire comunicazioni e dati archiviati, di monitorare in tempo reale le interazioni digitali. Si diffonde l'idea che l'informatica abbia introdotto una forma di intrusione qualitativamente inedita, capace di alterare l'equilibrio tra potere investigativo e diritti fondamentali. Eppure, al di là del mutamento tecnologico, la logica sottostante alle diverse forme di acquisizione di dati presenta elementi di continuità evidenti. Anche nel caso del captatore informatico l'accertamento si fonda su un'asimmetria informativa: l'indagato ignora l'attività di monitoraggio; l'autorità raccoglie dati in segreto; la conoscenza precede il confronto processuale. Mutano gli strumenti, non la struttura del dispositivo. Come il confidente nel processo inquisitorio, così il malware investigativo agisce all'interno dello spazio privato, raccogliendo informazioni che verranno successivamente tradotte in prova.

Nella società digitale l'attività investigativa non si limita alla captazione del contenuto delle comunicazioni, ma investe, invero non diversamente da quanto avveniva con il delatore, una molteplicità di dati esterni, localizzativi, comportamentali che, considerati singolarmente, possono apparire neutri, ma che, se raccolti ed elaborati nel loro insieme, consentono di ricostruire un profilo dettagliato dell'individuo. La distinzione tradizionale tra intercettazione e acquisizione documentale tende così ad attenuarsi; lo stesso concetto di comunicazione appare meno stabile; il confine tra captazione in tempo reale e acquisizione di dati già formati si fa più incerto.

In questo scenario, l'innovazione tecnologica procede più rapidamente della produzione

5. Più che di incarcerazione dovrebbe parlarsi di vero e proprio incarico ricevuto da Celestino, visto che negli annali dei frati Cappuccini veneti, ordine di cui il frate era membro, si legge: "Illustrissimi Signori sopra il Sant'Ufficio di Venetia mandarono a chiamare Fra Celestino da Verona, chierico, e lo posero nelle carceri della Santa Inquisizione". Si veda l'Archivio provinciale dei Cappuccini veneti, Annali, A-BB, c. 12r. Il brano è citato da MAIFREDA 2018 p. 138.

6. Sul captatore informatico vi è una letteratura vastissima, mi limito a richiamare l'analisi riassuntiva e completa del Trojan di Stato effettuata da Roberto Flor in FLOR-MARCOLINI 2022. Sul captatore informatico quale strumento ad elevata intrusività, tra esigenze investigative e tutela delle libertà costituzionali: GIORDANO 2020. In chiave critica, con riguardo alla natura *bifronte* dello strumento e alla sua utilizzabilità anche in funzione esplorativa e preventiva: NOCERINO 2020.

normativa, le prassi investigative anticipano il legislatore; la disciplina interviene spesso in modo frammentario; la giurisprudenza è chiamata a colmare vuoti interpretativi che incidono direttamente sull'ampiezza delle garanzie processuali⁷. Se nella stagione inquisitoria la segretezza costituiva la regola dell'accertamento, l'età costituzionale ha tentato di rovesciare quella logica, sottoponendo l'acquisizione occulta a limiti formali, controlli giurisdizionali e garanzie sostanziali; in questo senso, il captatore informatico si colloca evidentemente in un'area di tensione, essendo uno strumento altamente invasivo. Esso impone di interrogarsi sulla sua qualificazione giuridica e, di conseguenza, sul regime di limiti e controlli applicabile. Tuttavia, proprio mentre il diritto cerca di circoscrivere la captazione entro confini rigorosi, la tecnologia digitale ne espande in modo esponenziale le potenzialità. La raccolta massiva di dati, l'aggregazione algoritmica delle informazioni, la possibilità di monitoraggio continuo dello spazio digitale rendono sempre più sottile la linea di equilibrio tra sicurezza e libertà⁸. La tensione che ne deriva non è contingente, ma strutturale: quanto più cresce la capacità tecnica di conoscere, tanto più si intensifica il rischio di un ritorno a forme di controllo fondate sull'asimmetria informativa e sulla segretezza dell'accertamento.

In questa frizione tra disciplina costituzionale e potenza tecnologica si gioca il problema contemporaneo del captatore informatico. La genealogia qui ricostruita non mira a suggerire un'impropria equivalenza tra passato e presente, ma a mettere in luce una dinamica ricorrente: quando la sicurezza tende a prevalere senza adeguati contrappesi, il processo si avvicina a modelli nei quali la verità è prodotta nel segreto e solo successivamente resa pubblica. È su questa linea di tensione – tra garanzia e controllo, tra legalità e sorveglianza – che si colloca la riflessione che segue, volta a ricostruire la lunga storia della captazione delle informazioni

nel processo penale e le forme attraverso cui il diritto ha tentato, nel tempo, di disciplinarne la potenza.

2. Una questione di sicurezza: l'intercettazione durante l'*ancien régime*

Se nell'età digitale l'innovazione tecnologica impone di interrogarsi sulla tenuta delle categorie giuridiche tradizionali: comunicazione, domicilio, documento, intercettazione, etc., nell'*ancien régime* un simile problema teorico non viene avvertito, e ciò non soltanto perché mancano i diritti soggettivi nel senso moderno, in particolare le garanzie processuali, ma perché l'orizzonte che orienta l'azione del giudice è diverso; ciò che legittima l'indagine non è il bilanciamento tra libertà e potere, bensì l'esigenza primaria di preservare l'ordine. Che si tratti della stabilità del sovrano e dell'assetto politico o, nel caso del Santo Uffizio, della tutela dell'ortodossia cattolica, la sicurezza costituisce il fondamento implicito e sufficiente dell'intervento giurisdizionale. In questo quadro, allora, la captazione occulta delle informazioni non è percepita come frattura dell'ordine giuridico, ma come sua naturale estensione. Non vi è l'esigenza di *produrre* nuove categorie per disciplinare strumenti particolarmente invasivi, giacché la tutela dell'ordine religioso e politico è ritenuta, di per sé, principio idoneo a giustificare l'impiego. Del resto, il *paradigma della sicurezza* legittima per lungo tempo l'uso processuale dell'acquisizione delle informazioni *con ogni mezzo* sino all'entrata in vigore della nostra Costituzione.

Sebbene il tema delle intercettazioni sia già presente nell'antichità, per ovvie questioni di spazio mi limiterò a una rapida analisi del funzionamento della captazione presso il procedimento inquisitorio per eccellenza, il già richiamato processo della Santa Inquisizione⁹. Come è noto, in

7. Sul progressivo ampliamento dell'oggetto dell'indagine digitale e sulla crisi del concetto tradizionale di comunicazione, rimando agli approfondimenti: DI PAOLO 2025 e CAMON 2025.

8. Per una riflessione sulle trasformazioni del diritto penale nell'era dell'intelligenza artificiale, tra esigenze di prevenzione, rischio di espansione punitiva e crisi del paradigma individualistico della colpevolezza: PANATTONI 2025.

9. In questa sede non è possibile offrire neppure un quadro sintetico della vasta storiografia sull'Inquisizione. Senza pretesa di completezza, segnalo per un inquadramento generale dell'Inquisizione romana: DEL COL-PAOLIN 1991. Mentre, su alcuni aspetti specifici, richiamati nel presente contributo: ERRERA 2018, che riflette sulla fase iniziale della *inquisitio generalis* e sul nesso strutturale tra predicazione e procedimento inquisitorio. Sul modello

questo processo si realizza in forma paradigmatica la giustizia egemonica di apparato¹⁰: l'azione è promossa d'ufficio, il procedimento non è rimesso alla disponibilità delle parti e la figura del giudice, con il suo ampio *arbitrium*, diviene centrale nella formazione e nella raccolta delle prove. L'istruttoria, interamente scritta, si fonda su denunce spesso segrete, testimonianze e interrogatori; la confessione vi assume il ruolo di prova regina e può essere ottenuta anche mediante il ricorso alla tortura, concepita come strumento tecnico di perfezionamento probatorio. In questo quadro, la raccolta segreta di dati rientra nella fisiologia dell'apparato repressivo, coerente con un sistema che identifica nella sicurezza dell'ordine il proprio fondamento legittimante.

La finalità del processo inquisitorio non si esaurisce nell'accertamento di un fatto, ma mira alla costruzione di una verità giudiziaria formalmente valida, prodotta secondo canoni tecnici prestabiliti il cui fine è garantire la sicurezza della Chiesa e della fede. La procedura diviene così una vera e propria operazione di intelligence¹¹ *ante litteram*: non semplice scoperta di un dato preesistente, bensì organizzazione, selezione e talora riplasmazione delle informazioni fino alla loro stabilizzazione in una verità processuale. Le pratiche di acquisizione occulta delle informazioni costituiscono uno dei tratti distintivi di questo modello processuale; e ciò risulta evidente già dalle stesse fonti del processo inquisitorio. Le decretali pontificie antiereticali ne definiscono l'impianto normativo; il diritto comune romano-canonico ne struttura categorie e regole probatorie; la manualistica inquisitoriale ne disciplina in concreto l'*ordo procedendi*; infine, la

prassi notarile di verbalizzazione fissa per iscritto denunce, testimonianze e confessioni, stabilizzando la verità giudiziaria prodotta dall'istruttoria.

Già nella sua fase originaria, il processo inquisitorio mostra come l'intercettazione costituisca il presupposto indispensabile dell'azione giudiziaria. La normativa canonica del XIII secolo, agli albori del processo, richiedeva infatti che l'*inquisitio* fosse preceduta da una previa *infamia* o da una *clamorosa insinuatio*; così, ad esempio, la decretale *Licet Heli* di Papa Innocenzo III, nel 1199, stabiliva che il procedimento per inquisizione dovesse essere preceduto da *pubblica insinuazione*¹²; mentre la *Inquisitionis negotium* del 1212 ribadiva che "*inquisitio fieri debeat solummodo super illis, de quibus clamores aliqui praecesserunt*"¹³.

Successivamente, un altro Papa, Gregorio IX, nel 1233 completò il quadro normativo codificando la prassi della *praedicatio generalis* affidata agli inquisitori. La predicazione era un vero e proprio dispositivo giuridico-processuale, infatti l'inquisitore, in quanto frate predicatore, apriva la propria missione con un sermone pubblico sull'ortodossia e con l'editto di fede, con cui si intimava ai fedeli di denunciare, entro un termine stabilito, notizie relative a dottrine sospette o a persone coinvolte, sotto pena di scomunica. In questo modo si dava avvio alla fase dell'*inquisitio generalis*: attraverso di essa si sollecitava la raccolta delle informazioni e si attivava il circuito delle delazioni, trasformando il sermone in uno strumento preliminare di acquisizione della *notitia criminis* necessaria all'avvio del procedimento. Con il successivo *tempus gratiae sive indulgentiae* (15-30 giorni), le confessioni e le delazioni spontanee fornivano all'inquisitore le

processuale inquisitorio e sul rapporto tra *inquisitio* e tortura: SBRICCOLI 1991. Per una riflessione ampia sulla centralità della confessione nel processo e sui *miti inquisitori* nella costruzione della verità processuale LUPARIA-MARAFIOTI 2015 e più nel dettaglio GARLATI 2015. Infine, per un approfondimento della prospettiva probatoria CHIODI 2013.

10. Sulla categoria di "giustizia egemonica", intesa come modello di giustizia penale di apparato fondato sulla pubblicizzazione dell'azione, sulla centralità della legge, sull'ufficiosità del processo inquisitorio e sulla funzione repressivo-esemplare della pena, SBRICCOLI 2002.
11. Sul concetto di intelligence come processo strutturato di raccolta, selezione e analisi delle informazioni finalizzato all'assunzione di decisioni strategiche, e non come mera attività di acquisizione di dati: CALIGIURI 2025.
12. Secondo la disciplina canonica l'indagine giudiziaria poteva essere avviata a seguito di una notizia di reato che avesse un clamore sociale sufficientemente qualificato. Proprio la diffusione di tale informativa era il presupposto di legittimità per l'azione del giudice.
13. Innocentius III, *Inquisitionis negotium* (1212), in *Compilatio IV*, V, 1, 2, poi confluita in *Liber Extra* (X, 5, 1, 21).

informazioni necessarie per passare dall'*inquisitio generalis* all'*inquisitio specialis*, ossia il procedimento contro soggetti determinati.

Fin dalle origini, dunque, la raccolta e l'organizzazione delle notizie costituirono il presupposto strutturale di legittimità ed efficacia del processo inquisitorio.

La parola, o meglio il dato comunicativo, il passaggio di informazioni è al centro del processo inquisitorio. Tra XII e XIII secolo si registra una vera e propria *emersione della parola*: il nuovo modello processuale fondato sull'iniziativa officiosa del giudice attribuisce alla delazione e denuncia prima, e alla deposizione trascritta e sottoscritta dell'imputato, dopo, un ruolo decisivo, sino a fare della confessione la prova piena per eccellenza e della tortura un ordinario meccanismo di pressione durante l'interrogatorio¹⁴. La verità non viene semplicemente attestata attraverso strumenti probatori esterni, ma viene ricercata, sollecitata da intercettazioni (con l'aiuto di delatori e confidenti) e dalla tortura dell'imputato, e formalizzata mediante un dispositivo tecnico che si basa sulla verbalizzazione rigorosa delle domande e delle risposte. In questa centralità

della parola estorta, registrata e stabilizzata per iscritto, si coglie il cuore epistemologico del processo inquisitorio.

Accanto al *corpus* normativo del diritto canonico il processo viene disciplinato dai vari manuali inquisitoriali¹⁵ che nel dettaglio illustravano le prassi e le regole procedurali da seguire in concreto nel processo, queste opere, scritte da coloro che svolgevano la funzione di giudice, erano nate dall'esigenza di colmare le lacune della legislazione e di offrire strumenti operativi ai frati predicatori investiti dell'ufficio giudiziario. Tra i principali manuali medievali¹⁶ si può annoverare il *Directorium inquisitorum* di Nicolas Eymerich del 1376, destinato a divenire il modello di riferimento per tutta l'età moderna, considerato anche il commento tardo cinquecentesco del giurista Francisco Peña. Nel *Directorium*¹⁷ si rinviene una figura, a mio parere, assimilabile al confidente in senso moderno, ossia a un informatore stabilmente infiltrato e organicamente integrato nell'apparato giudiziario. La prassi indicata dal frate inquisitore presuppone e disciplina, infatti, un sistema organico di raccolta informativa che svolge quasi una funzione analoga a quella che oggi è svolta da un agente sotto copertura¹⁸.

14. Sul progressivo emergere della parola quale fulcro del processo inquisitorio, sulla centralità della confessione come prova piena e sulla funzione della tortura nell'interrogatorio: TAVILLA 2021.

15. Sulla funzione sistematica dei manuali inquisitoriali quali strumenti di formalizzazione dei procedimenti, di tipizzazione delle fattispecie ereticali e di regolazione tecnica dell'interrogatorio e della prova: ERRERA 2010. In modo più ampio, ERRERA 2000, ove si ricostruisce la progressiva tecnicizzazione della prassi inquisitoriale in età moderna, mostrando come i manuali non si limitino a recepire la normativa canonica, ma la rielaborino in chiave operativa, offrendo modelli di interrogatorio, schemi di verbalizzazione e criteri di valutazione della prova funzionali alla costruzione della verità processuale.

16. Tra i manuali più diffusi ricordo: il *Directorium* del 1242 di Raimondo di Penyafort, il *De inquisitione haereticorum*, attribuito a David d'Augusta (sec. XIII); Bernardo Gui e il suo *Practica inquisitionis heretice pravitatis* (1323-1324); il *Tractatus de haereticis* di Zanchino Ugolini (1330 ca.).

17. I passi citati in latino sono tratti da EYMERICI 1376, edizione romana del 1587, che si trova facilmente sul web. Stampata per iniziativa della tipografia camerale del Popolo Romano, costituisce la redazione post-tridentina del testo eymerichiano, arricchita da Francisco Peña. Per una lettura antologica e moderna di parti significative dell'opera si veda SALA-MOLINS 1973 che propone una sintesi commentata del trattato, cercando di restituirne integralmente la complessa stratificazione testuale.

18. Sulla figura dell'agente sotto copertura e sulla problematica della testimonianza resa sotto identità fittizia nel processo penale contemporaneo, si veda BIRAL 2023, ove si analizzano funzione, limiti e disciplina della deposizione dell'agente. In prospettiva storico-giuridica, è significativo osservare che nel *Directorium inquisitorum* non si rinviene una figura formalmente assimilabile all'agente infiltrato; tuttavia il manuale legittima la segretezza dei testimoni, l'assenza ordinaria di confronto con il reo e la gestione separata delle deposizioni, nonché la strutturazione e l'orientamento dei *delatores*. Ne risulta un modello nel quale la protezione dell'identità della fonte e l'asimmetria cognitiva costituiscono

Come previsto dalle fonti normative già analizzate, la raccolta della *notitia criminis* si fonda anzitutto sul circuito della *denuntiatio* e della *delatio*, e viene trattata come atto da organizzare e verificare proceduralmente. Non a caso si prescrive che i “*delatores interrogandi sunt ab inquisitoribus qua ratione et modo procedere velint*”, la fonte informativa non è un dato spontaneo, ma un materiale da vagliare, orientare e incanalare nell'economia dell'*inquisitio*. Parallelamente, il manuale legittima una segretezza strutturale nella gestione delle testimonianze. In materia di eresia la *confrontatio* con l'imputato non è ordinariamente ammessa, poiché la rivelazione dell'identità dei testi violerebbe il “*secretum quod circa testes haberi praecipitur*”. La protezione dell'identità del testimone è dunque regola, non eccezione. È in questa architettura normativa, fondata sull'asimmetria cognitiva e sulla non pubblicità della fonte, che diventa storicamente possibile l'impiego di figure come Celestino da Verona nel processo Bruno; non perché il *Directorium* tipizzi l'infiltrato, ma perché legittima la segretezza della fonte e l'assenza di contraddittorio nella fase acquisitiva.

Ancora più significativa è la disciplina della testimonianza. Per *favore fidei* l'inquisitore può costringere chiunque a giurare e a deporre sulla verità dei fatti “*in crimine haeresis quoscunque... compellendos esse ad iurandum de dicenda veritate*” ed è legittimato a reiterare l'esame qualora la deposizione risulti incompleta o confusa: “*si testes confuse deposuerint... iterato cum eis inquirat*”.

La captazione è qui tecnica processuale: la verità non è semplicemente raccolta, ma progressivamente costruita attraverso l'organizzazione, la reiterazione e, se necessario, la coercizione della fonte.

La prassi descritta dal giudice restituisce così un modello in cui l'acquisizione di dati non è tecnologica ma normativa. Non vi sono intercettazioni in senso moderno, vi è però un apparato che rende ogni fedele potenziale vettore di informazione, tutela la segretezza dei testimoni, sanziona l'occultamento e struttura proceduralmente la circolazione delle notizie.

Un sistema così costruito rimane coerente finché la sicurezza dell'ordine religioso e politico costituisce

il fondamento sufficiente dell'intervento giudiziario. Quando, tra XVII e XVIII secolo, l'orizzonte teorico muta e l'Illuminismo giuridico pone al centro non più la stabilità dell'apparato ma la libertà dell'individuo, l'intero edificio inquisitorio entra in crisi. La segretezza dell'istruttoria, l'anonimato delle fonti, la centralità della confessione e l'uso della tortura – prima strumenti fisiologici di protezione dell'ordine – diventano incompatibili con una nuova concezione del processo fondata sul contraddittorio, sulla pubblicità e sulla limitazione del potere punitivo. È in questo passaggio, dalla sicurezza come principio legittimante alla tutela dei diritti come criterio ordinatore, che si prepara la stagione delle riforme settecentesche e, successivamente, la codificazione ottocentesca del processo penale.

3. Ordine, sicurezza e limite: la captazione delle informazioni nell'età delle codificazioni

La crisi del paradigma inquisitorio non conduce alla scomparsa delle tecniche di captazione delle informazioni, bensì alla loro trasformazione giuridica. Con l'emergere del costituzionalismo moderno si pone per la prima volta in termini sistematici il problema dell'acquisizione, da parte dello Stato, di informazioni mediante strumenti invasivi. Ciò che in precedenza era considerato fisiologico nell'esercizio della giurisdizione diviene ora oggetto di scrutinio critico: al potere pubblico non è negata in sé la possibilità d'intercettare segretamente dati a fini processuali, ma ci si interroga sui limiti entro cui tale attività possa essere esercitata e sulle garanzie necessarie a renderla compatibile con la tutela delle nuove libertà individuali.

È tuttavia significativo che le prime dichiarazioni dei diritti e le conseguenti costituzioni non conoscano ancora un'esplicita tutela della riservatezza o della segretezza delle comunicazioni. Basti pensare alla *Dichiarazione dei diritti dell'uomo e del cittadino* del 1789, che di certo non contiene disposizioni dirette a proteggere la corrispondenza privata. La preoccupazione primaria è la libertà personale, la sicurezza, la legalità della pena; pertanto la dimensione comunicativa della

condizioni fisiologiche dell'accertamento, anticipando la tensione moderna tra sicurezza investigativa e garanzie difensive.

persona è trattata solo alla luce della libertà di opinione e di stampa¹⁹.

I diritti fondamentali, piuttosto, introducono un concetto che il giudice del Santo Ufficio conosce: il limite. Nel modello di antico regime la sicurezza dell'ordine costituiva fondamento sufficiente dell'azione giudiziaria, nel paradigma della modernità giuridica, invece, essa deve confrontarsi con diritti che precedono e vincolano il potere. La verità non può più essere prodotta attraverso un'asimmetria radicale, ma deve emergere entro un sistema di garanzie. Nel Settecento la crisi degli istituti del processo inquisitorio – *intercettazione*, tortura, confessione – coincide con la rottura del nesso epistemologico tra corpo, dolore e verità, e con l'affermazione dell'idea che il giudice debba limitarsi a stabilire una verità formale, costruita nel rigoroso rispetto delle regole processuali²⁰. In questo nuovo quadro, la captazione delle informazioni non scompare, viene sottoposta a legalità. La modernità giuridica non elimina l'intercettazione, la incardina in un sistema di autorizzazioni, controlli giurisdizionali e garanzie difensive. L'invasività diventa oggetto di bilanciamento tra sicurezza e libertà, tra esigenze investigative e diritti individuali. La logica non è più quella dell'ordine che assorbe ogni limite, ma quella del limite che disciplina l'ordine. Il processo penale ottocentesco, nelle sue codificazioni, traduce questa trasformazione in regole positive: pubblicità, contraddittorio, diritto al confronto con l'accusatore, tipizzazione dei mezzi di prova, esclusione della tortura. La captazione diviene gradualmente potere condizionato alla legge, e non più fisiologia incontestata dell'apparato.

Tale trasformazione si coglie con particolare chiarezza nelle codificazioni degli Stati italiani

preunitari. Nel *Codice di procedura penale per il Regno delle Due Sicilie* del 1819²¹, l'acquisizione dei dati è espressamente affidata alla polizia giudiziaria, cui *spetta investigare e scovire i reati, raccoglierne le prove* (art. 8), secondo competenze e forme rigorosamente tipizzate (artt. 13-23), con verbalizzazione obbligatoria degli atti (artt. 10-11). Anche la fase genetica dell'istruzione è regolata attraverso una disciplina dettagliata dei rapporti e delle denunce (artt. 24 ss.), mentre la delazione anonima è dichiarata irricevibile, salvo i soli casi di flagranza o di fatto permanente (art. 28), segnando così un evidente ridimensionamento delle pratiche più proprie del paradigma inquisitorio. Nei reati perseguibili a istanza di parte (artt. 38 ss.), l'azione penale stessa è condizionata alla volontà dell'offeso, con possibilità di rinuncia entro termini determinati (artt. 43-48). Tuttavia, in questo assetto non si rinviene ancora un riconoscimento espresso della segretezza delle comunicazioni quale diritto soggettivo inviolabile: la captazione e l'acquisizione di documenti sono concepite come attività investigative sottoposte a competenza e ritualità, non come eccezioni a una libertà costituzionalmente garantita. In questo senso, pur entro un quadro procedimentalizzato, sembra ancora prevalere la necessità della sicurezza sul diritto alla segretezza delle proprie comunicazioni. L'ordine pubblico continua a costituire il fondamento implicito dell'azione giudiziaria, mentre il limite della riservatezza non è ancora radicato in una sfera di diritti anteriori e vincolanti per il potere, ciò vale, ovviamente, anche per altri diritti processuali, sicché si può affermare che nei codici preunitari la legalità c'è, ma è una *legalità dell'apparato*, non ancora *legalità dei diritti*.

Un ulteriore riscontro della persistenza dei paradigmi della sicurezza e della ricerca della

19. Tali diritti furono tuttavia immediatamente limitati da Napoleone e, con la Restaurazione, anche negli ordinamenti italiani. Cfr. SCHIRÒ 2025.

20. Sul significato sistematico della tortura entro il modello inquisitorio, quale luogo di tensione tra esigenza di accertamento e costruzione di limiti giuridici all'*arbitrium iudicis*, cfr. PIFFERI 2019. L'autore evidenzia come l'elaborazione dottrinale delle regole sulla tortura costituisca al contempo strumento di legittimazione e tentativo di contenimento del potere giudiziale.

21. Si prende qui in esame il Codice per lo Regno delle Due Sicilie poiché si inserisce pienamente nel solco del modello processuale di matrice napoleonica, che rappresenta il principale punto di riferimento per le codificazioni europee e italiane del primo Ottocento. Le soluzioni adottate dalla legislazione borbonica risultano pertanto ampiamente rappresentative delle tecniche normative diffuse negli ordinamenti della penisola prima dell'unificazione. In generale, per un approfondimento dei processi che condussero alla codificazione penalistica siciliana, si veda MASTROBERTI-MASIELLO 2020.

verità processuale, pur entro una cornice di legalità formale, emerge se si guarda alle previsioni del codice penale emanato nello stesso anno. Qui la questione delle intercettazioni, e più in generale della circolazione delle informazioni, non è tematizzata come problema di libertà individuali. Non viene cioè costruita una sfera autonoma di segretezza opponibile al potere pubblico, né si concepisce la captazione come eccezione da giustificare mediante un bilanciamento tra esigenze investigative e diritti fondamentali. Al contrario, la codificazione assume come dato incontrovertibile la fisiologia dell'acquisizione di notizie da parte dell'apparato, ciò che merita attenzione non è l'invasività dell'indagine in sé, bensì l'affidabilità del circuito informativo che alimenta l'azione giudiziaria. La scelta di campo è rivelatrice. In un ordinamento ancora lontano dalla piena maturazione del costituzionalismo delle libertà, la preoccupazione primaria non è proteggere il privato dall'invasività del potere giudiziario, ma impedire che il processo, fondato strutturalmente su denunce, testimonianze, rapporti, verbalizzazioni, venga inquinato da informazioni calunniose, anonime o fabbricate ad arte. È per questo che la disciplina penale interviene soprattutto a reprimere gli abusi della fonte informativa, punendo la falsa denuncia quando il delatore attribuisca a taluno un misfatto inesistente o comunque riferisca il falso (art. 69); colpendo la denuncia anonima realizzata mediante foglio privo di sottoscrizione, considerata comportamento socialmente pericoloso e tipico veicolo di calunnia (art. 166); reprimendo con particolare severità la fabbricazione di falsi testimoni e la falsa testimonianza (artt. 187-188), punendo chi apriva o sopprimeva plichi postali (art. 251). In tutte queste norme il legislatore non protegge la comunicazione privata; protegge, invece, la macchina giudiziaria, cioè la sua capacità di produrre una verità formalmente valida senza essere deviata da un uso fraudolento dell'informazione²².

Il dato è tanto più significativo se letto in continuità con le regole procedurali già richiamate. Da un lato, la procedura del 1819 tipizza competenze, attribuisce alla polizia giudiziaria la funzione di investigare e raccogliere prove, disciplina rapporti e denunce, e limita la delazione anonima; dall'altro, il codice penale interviene a valle sul medesimo circuito, sanzionando chi lo altera. Ne risulta un sistema coerente: l'informazione è la linfa dell'azione repressiva, e l'ordinamento si preoccupa soprattutto della sua attendibilità e della sua *qualità* come materiale processuale, non della sua provenienza potenzialmente lesiva di una sfera privata inviolabile.

Il quadro non cambia se si prendono in considerazione le norme che vengono promulgate alla metà del secolo, come i codici albertini del 1859²³ che trovano applicazione alla vigilia dell'Unità d'Italia. Anche qui, non emerge ancora una vera e propria tutela della segretezza delle comunicazioni come diritto soggettivo.

Non sorprende, in questo quadro, che la questione della segretezza delle comunicazioni rimanga a lungo collocata al di fuori delle codificazioni penali e processuali, trovando piuttosto disciplina nella normativa amministrativa relativa al funzionamento dei servizi postali. La libertà di comunicare segretamente nasce infatti storicamente come situazione giuridica efficace soprattutto nei rapporti tra privati, legata alla circolazione di corrispondenza epistolare in ambito commerciale e alla necessità di proteggere il contenuto delle lettere rispetto a terzi. In antico regime la segretezza delle lettere non è concepita come diritto soggettivo inviolabile opponibile allo Stato, così, nelle monarchie europee erano ben disciplinati meccanismi pubblici di controllo della corrispondenza. Nella Francia del XVII secolo, vi era l'istituzione del *cabinet noir*, ufficio incaricato di controllare e riferire sul contenuto delle corrispondenze di alcune persone sorvegliate dalla polizia²⁴; analoghe pratiche

22. Norme del tutto simili si trovano negli altri codici penali, si veda l'articolo 257 del codice penale per il Ducato di Parma, Piacenza e Guastalla del 1820; o gli articoli 364 e 365 del Codice penale del 1853 del Granducato di Toscana, o ancora il codice estense del 1855 al suo articolo 266. L'impostazione dei codici italiani seguiva lo schema napoleonico. Sul debito italiano verso il modello francese e il successivo allontanamento liberale dalle misure più reazionarie della codificazione transalpina rimando a MILETTI 2006.

23. Per alcuni approfondimenti sulla codificazione penale sardo piemontese: VINCIGUERRA 2009.

24. Secondo GILLS 1927, il controllo della corrispondenza privata da parte dell'autorità pubblica viene per la prima volta regolato da una *ordonnance* di Luigi XI del 10 novembre 1454 che prevede "I corrieri e messaggeri

erano diffuse anche in Inghilterra, dove l'apertura delle lettere da parte delle autorità era ampiamente tollerata. Il controllo sulle comunicazioni private costituiva, quindi, nella logica della sicurezza, uno strumento fondamentale per la tutela dello Stato. L'illuminismo giuridico e la Rivoluzione francese affermano per la prima volta un principio esplicito di inviolabilità della corrispondenza²⁵: la legge del 10-11 giugno 1791 abolì i *cabinets noirs* e proclamò che "le secret des lettres est inviolable et, sous aucun prétexte, il ne peut y être porté atteinte ni par les individus ni par les corps administratifs". Tuttavia, lo sviluppo della tutela non fu lineare: il sistema di controllo delle lettere fu ripristinato da Napoleone con il *Bureau de révision* e nuovamente confermato durante la Restaurazione²⁶. In Italia, gli Stati preunitari si dotarono di diversi strumenti volti a garantire la sicurezza dell'ordine politico in un contesto segnato da congiure e movimenti rivoluzionari. In tale quadro il controllo della corrispondenza costituì uno degli strumenti utilizzati dall'autorità di polizia, anche se la relativa disciplina raramente trovava spazio in normazioni specifiche ed esplicite²⁷.

Sfogliando i regolamenti amministrativi che disciplinavano il servizio postale negli Stati italiani preunitari si rinvenivano disposizioni che affermano espressamente il principio della segretezza

della corrispondenza. Un esempio significativo è offerto dall'art. 65 del Regio Editto sull'amministrazione delle Regie Poste del 1836 emanato da Carlo Alberto di Savoia, che sancisce "il segreto della corrispondenza" quale obbligo per gli impiegati dell'amministrazione postale²⁸. Tale principio, tuttavia, non assume ancora la fisionomia di una libertà individuale inviolabile, poiché resta suscettibile di deroghe motivate da esigenze di sicurezza o di interesse pubblico. Il controllo delle comunicazioni rimane una prerogativa che lo Stato continua a esercitare in nome dell'ordine pubblico, mentre la tutela della riservatezza epistolare opera soprattutto nei rapporti tra privati o come obbligo imposto agli agenti dell'amministrazione postale. Solo nella seconda metà del secolo, con la maturazione del costituzionalismo liberale e con la progressiva affermazione dei diritti della persona, la segretezza delle comunicazioni inizierà a trasformarsi da interesse amministrativamente protetto in vera e propria libertà individuale opponibile al potere pubblico e inserita nel sistema delle garanzie legali. Sarà il progresso tecnologico, con l'introduzione delle comunicazioni a distanza, dal telegrafo al telefono, a porre in termini nuovi il problema della captazione delle comunicazioni all'interno del processo penale, facendo emergere la figura dell'intercettazione come oggi la conosciamo e imponendo

saranno visitati da commessi del gran Maestro, ai quali dovranno mostrare le loro lettere e denari, per conoscere se non vi ha nulla che porti pregiudizio al servizio del re", p. 5.

25. La legislazione rivoluzionaria francese afferma esplicitamente il principio secondo cui "Le secret des lettres est inviolable", in Italia la Costituzione del Regno delle Due Sicilie del 1848 prevede all'articolo 29 una disposizione simile, mentre lo Statuto Albertino non menziona affatto tale diritto.
26. BARILE-CHELI 1962, sul punto precisano che "Anche in tempi anteriori è dato reperire nelle legislazioni dei vari Stati alcuni riconoscimenti frammentari del principio della segretezza della corrispondenza epistolare: ma la tutela è concessa, normalmente, soltanto nei confronti dei fatti illeciti commessi da privati, senza considerare la possibilità di abusi dei pubblici poteri", p. 746.
27. Sul punto è interessante leggere la Convenzione postale stipulata il 4 settembre del 1822 tra il Granducato di Toscana e l'Austria, nella quale si prevede che tutte le lettere che dalla Toscana sono destinate all'estero passino prima sotto il controllo delle Imperiali poste austriache (il testo della convenzione è facilmente reperibile online). Accordi simili erano presenti anche negli altri Stati italiani sottoposti al controllo austro-ungarico.
28. Disposizioni analoghe si rinvenivano anche in altri ordinamenti europei e italiani della prima metà dell'Ottocento. I regolamenti amministrativi delle poste affermano generalmente il principio del segreto della corrispondenza quale obbligo imposto agli impiegati del servizio postale, pur lasciando margini di intervento all'autorità pubblica per ragioni di sicurezza. Norme di questo tipo sono presenti, ad esempio, nei regolamenti postali del Regno Lombardo-Veneto e dello Stato pontificio, nonché nella legislazione francese e austriaca. In tali disposizioni la segretezza epistolare appare tuttavia concepita soprattutto come obbligo amministrativo degli agenti della posta, più che come diritto fondamentale pienamente opponibile allo Stato.

una tutela che riguarda i limiti entro cui l'autorità pubblica può accedere alle comunicazioni dei cittadini.

4. Ascoltare per prevenire.

Le intercettazioni nel primo Novecento

“Badate, carissimi Fratelli in Cristo, e non dimenticate che ben spesso vi sono osservatori o delatori (dite spie e direte il vero), che, per zelo proprio o per incarico avuto, vi ascoltano per denunciarvi [...] ...vi diciamo e raccomandiamo istantaneamente: non affidate mai al telefono ciò che vi preme che non si sappia. Voi credete che la vostra parola vada senz'altro al lontano corrispondente, e invece essa, a un certo punto, viene avvertita e intercettata”²⁹.

Con queste parole Pio XI metteva in guardia dal rischio che le comunicazioni telefoniche potessero essere ascoltate. Il monito compare in un discorso preparato dal pontefice nel febbraio del 1939, in occasione del decimo anniversario dei Patti Lateranensi, che tuttavia non fu mai pronunciato a causa della morte del papa avvenuta il 10 febbraio dello stesso anno. Il passo è, a mio avviso, particolarmente significativo perché testimonia come ormai negli anni Trenta fosse diffusa, anche ai più alti livelli istituzionali e diplomatici, la consapevolezza della possibile intercettazione delle comunicazioni telefoniche da parte delle autorità pubbliche. In altre parole, ben prima che il tema fosse oggetto di una disciplina giuridica sistematica, la pratica dell'ascolto delle comunicazioni appariva già inserita nella più ampia tradizione dei sistemi di sorveglianza statale, che nel corso del Novecento si sarebbero progressivamente evoluti con lo sviluppo delle tecnologie della comunicazione.

Se fino al XIX secolo il problema giuridico si era concentrato prevalentemente sulla lettura e sul controllo della corrispondenza epistolare, l'introduzione delle comunicazioni elettriche, prima il telegrafo e poi il telefono, modifica profondamente il quadro tecnico e normativo entro cui si colloca l'attività investigativa dello Stato. Le nuove tecnologie consentono infatti una circolazione delle informazioni più rapida, più diffusa e, soprattutto, più facilmente intercettabile da parte dell'apparato pubblico. Il diritto liberale di fine Ottocento si

trova così di fronte a una tensione nuova. Da un lato si afferma con sempre maggiore forza l'idea della segretezza delle comunicazioni come proiezione della libertà individuale; dall'altro le stesse innovazioni tecnologiche rendono tecnicamente possibile una captazione delle conversazioni fino ad allora impensabile, che avviene istantaneamente, tra due soggetti che non sanno di essere intercettati. Ma andiamo con ordine. Il legislatore interviene sulla materia con la legge del 5 maggio del 1862 n. 604, fissando il principio, poi confermato dal Testo Unico delle leggi postali approvato con il Regio Decreto n. 501 del 1899, che afferma che “il segreto delle lettere è inviolabile”. La segretezza delle lettere viene progressivamente estesa anche alle comunicazioni che vengono prodotte attraverso le nuove tecnologie. Sicché anche il legislatore penale agisce sul tema attraverso il codice Zanardelli del 1889, che infatti dedica un capo specifico ai *delitti contro l'inviolabilità dei segreti* (dall'articolo 159 al 164), nel quale viene punita l'indebita intercettazione o rivelazione della corrispondenza privata, comprendendo espressamente anche le comunicazioni telegrafiche. La norma non è rivolta primariamente a limitare il potere pubblico, ma piuttosto a reprimere le interferenze di soggetti privati nella sfera comunicativa altrui. Essa testimonia tuttavia la progressiva percezione della comunicazione come spazio giuridicamente protetto.

Proprio mentre il diritto penale riconosce la segretezza delle comunicazioni come bene giuridico meritevole di tutela, lo sviluppo delle reti telefoniche pone nuovi problemi pratici. Le prime infrastrutture telefoniche funzionano infatti mediante centrali manuali, nelle quali il collegamento tra i diversi utenti è realizzato da operatori che intervengono direttamente nel circuito della comunicazione. Questa struttura tecnica rende l'ascolto delle conversazioni relativamente semplice e, in molti casi, inevitabile. Da qui, il legislatore intervenne con il Regio decreto n. 196 del 1903, recante il primo testo unico delle leggi telefoniche. L'articolo 31 stabiliva che la violazione del segreto delle comunicazioni telefoniche dovesse essere punita secondo le disposizioni già previste dal codice penale per la corrispondenza epistolare e

29. Il testo del discorso è riportato in appendice da FATTORINI 2007. Nel discorso il Papa ribadisce che non usa mai il telefono in quanto certo di poter essere intercettato. Rimando al già citato volume per una ricostruzione del contesto religioso e soprattutto politico del pontificato di Pio XI.

telegrafica. La norma segna un passaggio significativo: il telefono viene definitivamente assimilato alla corrispondenza tradizionale e ricondotto all'ambito della segretezza comunicativa.

Tuttavia, mentre la legislazione afferma la tutela del segreto *tra privati*, il diritto alla segretezza della corrispondenza non può essere fatto valere nei confronti dell'autorità pubblica, infatti, nella prassi amministrativa e investigativa si sviluppano forme sempre più strutturate di ascolto e controllo delle comunicazioni. L'autorità pubblica operava grazie a una interpretazione estensiva dell'articolo 13 del Testo Unico del 1899, che prevedeva la possibilità per l'autorità giudiziaria di sequestrare le lettere affidate alle Poste. Attraverso questo grimaldello legislativo, nei primi decenni del Novecento, l'amministrazione statale istituisce servizi di intercettazione telefonica destinati principalmente al controllo delle comunicazioni di personalità politiche, giornalisti, operatori economici o soggetti considerati rilevanti per la sicurezza dello Stato. Si tratta di attività svolte in modo riservato, spesso al di fuori di una disciplina legislativa esplicita, e riconducibili piuttosto alla sfera delle pratiche di polizia e di intelligence³⁰.

Nel silenzio del legislatore, la scienza giuridica dell'epoca non manca di segnalare le criticità derivanti dall'assenza di una disciplina esplicita dei poteri investigativi. In particolare, viene denunciato il rischio di una compressione della "libertà del cittadino", evidenziando come la mancanza di

norme chiare consenta alla polizia di intervenire senza limiti definiti nella sfera privata, fino a "violare il segreto postale e telegrafico"³¹; mentre per altri era del tutto ammissibile che "in certe gravi contingenze politiche o delittuose" il potere pubblico potesse "ricorrere alla violazione del segreto"³², come del resto, nella storia, aveva sempre fatto. In questo modo la captazione delle comunicazioni, pur formalmente tutelata sul piano penale nei rapporti tra cittadini, resta esposta a pratiche amministrative difficilmente controllabili quando esercitate dall'autorità pubblica.

Questa tendenza trova una chiara conferma anche sul piano processuale. Il codice di procedura penale del 1913³³ riconosce infatti in modo esplicito all'autorità la possibilità di accedere alle comunicazioni degli indagati. In particolare, l'articolo 170 stabilisce che gli ufficiali di polizia, nel procedere al sequestro della corrispondenza, debbano trasmettere all'autorità giudiziaria lettere, telegrammi e altri documenti senza aprirli, riservando al giudice la decisione sulla loro utilizzazione. Ancora più significativa è la previsione dell'articolo 238, che attribuisce al giudice la facoltà di ordinare negli uffici postali e telegrafici il sequestro della corrispondenza e di accedere agli uffici telefonici per intercettare o impedire comunicazioni o assumerne cognizione. La disciplina, tuttavia, non introduce particolari garanzie procedurali: non sono previsti limiti specifici quanto ai reati per i quali la misura può essere disposta, né un sistema di

30. Secondo alcune ricostruzioni, risalirebbe al 1903 la prima intercettazione telefonica documentata in Italia. In modo del tutto fortuito un telefonista avrebbe ascoltato una conversazione tra un ministro del governo Giolitti e la moglie nella quale si faceva riferimento all'imminente emanazione di un decreto di carattere finanziario suscettibile di influenzare l'andamento dei titoli azionari, suggerendone l'acquisto. Il centralinista redasse un verbale della conversazione e lo trasmise al capo di gabinetto del presidente del Consiglio, il quale dispose il rinvio della pubblicazione del decreto. L'episodio avrebbe indotto l'amministrazione statale a istituire all'interno della polizia un primo Servizio di intercettazione telefonica statale. Cfr. GUSPINI 1973.

31. Su questo punto le osservazioni di SOLAZZI 1910. Ma si possono richiamare anche le riflessioni di FLORIAN 1905. Riassume la tensione tra tutela della segretezza delle comunicazioni e l'interesse pubblico alla sicurezza GIORDANI 1911, il quale spiega che: "il principio della inviolabilità del segreto viene meno di fronte al diritto della società di reprimere le infrazioni alla legge penale" (p. 156), sottolineando, poi, che il potere della polizia non deve trasformarsi in abusi e arbitrio.

32. FANI 1909, p. 111.

33. Per la genesi e il significato storico del codice di procedura penale del 1913 si veda MILETTI 2003. Il volume ricostruisce in prospettiva storico-giuridica il lungo percorso che condusse all'elaborazione del codice, esaminando i progetti di riforma succedutisi tra la fine dell'Ottocento e l'età giolittiana, il dibattito tra le diverse scuole penalistiche e i lavori parlamentari che prepararono l'adozione della nuova disciplina processuale, nonché le reazioni critiche al codice.

autorizzazioni preventive o di controlli successivi sull'esercizio di tali poteri. Questa impostazione riflette una più ampia tradizione processuale nella quale la captazione delle informazioni è considerata un mezzo ordinario di accertamento del reato.

Il quadro non muta sostanzialmente con i codici del 1930. Il codice penale Rocco mantiene la tutela della segretezza delle comunicazioni nel titolo dedicato ai *delitti contro l'inviolabilità dei segreti*: gli artt. 616-620 puniscono infatti l'apertura, la sottrazione o la rivelazione della corrispondenza e la fraudolenta captazione di comunicazioni telefoniche tra privati. Sul piano processuale, nel codice di procedura penale del 1930, una base normativa per le pratiche di acquisizione dei dati veniva ricercata nell'articolo 226, il quale consentiva agli ufficiali di polizia giudiziaria, "per i fini del loro servizio", di accedere agli uffici o agli impianti telefonici del pubblico servizio e di intercettare o impedire comunicazioni o prenderne cognizione. Proprio l'inciso *per i fini del loro servizio* assume un rilievo decisivo, la formula, volutamente ampia e priva di specifiche delimitazioni normative, finiva infatti per attribuire agli organi investigativi un margine molto esteso di discrezionalità operativa, rimettendo in larga misura alla valutazione dell'autorità di polizia la decisione circa l'opportunità di procedere all'ascolto delle comunicazioni. In tal modo la disposizione riflette una concezione dell'attività investigativa fortemente orientata alla tutela della sicurezza pubblica e dell'ordine statale, nella quale le esigenze di controllo e di prevenzione prevalgono sulle garanzie della segretezza delle comunicazioni. L'ampiezza della clausola testimonia una mentalità giuridica e amministrativa consolidata

nel tempo, nella quale la captazione delle comunicazioni appare come uno strumento ordinario dell'azione di polizia, più che come una misura eccezionale sottoposta a rigorosi limiti giuridici. In tal modo, mentre la legge penale sanzionava la captazione fraudolenta delle comunicazioni tra privati, l'ordinamento non prevedeva una disciplina altrettanto puntuale dell'attività di intercettazione svolta dall'autorità pubblica, lasciando spazio a prassi di polizia e amministrative di controllo tipiche dei regimi totalitari. Ciò detto, non stupisce l'interpretazione estensiva che viene data al testo del *Codice postale e delle comunicazioni* emanato con Regio Decreto n. 645 nel 1936; in particolare l'articolo 12 prevedeva che "la pubblica autorità, nei casi e nei modi previsti dalla legge, ha facoltà di prendere visione, avere copia e procedere a sequestro della corrispondenza", inoltre il successivo articolo 13 prevedeva che non fosse inoltrata la corrispondenza suscettibile di costituire pericolo per la sicurezza dello Stato, per le persone o per le cose, ovvero contraria all'ordine pubblico o al buon costume. Il regime ricavò da tali disposizioni, in via implicita, un generale potere dell'autorità di pubblica sicurezza di controllare il contenuto delle comunicazioni.

Nel contesto politico fascista tali strumenti vengono progressivamente integrati all'interno di un sistema di controllo più ampio, nel quale le intercettazioni epistolari, telegrafiche e telefoniche rappresentano uno dei mezzi attraverso cui l'apparato di polizia esercita attività di sorveglianza³⁴ su oppositori politici, ambienti intellettuali e soggetti ritenuti pericolosi per la sicurezza del regime³⁵.

34. Una testimonianza particolarmente significativa sul funzionamento del sistema di intercettazioni telefoniche durante il regime fascista è offerta da GUSPINI 1973, che spiega come "nessuno poteva sfuggire al controllo telefonico". L'autore fu per lungo tempo tra gli addetti al servizio incaricato di ascoltare e stenografare le conversazioni telefoniche intercettate; il volume, fondato su questa esperienza diretta, riporta numerose trascrizioni di dialoghi captati nel corso degli anni, riguardanti non soltanto figure politiche e gerarchi del regime, ma anche conversazioni di natura privata o quotidiana. Ne emerge l'immagine di un sistema di ascolto esteso e burocraticamente organizzato, nel quale un apposito servizio provvedeva alla registrazione scritta e alla selezione delle comunicazioni ritenute di interesse per le autorità.

35. Durante il periodo fascista operava presso diverse prefetture un apparato organizzato di ascolto delle comunicazioni telefoniche. Alcune linee erano sottoposte a vigilanza permanente, altre a controlli episodici; le conversazioni potevano essere monitorate e, in alcuni casi, trascritte mediante stenografia. Il servizio funzionava in modo stabile ed era affidato al personale dell'amministrazione statale. La logica di questo sistema di sorveglianza politica non si discosta, nella sua struttura di fondo, da quella già praticata negli ordinamenti di antico regime attraverso strumenti come i *cabinet noir*, destinati al controllo delle comunicazioni private. Sul punto si veda anche ROSSI 1951.

Durante la guerra, poi, la captazione delle comunicazioni diviene uno strumento essenziale per il controllo delle informazioni strategiche e per la prevenzione delle attività di spionaggio.

Nel complesso, tra la fine dell'Ottocento e la seconda guerra mondiale si delinea un quadro caratterizzato da una evidente ambivalenza. Da un lato il diritto liberale riconosce la segretezza delle comunicazioni come bene giuridico meritevole di tutela e ne sanziona la violazione; dall'altro lo sviluppo tecnologico e le esigenze di sicurezza dello Stato favoriscono una crescente espansione delle pratiche di intercettazione da parte dell'apparato pubblico. Solo con la nascita dell'ordinamento costituzionale repubblicano tale tensione verrà affrontata in termini nuovi. L'articolo 15 della Costituzione del 1948 affermerà infatti per la prima volta, in forma esplicita, l'inviolabilità della libertà e della segretezza della corrispondenza³⁶ e di ogni altra forma di comunicazione, subordinando ogni limitazione a un atto motivato dell'autorità giudiziaria e alle garanzie stabilite dalla legge. In questo modo la captazione delle comunicazioni, pur restando uno strumento fondamentale dell'indagine penale, viene ricondotta entro un sistema di garanzie costituzionali destinato a disciplinarne l'uso.

Con l'affermazione delle garanzie costituzionali si apre una stagione di tensione che, a ben vedere, a mio parere, non è mai stata completamente superata. Per secoli il potere politico aveva potuto servirsi delle tecniche di captazione dei dati come strumenti ordinari di governo e di sicurezza, senza incontrare limiti giuridici effettivi. L'emersione del costituzionalismo e la progressiva affermazione dei diritti fondamentali, consacrati non solo nelle costituzioni nazionali ma anche nelle carte internazionali dei diritti, modificano radicalmente questo quadro.

Si determina così una frattura strutturale tra due esigenze difficilmente conciliabili, da un lato

le necessità investigative dello Stato, sostenute dal *principio della libertà della prova* e orientate alla ricerca della *verità reale*; dall'altro la tutela delle libertà individuali, che la giurisprudenza costituzionale e sovranazionale, insieme alla scienza giuridica, hanno progressivamente cercato di rafforzare e rendere effettiva.

5. Dalla costituzionalizzazione delle intercettazioni alla ricerca di una nuova connessione giuridica

Proprio questa tensione tra esigenze di sicurezza e garanzie della segretezza delle comunicazioni rende progressivamente inevitabili, nel secondo dopoguerra, azioni del legislatore e della giurisprudenza volte a ricondurre l'istituto entro i limiti del nuovo ordinamento costituzionale.

Un primo intervento significativo si ebbe con la legge del 18 giugno 1955 n. 517, che introdusse, all'articolo 7, l'obbligo del decreto motivato dell'autorità giudiziaria per autorizzare le operazioni di intercettazione, eliminando la precedente possibilità per la polizia giudiziaria di accedere autonomamente agli impianti telefonici. Tale riforma rappresentò un primo tentativo di adeguamento della disciplina alle nuove garanzie costituzionali, pur senza giungere a una regolamentazione organica della materia. Nel frattempo, anche il quadro sovranazionale contribuì a rafforzare la tutela della segretezza delle comunicazioni, infatti, la *Convenzione europea dei diritti dell'uomo* del 1950, ratificata dall'Italia nel 1955, riconosceva all'art. 8 il *diritto al rispetto della vita privata e della corrispondenza*, introducendo un ulteriore parametro di controllo sulle ingerenze dei pubblici poteri nella sfera comunicativa dell'individuo³⁷. In questo modo, tra gli anni Cinquanta e Settanta, la captazione delle comunicazioni viene progressivamente ricondotta da pratica investigativa largamente discrezionale a strumento processuale sottoposto a garanzie giurisdizionali e a un crescente controllo di legittimità.

36. Sulla libertà e segretezza della corrispondenza e delle comunicazioni, quale diritto fondamentale dell'ordinamento costituzionale si è ovviamente scritto tantissimo, mi limito a richiamare contributi redatti in periodi storici diversi: ITALIA 1963; CARETTI 1989; PACE 1992; VALASTRO 2001; CARUSO 2013. In una prospettiva più recente CALIFANO 2023, che ricostruisce la proiezione costituzionale dell'art. 15 Cost. come garanzia dell'inviolabilità delle comunicazioni interpersonali e come presidio del nucleo essenziale dei diritti della persona nel bilanciamento con le esigenze investigative e con le nuove forme di comunicazione digitale.

37. Per alcuni esempi di riflessioni degli anni Sessanta sulla Convenzione quale parametro di tutela della riservatezza e della segretezza delle comunicazioni: PISANI 1966 e BRICOLA 1967.

Un momento decisivo nella ridefinizione dell'istituto si ebbe con la sentenza n. 34 del 1973 della Corte costituzionale. Pur respingendo formalmente la questione di illegittimità, la Corte affermò che le intercettazioni costituiscono una limitazione alla libertà e segretezza delle comunicazioni garantita dall'art. 15 Cost., ammissibile solo quando giustificata da esigenze di giustizia e subordinata all'atto motivato dell'autorità giudiziaria. La pronuncia individuò inoltre alcuni principi fondamentali, come la necessità di indicare la durata delle operazioni e di sottoporle al controllo del giudice. Tale decisione contribuì a rendere evidente l'inadeguatezza della disciplina vigente e favorì l'intervento del legislatore con la legge n. 98 dell'8 aprile 1974, che introdusse per la prima volta una regolamentazione organica delle intercettazioni³⁸.

Negli anni immediatamente seguenti, anche sotto la pressione delle emergenze legate al terrorismo e alla criminalità organizzata, il legislatore intervenne nuovamente sulla materia, introducendo modifiche che in alcuni casi attenuarono il rigore delle garanzie inizialmente previste³⁹. Il definitivo riassetto dell'istituto si realizzò con il codice di procedura penale del 1988, che collocò le intercettazioni tra i mezzi di ricerca della prova (artt. 266-271 c.p.p.), delineandone in modo più organico i presupposti di ammissibilità, le modalità di autorizzazione e di esecuzione, nonché i limiti di utilizzabilità nel processo. A partire dagli anni Novanta, tuttavia, il rapido sviluppo delle tecnologie informatiche e delle comunicazioni digitali impose un ulteriore adattamento della disciplina. Con la legge del 23 dicembre 1993 n. 547 venne introdotto l'art. 266-bis c.p.p., che estese la possibilità di intercettazione anche ai flussi di comunicazioni informatiche e telematiche, segnando l'ingresso dell'istituto nell'ambito delle nuove tecnologie della comunicazione.

Nel corso del XXI secolo la progressiva digitalizzazione della vita sociale e delle relazioni interpersonali ha ulteriormente ampliato le tecniche di captazione delle informazioni, portando all'elaborazione di strumenti investigativi sempre più sofisticati. In questo contesto si colloca l'introduzione del cosiddetto captatore informatico.

Siamo arrivati all'attualità. Il trojan di Stato rappresenta oggi una delle frontiere più avanzate delle tecniche di investigazione penale, poiché consente una forma di controllo delle comunicazioni particolarmente penetrante e potenzialmente estesa all'intero ambiente digitale dell'individuo. Da un lato l'utilizzo di tale tecnologia sembra essere l'unico modo per contrastare forme di criminalità sempre più diffuse e dannose che operano nel web in contesti sovranazionali; dall'altro queste forme di indagini finiscono per violare moltissimi aspetti della vita privata del soggetto, il quale ripone nei suoi *device* il suo *io digitale*⁴⁰.

Allo storico del diritto questa tensione non sorprende. Ogni volta che una nuova tecnologia della comunicazione ha trasformato il modo in cui gli individui scambiano informazioni, dalla lettera al telegrafo, dal telefono alla rete digitale, il potere pubblico ha cercato, quasi inevitabilmente, di adattare i propri strumenti di controllo e di sicurezza. La storia delle intercettazioni mostra così un movimento ricorrente, per cui, alle innovazioni tecniche corrisponde l'espansione delle possibilità di captazione delle informazioni, cui segue, spesso con ritardo, un tentativo del diritto di ricostruire un equilibrio tra libertà e sicurezza. Se questa è la lezione che proviene dalla lunga durata delle istituzioni giuridiche, allora la sfida del presente non consiste tanto nel rifiutare le nuove tecnologie investigative, quanto nel governarle mediante categorie giuridiche adeguate alla società digitale.

38. Sulle intercettazioni senza alcuna pretesa di completezza, si vedano, tra i molti contributi: ILLUMINATI 1983; CAPRIOLI 1991; CAMON 1996. Per una riflessione più recente, successiva alla riforma della disciplina delle intercettazioni, si veda MAGGIO 2023.

39. Nel contesto della legislazione emergenziale adottata alla fine degli anni Settanta per fronteggiare il terrorismo, la legge n. 191 del 1978 intervenne sulla disciplina delle intercettazioni telefoniche, eliminando il limite massimo complessivo di durata precedentemente previsto dall'art. 226-ter, comma 2, c.p.p., che fissava il termine di quarantacinque giorni. La riforma rese così possibile la reiterazione delle proroghe senza la previsione di un limite temporale complessivo: PALTRINIERI-UBERTIS 1979.

40. Sul ruolo degli smartphone e dei dispositivi informatici quali archivi della vita privata dell'individuo e sulle implicazioni che ciò comporta per le garanzie processuali nelle attività di acquisizione probatoria: LORENZETTO 2025.

In questo senso, l'età delle reti e degli algoritmi potrebbe richiedere una nuova stagione di riflessione giuridica paragonabile, per portata culturale, a quella che nel XVIII secolo accompagnò l'emergere dello Stato di diritto. Come l'Illuminismo giuridico seppe porre limiti razionali al potere punitivo dello Stato e fondare un sistema di garanzie per la libertà individuale, così la società digitale sembra oggi richiedere un rinnovato sforzo di elaborazione teorica capace di conciliare le esigenze di sicurezza con la tutela dei diritti fondamentali. Sembra auspicabile una *connessione giuridica*⁴¹, nella quale il legislatore, ma anche la dottrina e la giurisprudenza⁴² siano chiamati a ridefinire, alla luce delle nuove tecnologie, il significato stesso della libertà e della segretezza delle comunicazioni.

L'alternativa è un ritorno al passato, all'uso indiscriminato delle tecniche di captazione in nome della sicurezza, con il rischio che esse si trasformino, in contesti politici segnati da una

crescente concentrazione del potere esecutivo e dall'indebolimento delle garanzie istituzionali, in strumenti di difesa del potere piuttosto che di tutela dei diritti. Da qui, l'immagine del *panopticon*, modello teorico della società disciplinare moderna⁴³, si mischia al futuro distopico orwelliano, nel quale "non è possibile sapere se e quando si era sotto osservazione": in ogni stanza è presente uno schermo capace di osservare e ascoltare; le informazioni sono manipolate al fine di creare un'unica coscienza collettiva; la sicurezza dell'ordinamento viene garantita reprimendo ogni forma di dissenso. In questa società del controllo il futuro è descritto attraverso un'immagine precisa: "uno stivale che calpesta un volto umano in eterno". Del resto, come ci insegna la vicenda di Giordano Bruno: "Quel volto da calpestare ci sarà sempre, così come sempre ci sarà l'eretico, il nemico della società, da sconfiggere e umiliare in un circuito senza fine"⁴⁴.

Riferimenti bibliografici

- P. BARILE, E. CHELI (1962), *Corrispondenza (libertà di)*, in "Enciclopedia del diritto", vol. X, Giuffrè, 1962
- M. BIRAL (2023), *Testimonianza anonima e agente sotto copertura*, Cedam, 2023
- F. BRICOLA (1967), *Prospettive e limiti della tutela penale della riservatezza*, in "Rivista italiana di diritto e procedura penale", vol. 10, 1967
- L. CALIFANO (2023), *La libertà e la segretezza delle comunicazioni*, in "Cultura giuridica e diritto vivente", vol. 11, 2023
- M. CALIGIURI (2025), *Intelligence*, Treccani, 2025

41. Con l'espressione *connessione giuridica* si intende qui alludere alla necessità di un rinnovato sforzo di elaborazione teorica capace di adattare le categorie tradizionali del diritto alle trasformazioni prodotte dall'ambiente digitale e algoritmico. Come in altri momenti della storia giuridica, anche oggi lo sviluppo di nuove tecnologie della comunicazione e della captazione delle informazioni, in contesti istituzionali spesso segnati da una crescente concentrazione del potere decisionale nell'esecutivo e da un indebolimento dei tradizionali contrappesi tra i poteri dello Stato, rende particolarmente urgente la costruzione di nuovi limiti giuridici all'esercizio dell'autorità. La società delle reti e dei dati richiede pertanto un paradigma interpretativo capace di mettere in relazione diritto e tecnologie che ridefiniscono gli spazi della comunicazione, della sorveglianza e della sicurezza. In questa prospettiva, la "connessione" indica la necessità che il diritto si confronti criticamente con la nuova realtà tecnologica, elaborando strumenti concettuali idonei a preservare i diritti fondamentali nell'ecosistema digitale.

42. Per una riflessione sul superamento della concezione *statual-legislativa* del diritto e sul crescente ed essenziale ruolo della giurisprudenza e della scienza giuridica, particolarmente evidente nell'esperienza giuridica europea: GROSSI 2020.

43. Il riferimento, qui, è alla nota elaborazione teorica di FOUCAULT 1975.

44. ORWELL 1949 p. 275.

- A. CAMON (2025), *I confini mobili delle intercettazioni*, in G. Di Paolo, L. Pressacco (a cura di), "Indagini e prove nella società digitale. Questioni attuali e prospettive future", Università degli Studi di Trento, 2025
- A. CAMON (1996), *Le intercettazioni nel processo penale*, Giuffrè, 1996
- F. CAPRIOLI (1991), *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in "Rivista italiana di diritto e procedura penale", vol. 34, 1991
- P. CARETTI (1989), voce *Corrispondenza (libertà di)*, in "Digesto delle discipline pubblicistiche", vol. 4, Utet, 1989
- C. CARUSO (2013), *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, in "Forum di quaderni costituzionali", vol. 10, 2013
- G. CHIODI (2013), *Nel labirinto delle prove legali: la testimonianza del complice nel processo penale d'età moderna*, in "Rivista Internazionale di Diritto Comune", vol. 24, 2013
- D. DEI (a cura di) (2000), *Atti del processo di Giordano Bruno*, Sellerio, 2000
- A. DEL COL, G. PAOLIN (1991), *L'Inquisizione romana in Italia nell'età moderna. Archivi, problemi di metodo e nuove ricerche*, Ministero per i beni culturali e ambientali, 1991
- G. DI PAOLO (2025), *Comunicazioni digitali e prova penale. Note introduttive*, in G. Di Paolo, L. Pressacco (a cura di), "Indagini e prove nella società digitale. Questioni attuali e prospettive future", Università degli Studi di Trento, 2025
- A. ERRERA (2018), *La procedura inquisitoriale tra predicazione e diritto: la fase della inquisitio generalis*, in L. Gaffuri, R.M. Parrinello (a cura di), "Verbum e ius. Predicazione e sistemi giuridici nell'Occidente medievale", Firenze University Press, 2018
- A. ERRERA (2010), *Manuali per inquisitori*, in "Dizionario storico dell'Inquisizione", diretto da A. Prosperi, vol. II, Scuola Normale Superiore, 2010
- A. ERRERA (2000), *Processus in causa fidei. L'evoluzione dei manuali inquisitoriali nei secoli XVI-XVIII e il manuale inedito di un inquisitore perugino*, Monduzzi, 2000
- F.N. EYMERICI (1376), *Directorium inquisitorum, cum commentariis Francisci Pegnae*, In aedibus Populi Romani, 1587
- A. FANI (1911), *Le basi giuridiche della libertà moderna*, Fratelli Bocca, 1911
- E. FATTORINI (2007), *Pio XI, Hitler e Mussolini. La solitudine di un papa*, Einaudi, 2007
- R. FLOR, S. MARCOLINI (2022), *Dalla data retention alle indagini ad alto contenuto tecnologico. La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato. Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022
- E. FLORIAN (1905), *Trattato di diritto penale*, vol. II, Vallardi, 1905
- M. FOUCAULT (1975), *Sorvegliare e punire. Nascita della prigione*, traduzione italiana: Einaudi, 1976
- L. GARLATI (2015), *Miti inquisitori: la confessione tra ricerca della verità e "garanzie processuali"*, in L. Luparia, L. Marafioti (a cura di), "Confessione, liturgie della verità e macchine sanzionatorie", Giappichelli, 2015
- M.L. GHEZZI (a cura di) (2011), *Processo e morte di Giordano Bruno. I documenti*, con un saggio di L. Parinetto, Mimesis, 2011
- T. GILLS (1927), *Traité de Législation postale*, Imprimere Cooperative, 1927
- G. GIORDANI (1911), *Il segreto epistolare*, in "Rivista di diritto penale e sociologia criminale", vol. 12, 1911

- L. GIORDANO (2020), *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in "Sistema penale", 2020, n. 4
- P. GROSSI (2020), *Oltre la legalità*, Laterza, 2020
- U. GUSPINI (1973), *L'orecchio del regime. Le intercettazioni telefoniche al tempo del fascismo*, Mursia, 1973
- G. ILLUMINATI (1983), *La disciplina processuale delle intercettazioni*, Giuffrè, 1983
- V. ITALIA (1963), *Libertà e segretezza della corrispondenza e delle comunicazioni*, Giuffrè, 1963
- E. LORENZETTO (2025), *I sequestri di smartphone, dispositivi informatici e memorie digitali*, in G. Di Paolo, L. Pressacco (a cura di), "Indagini e prove nella società digitale. Questioni attuali e prospettive future", Università degli Studi di Trento, 2025
- L. LUPARIA, L. MARAFIOTI (a cura di) (2015), *Confessione, liturgie della verità e macchine sanzionatorie*, Giappichelli, 2015
- P. MAGGIO (a cura di) (2023), *La nuova disciplina delle intercettazioni*, Giappichelli, 2023
- G. MAIFREDA (2018), *Io dirò la verità. Il processo a Giordano Bruno*, Laterza, 2018
- G. MAIFREDA (2016), *Giordano Bruno e Celestino da Verona. Un incontro fatale*, Edizioni della Normale, 2016
- F. MASTROBERTI, G. MASIELLO (a cura di) (2020), *Il codice per lo Regno Delle Due Sicilie. Elaborazione, applicazione e dimensione europea del modello codicistico borbonico*, Editoriale Scientifica, 2020
- M.N. MILETTI (2006), *Il velo squarciato. Riforme dell'instruction nella Terza Repubblica e riflessi nell'Italia liberale*, in "Riti, tecniche, interessi. Il processo penale tra Otto e Novecento" (Foggia, 6-6 maggio, 2006), Giuffrè, 2006
- M.N. MILETTI (2003), *Un processo per la terza Italia. Il codice di procedura penale del 1913*, Giuffrè, 2003
- W. NOCERINO (2020), *Il captatore informatico: un giano bifronte. Prassi operative vs risvolti giuridici*, in "Cassazione penale", 2020, n. 2
- G. ORWELL (1949), 1984, traduzione italiana: Mondadori, 2010
- A. PACE (1992), *Problematica delle libertà costituzionali*, vol. II, Cedam, 1992
- V. PALTRINIERI, G. UBERTIS (1979), *Intercettazioni telefoniche e diritto umano alla privacy nel processo penale*, in "Rivista italiana di diritto e procedura penale", vol. 22, 1979
- B. PANATTONI (2025), *Generative AI and criminal law*, in "Cambridge Forum on AI: Law and Governance", vol. 1, 2025
- M. PIFFERI (2019), *Le insanabili antinomie della tortura. Modelli di verità e significato del dolore nella quaestio per tormenta medievale*, in "La legislazione penale", 2019
- M. PISANI (1966), *Convenzione europea dei diritti dell'uomo e riforma del processo penale*, in "Il Foro italiano", vol. 89, 1966, n. 4
- P. ROSSI (1951), *Lineamenti di diritto penale costituzionale*, Priulla, 1951
- C. ROVELLI (2014), *Sette brevi lezioni di fisica*, Adelphi, 2014
- L. SALA-MOLINS (a cura di) (1973), *N. Eymerich, Il manuale dell'Inquisitore*, traduzione italiana: Fanucci Editore, 2000
- M. SBRICCOLI (2002), *Giustizia criminale*, in M. Fioravanti (a cura di), "Lo Stato moderno in Europa. Istituzioni e diritto", Laterza, 2002

- M. SBRICCOLI (1991), *Tormentum idest torquere mentem. Processo inquisitorio e interrogatorio per tortura nell'Italia comunale*, in J.-C. Maire Vigueur, A. Paravicini Bagliani (a cura di), "La parola all'accusato", Sellerio, 1991
- P. SCHIRÒ (2025), *Controllare, validare, diffondere. Le norme sulla diffusione delle belle arti nel Ducato di Parma, Piacenza e Guastalla*, in "Ricerche di S/Confine", Dossier 9, 2025
- G. SOLAZZI (1910), *Note critiche sulla libertà giuridica individuale*, Zanichelli, 1910
- E. TAVILLA (2021), *Patire nel processo: tortura e confessione nella procedura penale d'antico regime*, in "DNA – Di Nulla Academia", vol. 2, 2021
- A. VALASTRO (2001), *Libertà di comunicazione e nuove tecnologie*, Giuffrè, 2001
- S. VINCIGUERRA (a cura di) (2009), *Il codice penale per gli Stati del re di Sardegna e per l'Italia unita (1859)*, Cedam, 2009



ROSA MARIA VADALÀ

Ricadute sostanziali delle prescrizioni e dei divieti del regolamento europeo sull'intelligenza artificiale

Muovendo da una prospettiva reo-centrica orientata ai diritti, saranno analizzate le norme dell'*AI Act* che incidono sull'azione penale, evidenziandone le potenzialità garantistiche, sostanziali e processuali. Tali potenzialità si confrontano, da un lato, con la legge italiana sull'intelligenza artificiale (l. n. 132/2025), che non ha sostanzialmente introdotto istituti idonei a recepire nel processo penale le previsioni sovranazionali; dall'altro, con le disposizioni penali nazionali che incidono sull'operatività dell'*AI Act*. Costituisce inoltre un limite invalicabile il sistema di divieti ed eccezioni delineato dall'art. 5 del regolamento europeo, che si fonda sul diritto all'autodeterminazione informativa e sul principio di proporzionalità. Quest'ultimo consente quella capacità di resistenza dei diritti rispetto a derive securitarie, per cui l'AI potrebbe segnare un punto di non ritorno.

Intelligenza artificiale – Giustizia penale – Proporzionalità – Reo – Diritti fondamentali

Criminal implications of the prohibitions and restrictions of AI ACT

Adopting a defendant-centred, rights-based perspective, this article examines the provisions of the AI Act that affect criminal proceedings, highlighting their substantive and procedural safeguards. The effectiveness of these safeguards must be assessed, on the one hand, in light of the Italian Artificial Intelligence Act (Law No. 132/2025), which has largely failed to introduce legal mechanisms capable of incorporating the supranational framework into criminal proceedings, and, on the other hand, against the backdrop of domestic criminal law provisions that shape the implementation of the AI Act. A further, non-derogable constraint is represented by the system of prohibitions and exceptions established under Article 5 of the Regulation, which is grounded in the right to informational self-determination and the principle of proportionality. The latter provides a crucial safeguard against security-driven excesses, in the face of which AI could otherwise mark a point of no return.

Artificial intelligence – Criminal justice – Proportionality – Offender – Fundamental rights

L'Autrice è docente a contratto di Cybercrime presso il Dipartimento di informatica dell'Università di Verona. Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2*, a cura di Gaetana Morgante e Gaia Fiorinelli.

SOMMARIO: 1. Premessa sulla dimensione sostanziale in gioco. – 2. L'AI nella giustizia penale: disposizioni "dirette" dal regolamento (UE) 2024/1689 alla legge n. 132/2025. – 3. Profilazione tra conferme e novità. – 3.1. Il divieto dell'art. 5 tra predizione "decisoria" e predizione di polizia. – 4. *Scraping* e dati biometrici: usi legittimi secondo l'autodeterminazione informativa. – 4.1 Il riconoscimento facciale tra impieghi ed eccezioni "proporzionali".

1. Premessa sulla dimensione sostanziale in gioco

L'analisi delle ricadute sostanziali delle previsioni del regolamento (UE) 2024/1689, c.d. *AI Act*, sugli impieghi di sistemi intelligenti in funzione di prevenzione e accertamento dei reati¹ chiama in causa la più ampia riflessione sui diritti fondamentali in gioco. Come messo chiaramente in luce, l'atto regolamentare esplicita quel "nesso molto significativo tra l'ambizione alla sovranità digitale da parte dell'Unione europea e la stessa identità costituzionale europea, laddove la prima risulta funzionale al consolidamento di quel costituzionalismo digitale europeo (...) in modo che quest'ultimo possa disporre dei poteri adeguati a garantire la tutela dei diritti fondamentali"².

Per la giustizia penale l'adozione di questa prospettiva concentra il focus d'intervento della legge sulla sfera giuridica dell'individuo sulla quale lo *ius puniendi* sarà destinato a dispiegarsi. Come è stato autorevolmente evidenziato, "il contributo

più significativo offerto dalla giurisprudenza di Strasburgo (...) è quello di avere chiarito che ogni estrinsecazione di potere pubblico abbisogna di una giustificazione dalla specifica prospettiva della persona sulla quale il potere va ad incidere, chiamando necessariamente in causa i suoi 'diritti' di fronte all'autorità"³.

In particolare, lo sviluppo tecnologico consente indagini pro-attive, che combinano aspetti di quelle preventive e di quelle repressive⁴, configurandosi come attività esplorative volte alla ricerca delle notizie di reato⁵. Questa commistione si traduce nell'impiego di "tecniche operative miste, anfibie, ambivalenti"⁶ con una crescita non solo dei poteri e compiti di polizia, ma anche della commistione con le attività di *intelligence*⁷. Quanto sopra impone di anticipare la predetta visione "orientata" ai diritti ad una fase antecedente al processo o al procedimento penale⁸, estendendo l'ambito da presidiare agli atti particolarmente intrusivi di tipo investigativo in senso ampio.

1. Riconoscono ante *AI Act* le potenzialità dell'AI in questa duplice direzione BORGES BLÀZQUEZ 2021, p. 111; MANES 2020, p. 6.

2. CARAMASCHI 2025, p. 10.

3. VIGANÒ 2023, p. 17.

4. SIGNORATO 2016, p. 194; BLOUNT 2021, p. 39.

5. TORRE 2019, p. 1437.

6. NEGRI 2016, p. 3.

7. NOCERINO 2020, p. 822.

8. Sulla prospettiva del diritto penale reo centrico, che concepisce il soggetto nei confronti del quale si procede come l'anello debole della macchina repressiva si rinvia, anche per i relativi riferimenti bibliografici, a BERNASCONI 2022.

In conformità, pertanto, sia alle peculiarità dell'intelligenza artificiale, quale tecnologia di per sé *disruptive*⁹, sia alla sua idoneità ad operare più come strumento d'indagine, che di giudizio¹⁰, l'*AI Act* considera quale contesto "penale" di riferimento quello di *law enforcement*, quale "attività svolta dalle autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse"¹¹.

Questa scelta di campo è espressione emblematica di un tecno-diritto¹², che non è più declinabile secondo una prospettiva di prevalenza o di resistenza della legge rispetto al *code*¹³, ma d'integrazione funzionale, che, alla luce dei nuovi fattori di rischio tecnologico, estende o introduce apposite garanzie sostanziali e procedurali, consentendo, però, quegli impieghi di sistemi di AI che possono apportare importanti benefici.

Per evitare, però, che la trasformazione tecnologica alimenti un'inammissibile diritto penale

*gendarmo*¹⁴, che sublima prevenzione e sicurezza, queste garanzie dovrebbero essere funzionali a confinare entro un'area di *legal risk*¹⁵ le potenzialità pregiudizievoli associabili a questi impieghi.

Il richiamo al concetto di rischio non è qui, però, operato secondo quella logica di tipo precauzionale di cui certamente è pervasa l'*AI Act*, data la classificazione delle forme di manifestazione dell'intelligenza artificiale a cui si associano regimi differenti¹⁶. Come autorevolmente evidenziato, gli standard richiesti dal regolamento europeo costituiscono la futura piattaforma concettuale per la disciplina dei profili di responsabilità penale per l'immissione nel mercato e l'utilizzo di strumentazioni di AI¹⁷.

Ma la prospettiva che qui si intende adottare è un'altra: guardare a questi standard come fattori che confinano l'invasività o potenzialità lesiva dell'AI quale strumento dell'azione di contrasto. Per essere più chiari, il *legal risk* a cui si fa riferimento dovrebbe essere la traduzione normativa di quel bilanciamento, costantemente ricercato dalle Corti per le indagini tecnologiche, tra le esigenze

9. *Disruptive innovation* è termine coniato nel 1995 da Clayton Christensen per indicare l'effetto di una nuova tecnologia o di un nuovo modo di operare su un modello di business, che porta a modificare completamente la logica fino a quel momento presente nel mercato, introducendo comportamenti e interazioni nuove. Sul punto CHRISTENSEN-RAYNOR-McDONALD 2015, p. 44 ss.

10. CAMON 2025, p. 3009.

11. In questi termini l'art. 3, n. 46, dell'*AI Act*.

12. Per AMATO MANGIAMELI 2023, p. 469 ss., questa espressione designa il diritto con/della/per la tecnologia, potendosi in proposito distinguere: 1. le procedure prodotte dall'evoluzione tecnologica e recepite dal diritto; 2. quelle sinergicamente generate dalla tecnica e dal diritto; 3. quelle sviluppate dal diritto per disciplinare la tecnica.

13. Sul rapporto tra *code* e legge LESSING 2000; HASSAN-DE FILIPPI 2017, p. 88. Con specifico riferimento al diritto penale SGUBBI 2019, p. 40, discorre di formante algoritmico per rappresentare come nel sistema penale, che si avvia ad essere disciplinato tramite codice, la certezza del tipo di fatto punito dipende dalla predittività della decisione giudiziale fondata su calcoli algoritmici.

14. BARONA VILAR 2019, p. 33.

15. Per CANATO 2024, p. 15, questo rischio è costituito da quella quota di rischi che residua dai presidi imposti dall'*AI Act* ed è predeterminata senza un'adeguata attenzione alla effettiva dimensione fattuale.

16. I sistemi di AI sono classificati secondo 4 livelli di rischio: inaccettabile, alto, limitato e minimo. Nel presente lavoro verranno considerati solo i primi due livelli a cui corrispondono sistemi che, per l'impatto che possono avere sui diritti fondamentali, sono o vietati, ancorché con alcune eccezioni limitati, o ammessi, ma nel rispetto di requisiti molto rigorosi.

17. In questi termini CONSULICH 2024, per cui nonostante "la categorizzazione impiegata, che sostanzialmente identifica una scala decrescente di rischio, ha una conformazione statica (...) nel testo del Regolamento emerge la consapevolezza di dover adottare un modello di regolazione flessibile per adeguarsi ad un contesto fattuale così fluido: non a caso infatti, ma per necessità, si assiste all'impiego di norme standard, che non descrivono condotte vietate, ma livelli di sicurezza da soddisfare, sulla base di valutazioni tecniche".

di tutela dei diritti fondamentali e l'interesse generale all'accertamento dei reati¹⁸.

Non è un caso che principio, attraverso cui l'*AI Act* sembra tentare di fare ciò, è quello di proporzionalità, il quale richiede di rapportare l'importanza dell'obiettivo perseguito con l'atto d'indagine alla gravità dell'ingerenza, come schermata dalla qualità e quantità delle cautele applicabili a favore dei soggetti interessati¹⁹.

Allo stesso tempo sembra che il regolamento, almeno con riferimento ai sistemi maggiormente invasivi per i diritti, vada oltre questa impostazione²⁰, mostrando un'attenzione che è pregevole se pensiamo che l'*AI Act* "si rivolge al mercato e non ai soggetti istituzionali, prima istanza di presidio delle garanzie fondamentali": il regolamento va ascritto entro "una cornice dettagliata e consolidata, costituita dalla stratificazione di molti strumenti normativi specificamente legati alla dimensione 'non tecnica', ma processuale"²¹.

2. L'AI nella giustizia penale: disposizioni "dirette" dal regolamento (UE) 2024/1689 alla legge n. 132/2025

Con questa consapevolezza vanno considerate le prescrizioni che in via non solo diretta, ma soprattutto indiretta impattano sull'azione penale.

In via diretta, l'allegato III, paragrafo 6, indica alcune tipologie di sistemi di AI impiegabili nell'attività di contrasto, tra cui, alla lett. a), quelli per determinare il rischio per una persona fisica di diventare vittima di reati.

Premesso che la vittima è "tradizionalmente tenuta alla porta dal magistero punitivo"²², sia che si adotti la visuale europea, che la identifica con il soggetto direttamente o indirettamente pregiudicato dal reato, sia quella dogmatica, che guarda al titolare del bene offeso²³, il concetto di vittima rimanda oggi sempre più ad un bisogno particolare di protezione mediante il diritto penale. A fronte dell'emersione di supervittime, come minori o donne²⁴, e della categoria delle vittime potenziali, quali titolari del diritto fondamentale alla sicurezza²⁵, lo statuto penal-processuale ha finito però per assumere un'impronta paternalistica vittimocentrica, divenendo modulabile in funzione del tipo di fatto o del tipo di autore. A fronte di reati che cercano di coprire fenomeni sociali complessi, questa modulabilità dello statuto si è tradotta nella mobilità delle garanzie, innalzabili per la vittima ed abbassabili per l'autore²⁶.

Alla luce di quanto sopra, al fine di evitare che anche l'AI ricada in questa logica efficientista securitaria, potenzialmente in contrasto con la visione reo centrica orientata ai diritti che abbiamo avanzato nella premessa, opportuna appare la delimitazione dell'impiego dei sistemi di *victim prediction* ad alcuni reati particolarmente gravi o afferenti a dinamiche che ne compromettono l'emersione.

Sotto questo profilo, il pensiero corre immediatamente a quei *tool* che sono stati sviluppati a partire da *VioGén*, che è uno strumento algoritmico che stima il rischio di ri-vittimizzazione delle donne che hanno denunciato episodi di violenza

18. Su questo bilanciamento, alla luce della giurisprudenza della Corte di giustizia e di alcune Corti Costituzionali europee, con riferimento alla *data retention* ed alle altre indagini investigative a contenuto tecnologico, si rinvia a FLOR 2022, p. 74 ss.

19. Sulla configurazione sovranazionale del principio di proporzionalità, come emergente in particolare dalle statuizioni adottate dalla Corte di giustizia con la pronuncia del 30 aprile 2024, C178/22, in tema di *data retention*, PARODI 2025, p. 11.

20. Questa valutazione è imposta per l'impiego di sistemi di riconoscimento facciale *real time*, per cui si rimanda al paragrafo 4.

21. Così QUATTROCOLO 2025.

22. BERNASCONI 2019, p. 2.

23. Su questa duplice visione vedi VENTUROLI 2017.

24. PAVAN 2013, p. 4 della versione digitale consultabile nella banca dati *one legale*.

25. VENTUROLI 2021, pp. 9-10.

26. MAGGIO 2017, p. 694.

domestica²⁷. Risponde a finalità analoghe anche il sistema intelligente *Vides* (*Violence detection system*) elaborato da un team multidisciplinare dell'Università di Torino per rilevare episodi di violenza sulla base dell'analisi dei referti del pronto soccorso²⁸. In linea con la trasparenza che l'*AI Act* impone quale requisito dei sistemi ad alto rischio, *Vides* è stato progettato in modo da esplicitare gli elementi che supportano l'interpretazione del referto come relativo a lesioni di origine violenta²⁹.

A fronte anche di questa "spiegabilità", l'impiego di sistemi simili è apprezzabile dal punto di vista penale perché consente d'intercettare reati, come i maltrattamenti in famiglia, in cui la violenza è pratica reiterata in una condizione di soggezione della vittima ed in assenza di testimoni³⁰. Le potenzialità dell'AI, consentendo un tempestivo rilevamento di queste dinamiche, contribuirebbero ad incrementare, ad avviso di chi scrive, il livello d'effettività ed efficacia della disciplina nazionale contro non solo la violenza domestica, ma anche di genere, prevenendo potenziali decorsi tragici, come il femminicidio³¹. Proprio alla luce dei contenuti della recente riforma che ha portato all'introduzione di questo reato³², il regolamento in esame potrebbe essere valorizzato per colmare la mancata adozione di previsioni

apposite su modi e tempi di valutazione del rischio di *escalation* da parte di operatori di polizia e giudici; in questo modo verrebbe, peraltro, dato corso ai moniti inascoltati della Corte di Strasburgo, che concepisce queste procedure di valutazione cruciali ai fini dell'adempimento degli obblighi di tutela discendenti dalla Convenzione di Istanbul³³.

Anche in considerazione di questo contributo, i sistemi di AI di *victim prediction* risultano impiegabili in maniera affidabile e senza grandi criticità essenzialmente come strumenti predittivi con compiti di screening iniziale³⁴. In questo modo è evitabile il rischio, da cui abbiamo preso le mosse, di disequilibrio tra la protezione accordata alla vittima e le garanzie spettanti al reo. Sul punto, peraltro, la qualificazione ad alto rischio anche di questi sistemi ne comporta la sottoposizione a regole di *compliance* per sviluppatori e *deployer*, che possono positivamente impattare sulla posizione del reo, come gli oneri di trasparenza e robustezza, nonché di supervisione umana³⁵. Per autorevole dottrina anzi alcune disposizioni del regolamento rilevarebbero propriamente quali garanzie processuali aggiuntive³⁶. In particolare, le prescrizioni relative sia all'iscrizione dei sistemi di AI in banche dati³⁷ e alla registrazione

27. Sulle caratteristiche tecniche di questo sistema e sulle sue criticità, soprattutto sul piano della compatibilità tra la logica tecnologica, basata sulla predizione del rischio individuale, e gli obiettivi del quadro legislativo spagnolo sul contrasto alla violenza di genere e alla violenza sessuale, vedi MORONDO TARAMUNDI 2025, p. 69.

28. MENSA-COLLA-DALMASSO et al. 2020, p. 263 ss.

29. *Ivi*, p. 271.

30. Cass. pen., Sez. VI, 11 settembre 2025, n. 35067/2025; Cass. pen., Sez. VI, 18 aprile 2023, n. 16466.

31. Sulla configurazione del reato di maltrattamenti in famiglia quale antecedente o reato spia di questo epilogo nella sua valenza sociologica Cass. pen., Sez. I, 12 aprile 2022, n. 14016; COLONE-ESPOSITO-MEGLIO et al. 2023, p. 101 ss. Sul femminicidio quale fattispecie di reato sia consentito rinviare, senza alcuna pretesa di esaustività, a MASSARO 2025, PECORELLA 2025, DI NICOLA TRAVAGLINI 2025.

32. LAZZERI 2025.

33. PULITO 2024, p. 223.

34. In senso critico PULITO 2024, p. 231, che lo concepisce come un uso depotenziato questi strumenti.

35. Norme di riferimento sul punto sono: l'art. 9 sull'adozione di un sistema di gestione dei rischi, l'art. 11 sull'aggiornamento della documentazione tecnica, l'art. 12 sulle procedure e tempi di registrazione automatica degli eventi, l'art. 13 sulla trasparenza del funzionamento, l'art. 14 sulla supervisione umana e l'art. 15 sui requisiti di accuratezza, robustezza e cybersicurezza.

36. CAMON 2025, p. 3019, che ritiene in questo senso particolarmente rilevante l'art. 14 comma 5) sul principio dei "quattro occhi".

37. Ai sensi dell'art. 49 dell'*AI Act* per i sistemi ad alto rischio di cui all'allegato III, paragrafo 6, impiegati nelle attività di contrasto la registrazione avviene, però, in una sezione sicura non pubblica della banca dati dell'Ue di cui all'articolo 71 e comprende, a seconda dei casi, solo alcune informazioni.

automatica degli eventi³⁸ sia quelle che, a certe condizioni, consentono l'accesso ai codici sorgenti attuerebbero rispettivamente quelle istanze sulla tracciabilità della prova informatica e sull'effettività del contraddittorio sull'ammissibilità dello strumento computazionale e dei relativi output³⁹.

Pur condividendosi questa opinione, si ritiene che le potenzialità processual-garantistiche di queste regole richiedano uno sforzo "ricettivo" al livello nazionale, che non è stato al momento esercitato dalla legge n. 132/2025, contenute le "disposizioni e deleghe al Governo in materia di intelligenza artificiale".

Infatti, i non detti di questa legge sono superiori ai detti, essendosi limitata, da un lato, a riservare al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti. Dall'altro, è stata conferita delega per l'adozione di disciplina apposta sugli impieghi dei sistemi di AI rispettivamente al Ministero della giustizia per l'organizzazione e semplificazione del lavoro giudiziario e al Governo per l'attività di polizia⁴⁰.

Si tratta di poche e deludenti disposizioni che nulla apportano sul piano degli istituti e delle categorie che possano veicolare nella giustizia penale le previsioni sovranazionali. In proposito si rammenta che queste previsioni vanno in ogni caso applicate, per espressa disposizione del regolamento relativa proprio ai sistemi del predetto allegato III, conformemente al diritto nazionale.

Quanto sopra comporta che la legge n. 132/2025, così come anche le altre previsioni di contenuto specificamente penale impattino sulla operatività dell'*AI Act*, limitandola o fungendo da vero e proprio sbarramento.

Nel primo senso, la segnalata riserva decisoria al magistrato prevista dalla legge n. 132 assegna una

funzione ausiliare a quei sistemi di AI di cui alla lett. c) dell'allegato III, relativi alla valutazione di affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati. Anzi, in forza del coordinamento garantistico tra fonti, dovrebbe ritenersi che la valutazione del sistema operi a supporto della decisione giudiziale in via succedanea ed a maggior ragione se a favore del prevenuto⁴¹.

Un effetto di sbarramento in senso proprio è svolto, invece, dall'art. 188 c.p.p. con riguardo ai sistemi di cui alla lett. b) dell'allegato III, che possono svolgere funzioni di poligrafo. Il divieto nazionale di metodi o tecniche che siano idonee ad influire sulla libertà di autodeterminazione riguarda, infatti, i sistemi che generano anche solo una qualche forma di pressione, a causa dello stato di soggezione psicologica del soggetto esaminato⁴². Ulteriore rischio che il divieto nazionale sarebbe chiamato ad evitare è quello di trasformare l'individuo, attraverso il ricorso a questi sistemi, "da 'fonte di prova dichiarativa' a 'fonte di prova reale'" con compromissione della sua dignità umana⁴³.

Com'è stato giustamente rilevato, però, la rigidità di questo divieto non dovrebbe essere considerata assoluta almeno per il testimone, che è obbligato a dire la verità⁴⁴; anche per il reo potrebbe ritenersi recessivo, in presenza di libero e volontario consenso⁴⁵ a sottoporsi a verifiche di verità condotte con sistemi di AI, che siano affidabili perché *compliant* agli standard del regolamento e necessari per dimostrare la sua innocenza.

3. Profilazione tra conferme e novità

Le previsioni dell'allegato III, paragrafo 6, sui sistemi intelligenti per determinare il rischio di commissione del reato o di recidiva, e di profilazione (lett. d) ed e)) ripropongono non solo la necessità di coordinamento multilivello tra le fonti, ma

38. In base all'art. 12 dell'*AI Act* i sistemi ad alto rischio devono essere muniti di meccanismi per la registrazione automatica degli eventi ("log") per l'intera durata del ciclo di vita del sistema.

39. CAMON 2025, p. 3018.

40. Art. 15 comma 2 e art. 24 lett. h) della legge n. 132/2025.

41. Non introducono sul punto preclusioni, ammettendo che le risultanze dell'AI possano supportare una decisione anche sfavorevole, LUPARIA-FIORELLI 2022, p. 42.

42. CHELO 2025, p. 113.

43. LUPARIA-FIORELLI 2022, p. 39.

44. CAMON 2025, p. 3016.

45. In questi termini, con riguardo a "prove di verità" di matrice neuroscientifica, PALMA 2020, pp. 56-57.

anche criticità sul piano della coerenza interna dell'*AI Act*. L'ammissibilità o meno di questi sistemi è, infatti, questione da definire in coordinamento con l'art. 5 del regolamento, che individua quelli vietati perché generativi di rischi inaccettabili⁴⁶.

Aspetto problematico di questo intreccio è che l'art. 5 definisce questi sistemi mediante "fattispecie complesse, descritte attraverso nozioni talvolta generiche e, in ogni caso, costruite attorno a una serie di limiti, espliciti o impliciti"⁴⁷.

In questo senso emblematica è proprio la lett. d) dell'art. 5 che, da un lato, in apparente contraddizione con le sopra indicate lettere d) ed e) dell'allegato III, vieta l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di AI per prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione o della valutazione dei tratti e delle caratteristiche della personalità; dall'altra, ammette, però, quei sistemi di AI utilizzati a sostegno della valutazione umana del coinvolgimento oggettivamente comprovato e verificabile di una persona in un'attività criminosa.

Il predetto divieto opera a tutela della presunzione d'innocenza⁴⁸ e del principio di materialità del diritto penale⁴⁹. La definizione dei sistemi intelligenti predittivi e di profilazione esterni alla sua area rileva, in particolare, quale "coefficiente di resistenza" di un diritto penale del fatto, in quanto "se l'attività giurisdizionale concretizza l'ordinamento è evidente che le sue disposizioni sono le norme di chiusura dello stesso, volte ad assicurare la sua complessiva tenuta"⁵⁰.

Per poter comprendere quali sistemi di profilazione e di predizione siano ammissibili è necessario

operare prima di tutto un previo distinguo tra predizione e profilazione. Partendo dalla profilazione, nonostante l'*AI Act* richiami sul punto la nozione del GDPR, riferimento specifico per il contesto penale non può che essere la direttiva (UE) 2016/680, c.d. LED, relativa 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, nonché alla libera circolazione di tali dati⁵¹. In attuazione dell'atto sovranazionale, il d.lgs. n. 51/2018, definisce la profilazione come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"⁵². Sulla scia della direttiva attuata e del GDPR, il decreto vieta, inoltre, espressamente le decisioni basate unicamente su un trattamento automatizzato che producono effetti negativi nei confronti dell'interessato, salvo che siano autorizzate dal diritto dell'Unione europea o da specifiche disposizioni di legge, in presenza di garanzie adeguate per i diritti e le libertà dell'interessato. È altresì precisato che queste decisioni non possono, in ogni caso, basarsi su quelle categorie di dati personali previsti dall'art. 9 del GDPR, il cui trattamento può generare il rischio di discriminazioni⁵³.

Questo divieto ed in generale le misure relative ai diritti dell'interessato e sul trattamento dei dati

46. Si segnala che le disposizioni del regolamento relative a questi sistemi sono applicabili già a partire dal 2 febbraio 2025 perché, come specificato al considerando 179, "sebbene la piena efficacia di tali divieti discenda dall'istituzione della governance e dall'esecuzione del presente regolamento, è importante anticipare l'applicazione di detti divieti per tenere conto dei rischi inaccettabili e avere un effetto su altre procedure, ad esempio nel diritto civile".

47. SPEZIALE 2025, p. 340.

48. In questo senso esplicito è il considerando 42 dell'*AI Act*.

49. Su questo principio, quale baluardo di un diritto penale di libertà, MANTOVANI 1992, p. 25.

50. RUGGIERO 2023, p. 1485.

51. Si rinvia per un'analisi della *ratio* e dei contenuti che contraddistinguono questo atto europeo a GALGANI 2019, pp. 5-8.

52. Così art. 2, lett. e, d.lgs. 51/2018; per un'analisi sul punto si rinvia a BACCARI-CONTI 2021, p. 711 ss.; ZIROLDI 2019.

53. Si tratta dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dei dati genetici, di quelli biometrici, intesi a

in sé, quale espressione dei principi di *privacy by design* e *privacy by default*, fungono da fattori di emersione e rimozione degli eventuali pregiudizi⁵⁴.

Rispetto a questo assetto, la previsione dell'allegato III, lett. e), che ammette l'impiego dell'AI profilativa può essere concepita come "confermativa": ne bilancia l'insidiosità attraverso le apposite cautele discendenti dalla qualificazione di questi sistemi ad alto rischio, compresi i requisiti in materia di set di dati di addestramento, convalida e prova.

Allo stesso tempo, l'art. 5 non fissa alcuna preclusione in ordine alla profilazione in sé, anche se "intelligente". Conformemente alla *ratio* di questa disposizione, ad essere vietati sono i sistemi di AI di valutazione del rischio individuale di commissione di reato che si fondino esclusivamente sulla profilazione. In questo modo l'area del divieto ne include solo un utilizzo e specificamente quello che, a causa della sua valenza determinante rispetto alla predizione del rischio reato, non ci tiene indenni da un diritto penale d'autore perché "proiettando la valutazione del singolo caso sullo sfondo di generalizzazioni statistiche in funzione predittiva, allontana la valutazione dal fatto"⁵⁵.

3.1. Il divieto dell'art. 5 tra predizione "decisoria" e predizione di polizia

Stesso discorso vale per i sistemi di AI in cui questa predizione è fondata unicamente sulla valutazione dei tratti e delle caratteristiche della personalità del soggetto e non sia a supporto di un previo giudizio umano attestante, sulla scorta di elementi fattuali obiettivi, il suo coinvolgimento in attività criminosa. Come chiarito dalle linee guida emanate dalla Commissione in funzione orientativa per l'interpretazione e l'applicazione dei divieti e

delle eccezioni dell'art. 5⁵⁶, la predetta ipotesi è da concepire come alternativa rispetto alla profilazione, in quanto categoria ampia a valenza residuale. Sul punto, aspetto, che è messo in luce dalla Commissione e che è idoneo ad influire sull'affidabilità e attendibilità di queste valutazioni, riguarda la distinzione, applicabile anche alla profilazione, delle caratteristiche personali in "Known, inferred or predicted": se le prime costituiscono input verificabili, le seconde e le terze o si basano su informazioni dedotte dal sistema da altri dati o sono stimate sulla base di modelli, con un grado di accuratezza inferiore al 100%⁵⁷.

Queste due ultime categorie sono proprio quelle informazioni che sarebbe più complesso e con tempi più lunghi ottenere da un'analisi manuale dei dati, con la conseguenza che essi rappresentano al tempo stesso il "valore aggiunto – ma anche il potenziale lesivo – dell'automazione"⁵⁸.

Nella dottrina nazionale, poi, la diffidenza verso sistemi che impiegano aspetti afferenti alla personalità in funzione di *risk assessment* è strettamente connessa alla loro riconduzione alla c.d. "perizia criminologica", con conseguente operatività del divieto dell'art. 220, comma 2, c.p.p., quale norma, pertanto, di sbarramento⁵⁹.

In realtà, la predetta associazione appare non convincente tanto nel merito della somiglianza dei sistemi di AI in esame con la verifica peritale, essendo l'output l'esito dell'elaborazione di dati e non certo di esplorazione del foro interiore della persona, quanto per la sua eccessiva rigidità rispetto a quell'esigenza d'individualizzazione dell'accertamento che è imposta dai diversi istituti – afferenti sia alla fase delle indagini, sia a quella del giudizio, come pure al momento dell'esecuzione

identificare in modo univoco una persona fisica, e di quelli relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

54. PIETROCARLO 2023, p. 57.

55. MANES 2020, p. 13.

56. Si tratta delle *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, doc. C (2025) 5052, che costituiscono, come esplicitato da SPEZIALE 2025, p. 345, uno strumento di soft law privo di efficacia vincolante.

57. In proposito il paragrafo 4.2.1. delle *Guidelines*.

58. MERLER 2023, p. 688.

59. MACRÌ 2025, p. 11 ss.

della pena – che impongono, ancorché in misura diversa, un giudizio personologico⁶⁰.

I sistemi predittivi sono idonei a soddisfare le esigenze valutative imposte da queste differenti fasi, essendo distinguibili in quelli: (1) *pre-crime*⁶¹, che sono impiegabili nella gestione della sicurezza pubblica e specificamente nella attività di polizia⁶² per fare previsioni su futuri eventi criminali; (2) *pre-trial*, che consentono la prognosi di pericolosità per l'applicazione di misure cautelari custodiali; e, infine, (3) di *sentencing*, che sono utilizzabili per la commisurazione della pena e la valutazione del rischio recidiva⁶³.

L'allegato III, paragrafo 6, sembra riferibile sulla base della formulazione testuale ai sistemi di *pre-trial* e di *sentencing*. Questa conclusione è confermata dalle linee guida della Commissione, che ne delimitano l'operatività, in conformità all'art. 5, in funzione di ausilio della decisione dell'autorità competente che si basi già su fatti oggettivi e verificabili, direttamente connessi a un'attività criminosa⁶⁴.

Tale funzione di ausilio deve comunque fare i conti, in particolare per i sistemi AI di *sentencing*,

con la necessità di adottare misure sanzionatorie che siano idonee a “perseguire quei risultati di individualizzazione e di risocializzazione fissati dalla Costituzione”, superando quella “concezione processuale tuttora saldamente ancorata ad una giustificazione retributiva della pena e ad anacronistici retaggi del tecnicismo giuridico”⁶⁵.

Ma la predizione intelligente con cui siamo chiamati a confrontarci ha carattere eminentemente probabilistico, operando secondo regole di tipo essenzialmente statistico e di natura criminologica⁶⁶, con la conseguenza che l'auspicata individualizzazione può essere supportata dall'impiego di questi *tool* solo laddove l'output, che sia ottenuto anche mediante elaborazione di dati personalistici, venga calato nella specificità del caso concreto.

Ritornando alla predetta decisione umana oggettivamente fondata e verificabile, con cui le risultanze intelligenti saranno chiamate ad integrarsi in via subalterna, interessante è il tentativo delle linee guida della Commissione di definirla alla luce delle statuizioni adottate dalla Corte di giustizia in ordine al divieto di decisioni completamente automatizzate sul rischio che i passeggeri

60. Come chiarito da PULITO 2025, p. 16, la valutazione della personalità dell'imputato rileva: nella fase delle indagini per l'applicazione delle misure cautelari; nel giudizio per la commisurazione della pena o per l'applicazione delle misure di sicurezza; nella fase dell'esecuzione della pena per una concreta determinazione del trattamento penale.

61. GIRALDI 2020, p. 47.

62. SORBELLO 2019, p. 377, definisce la polizia di sicurezza come quelle “varie attività finalizzate al riscontro e alla ricerca di situazioni ‘oggettive’ di pericolo o di inizio di attività criminose (...) Essa ha carattere preventivo in quanto è tesa ad impedire qualunque violazione dell'ordine sociale e si differenzia dalla polizia giudiziaria le cui funzioni sono esercitabili, alle dipendenze e sotto la direzione dell'autorità giudiziaria, all'emergere degli indizi di un fatto penalmente rilevante”.

63. PERRONE 2022, p. 83.

64. Al paragrafo 5.3.2. della *Guidelines on prohibited artificial intelligence practices* sono indicati, come esempi di sistemi AI che non rientrano nel divieto dell'art. 5 lett. d), le seguenti ipotesi: 1. “Un giudice conduce un'udienza per la custodia cautelare di una persona accusata di un reato grave, per valutare se possano essere applicate misure non detentive. La decisione si basa sulla valutazione di elementi concreti che giustificano la custodia cautelare, come il rischio di reiterazione del reato, fuga o intralcio alle indagini. A supporto, il giudice utilizza uno strumento di valutazione del rischio basato sull'IA, addestrato su dati relativi a precedenti penali in casi simili e su fattori quali età, comportamento sociale, reddito e occupazione”; 2. “Un sistema di IA è utilizzato per supportare la valutazione di un agente nel determinare il rischio che una persona sottoposta a misure alternative violi le condizioni di rilascio o si sottragga alla giustizia, sulla base di comportamenti criminali passati e fatti oggettivi che giustificano il sospetto, come il rispetto delle condizioni di rilascio, esiti di valutazioni psicologiche e raccomandazioni dei servizi sociali. Sulla base di tali informazioni, l'agente decide se mantenere o modificare le condizioni”.

65. VENTUROLI 2022, p. 256.

66. ALGIERI 2021, p. 730.

aerei siano coinvolti in reati gravi, ai sensi della direttiva (UE) 2016/681, c.d. direttiva PNR. Come messo in luce dalla dottrina, questo divieto rileva quale regola di valutazione della prova che si applica, per ragioni di tutela della libertà individuale e del diritto di difesa, anche alle determinazioni degli organi inquirenti relative ad atti d'indagine per verificare il coinvolgimento criminale⁶⁷.

Il richiamo a queste statuizioni della Corte di giustizia, e specificamente alla funzione assegnata alla valutazione umana di strumento di controllo individualizzante ed antidiscriminatorio degli esiti sfavorevoli discendenti dai trattamenti automatizzati⁶⁸, conferma come la decisione umana che l'AI predittiva deve supportare debba avere di per sé un'autonoma attendibilità, sulla base di dati oggettivi e verificabili, implicanti una relazione diretta tra il soggetto e il reato.

La predetta verificabilità costituisce, inoltre, requisito che dovrebbe evitare o comunque rendere sindacabili sia fenomeni di *automation bias*, sia quelli di recepimento dell'output per rafforzarne *bias* del giudice, foriere di diseguaglianza⁶⁹. Funzionale a questo duplice ruolo è il diritto, espressamente previsto dall'*AI Act* per le autorità nazionali che devono far rispettare gli obblighi unionali a tutela dei diritti fondamentali, di richiedere in relazione all'uso dei sistemi di AI ad alto rischio dell'allegato III l'accesso a qualsiasi documentazione creata o mantenuta a norma del regolamento⁷⁰. Alla luce di questa disposizione sembra possibile ritenere che l'autorità giurisdizionale, in via di adozione e soprattutto di ricorso del provvedimento supportato dal sistema predittivo, possa accedere

ai dati di sviluppo e addestramento per verificare la violazione del diritto alla non discriminazione, autorizzando, a tutela dell'effettività del contraddittorio e dello stesso diritto di difesa, il potenziale reo o soggetto interessato a farlo.

Quanto sopra potrebbe contenere il rischio d'emersione per mezzo dell'AI predittiva di un inaccettabile *Tätertyp*⁷¹, della giustificazione di misure pregiudizievoli nell'azione di contrasto sulla base di pericolosi profili di autori derivanti dalla stigmatizzazione criminale di gruppi o categorie sociali⁷², quale versione "intelligente" di un diritto penale del nemico⁷³.

Queste considerazioni valgono a maggior ragione per i sistemi *pre-crime* e specificamente di *predictive policing*, la cui ammissibilità richiede di distinguere tra quelli che consentono di localizzare le aree di probabile compimento di attività criminali (*hot spots*), a garanzia della tempestività ed efficienza dell'intervento (c.d. *place-based*)⁷⁴, e quelli, invece, che identificano coloro che potrebbero commettere reati (c.d. *person-based*)⁷⁵.

Per la Corte federale tedesca, chiamata ante *AI Act* a pronunciarsi sul trattamento automatizzato dei dati per finalità di polizia, i *place-based systems* sarebbero ammissibili perché l'interferenza nei diritti fondamentali è lieve, essendo l'analisi o la valutazione dei dati non finalizzata ad approfondimenti personali⁷⁶. In presenza, invece, di questi approfondimenti, la tutela del diritto alla autodeterminazione informativa impone che la base giuridica che ne consente il ricorso fissi pure le condizioni per garantire che l'impatto sui diritti e sulle libertà costituzionali degli individui sia

67. TROISI 2019, p. 178.

68. Espliciti in questi termini i paragrafi 157 e 203 di Corte di giustizia, Grande Sez., 21 giugno 2022, *Ligue des droits humains*, C-817/19.

69. Su questi fenomeni, nonché sulla presenza pure di *bias* strutturali del sistema legale, vedi FERRARA 2025, pp. 144-145.

70. Art. 77, par. 1 dell'*AI Act*.

71. Sull'origine di questo concetto e la sua applicazione nel diritto penale della Germania nazista BRICOLA 1973, p. 29 ss.

72. CASTELS RENARD 2022, pp. 100-102.

73. Su caratteristiche e contenuti del diritto penale del nemico, dall'elaborazione che si deve Jakobs, e quale paradigma concettuale della politica penale DONINI-PAPA 2007.

74. UTSET 2021, p. 179.

75. BASILE 2022, p. 6.

76. *Bunderversfassungsgericht*, I Senato (Presidente Stephan Harbarth), 16 febbraio 2023-1 BvR 1547/19, 1 BvR 2634/20.

proporzionato al bene giuridico tutelato e al pericolo allo stesso da prevenire⁷⁷. Com'è stato messo in luce con riferimento ad altre pronunce della Corte⁷⁸, espressive di analogo orientamento, il predetto diritto all'autodeterminazione informativa "va oltre la tutela della privacy e non si limita ad informazioni sensibili per loro natura" identificandosi con "il potere di determinare, in sé, la divulgazione e l'utilizzo dei [suoi] dati personali, anche se connotati da un contenuto informativo minimo"⁷⁹.

A causa dei rischi per diritti anche di questo tipo, è stato sostenuto con riferimento all'*AI Act* che i *person-based systems* siano del tutto vietati⁸⁰, mentre quelli *place-based systems* sarebbero ammessi ma laddove "puri", cioè predittivi di un rischio criminale impersonale e fondato su dati spaziali o statistici⁸¹. Questa tesi appare condivisibile, ancorché forse eccedente rispetto alla portata dell'eccezione prevista dall'art. 5 lett. d), ma non può non essere condivisa per la ragione dirimente che in presenza di sistemi misti non è facile stabilire quale sia stato il fattore determinante (spaziale o personologico) che ha influito sull'output⁸².

Nel silenzio della legge n. 132/2025, questione, di contro, che rimane aperta afferisce ancora una volta a quale debba essere l'istituto processuale che dia veste alle risultanze dei sistemi predittivi spaziali ammessi, consentendo di farli transitare nel processo. Prima ancora che per ragioni di garanzia, una critica interazione tra uomo e macchina, imposta dal paradigma *human-centred AI*,

impone di concepirli quali prove indiziarie soggette ai requisiti prescritti dall'art. 192 c.p.p.⁸³

In generale, come anche recentemente confermato dall'Unesco, "il sistema giudiziario dovrebbe puntare a utilizzare gli strumenti di AI per rafforzare, e non per sostituire, il giudizio umano"⁸⁴.

4. *Scraping* e dati biometrici: usi legittimi secondo l'autodeterminazione informativa

Il diritto all'autodeterminazione informativa costituisce il fulcro anche del divieto di cui alla lett. e) dell'art. 5 per i sistemi di AI che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da Internet o da filmati di telecamere a circuito chiuso.

Con questo divieto, insieme a quelli di cui alle lett. g) e h), l'*AI Act* copre le tecnologie biometriche applicate alla sicurezza, che sono suddivisibili nelle applicazioni di autenticazione ed in quelle di sorveglianza⁸⁵. Quest'ultime, in particolare, sono state considerate espressione della c.d. *crime society*, di una società che, nell'illusione di controllare la percezione di un rischio reato pervasivo ed onnipresente, ammette strumenti di controllo di massa, che, in realtà, finiscono per alimentare il senso di insicurezza⁸⁶.

Con specifico riferimento allo *scraping*, è, soprattutto, evidente la connessione con quel fenomeno che è stato definito di "datificazione" delle nostre esistenze, quale "possibilità di convertire ogni

77. MERLER 2023, p. 691.

78. Si tratta delle sentenze del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *Online Durchsuchung* e del 2 marzo 2010 sulla *data retention*, con cui sono stati dichiarati incostituzionali rispettivamente il § 5 co. 2, n. 11, della Legge sulla protezione della Costituzione del Nord Reno Westfalia in materia di raccolta e trattamento dei dati degli utenti, e i §§ 113a e 113b del *Telekommunikationsgesetz*, come modificato dalla legge di riforma del settore delle telecomunicazioni e delle altre misure d'indagine sotto copertura. Per un commento ad entrambe le sentenze FLOR 2012, p. 7.

79. FLOR 2015, p. 235.

80. BARONE 2024, p. 1058.

81. CAMALDO 2024, p. 244.

82. Per le difficoltà di distinguo per sistemi di questo tipo cfr. il paragrafo 5.3.1. della *Guidelines on prohibited artificial intelligence practices*.

83. CAMALDO 2024, p. 245.

84. Unesco, *Guidelines for the use of AI Systems in Courts and Tribunals*, p. 32.

85. PIZZOLANTE 2025, p. 158.

86. Su questa ricostruzione sociologica che si deve a Koops si rinvia, anche per i relativi riferimenti bibliografici, a GALLI 2022, p. 121.

aspetto della vita (privata e sociale) in dati digitali da raccogliere e analizzare⁸⁷. Il diritto all'autodeterminazione informativa protegge questi dati quale propagazione virtuale della nostra personalità, consentendo la tutela anche delle differenti aree informatiche in cui si trovano⁸⁸. Prendendo a prestito le parole d'insigne Maestro "la libertà in rete, tuttavia, non vale solo contro l'invasione degli Stati, ma si proietta anche verso i nuovi 'signori dell'informazione' che, attraverso le gigantesche raccolte di dati, governano le nostre vite. Di fronte a tutto questo la parola 'privacy' evoca non solo un bisogno d'intimità, ma sintetizza le libertà che ci appartengono nel mondo nuovo dove ormai viviamo"⁸⁹.

Con specifico riferimento allo *scraping* non mirato d'immagini facciali, di cui al regolamento in esame, l'inclusione dello spazio aperto d'Internet è espressione di questo retroterra, chiamando in causa, in particolare, la conformità al principio di lealtà del trattamento dati, che è codificato al comma 2 all'art. 8 della Carta europea dei diritti fondamentali⁹⁰. A questo principio sono ispirati gli orientamenti espressi nel caso di *Clearview AI* dal Garante europeo della protezione dei dati e dal nostro Garante privacy. In particolare, quest'ultimo ha sostenuto che la mera accessibilità pubblica delle immagini non è sufficiente a giustificare lo *scraping* in quanto gli interessati non possono ragionevolmente aspettarsi che le proprie immagini vengano utilizzate per finalità di riconoscimento facciale, per cui non hanno manifestato il proprio consenso⁹¹. Con specifico riferimento al contesto di *law enforcement*, il Garante europeo⁹² ha chiarito, inoltre, che se il trattamento iniziale dei dati

per finalità private non è conforme al GDPR, le autorità di contrasto non li possono utilizzare in quanto l'obiettivo generale di migliorare l'efficienza nella lotta ai reati gravi non costituisce, di per sé, una giustificazione valida per la raccolta e il trattamento indiscriminato di dati⁹³.

Il divieto dell'*AI Act* sullo *scraping* non mirato, ponendosi in conformità con questi orientamenti, va concepito alla luce dei principi e criteri del GDPR e della direttiva LED, la quale, peraltro, impone all'art. 10 che il trattamento di dati sensibili operato dalle autorità di contrasto sia informato al criterio della "stretta necessità"⁹⁴.

La sensibilità del dato, per i profili anche discriminatori che vi possono essere connessi, è aspetto centrale altresì nel divieto di cui alla lett. g) dell'art. 5, in ordine ai sistemi di categorizzazione biometrica per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda, però, l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente nell'ambito delle attività di contrasto.

L'*AI Act* definisce i dati biometrici come quelli "personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici"⁹⁵. Questa nozione si pone ancora una volta in continuità con il GDPR, che vieta l'impiego di questi dati, salvo se, tramite il loro trattamento, con le dovute garanzie, si possa giungere all'identificazione univoca o all'autenticazione di una persona fisica, in presenza del

87. FLOR 2012, p. 13.

88. In base al tenore letterale della previsione sono ammissibili trattamenti di dati che avvengano "per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge".

89. RODOTÀ 2010, p. 342.

90. BELVINI 2026, p. 157.

91. Garante Privacy, Ordinanza ingiunzione nei confronti di *Clearview AI* del 10 febbraio 2022, n. 9751362/2022.

92. Garante europeo della protezione dei dati, *Parere sull'uso di Clearview AI da parte di Europol* (Case 2020-0372).

93. In questi termini espliciti le *Guidelines on the use of facial recognition technology in the area of law enforcement*, adottate il 26 aprile 2023 dal Comitato europeo per la protezione dei dati (EDPB).

94. Per l'incompatibilità di questo criterio proprio con forme di *screening* generalizzati via web vedi BELVINI 2026, p. 160.

95. Art. 3, n. 34 dell'*AI Act*.

requisito alternativo del consenso esplicito oppure della necessità per ragioni di pubblico interesse⁹⁶.

L'area di eccezione ammessa dall'*AI Act* rientra in quest'ultima ipotesi e di conseguenza soggiace agli ulteriori requisiti che sono fissati dal sopraccitato art. 10 della direttiva LED⁹⁷, operando, ad avviso di chi scrive, a causa della considerazione dei sistemi di etichettatura e filtraggio ammessi come ad alto rischio, come fattore di emersione di ulteriori cautele.

L'autonomia parziale di questa disciplina con riferimento all'area penale comporta, però, anche la permanenza del quadro di pesi e contrappesi che le corti sovranazionali hanno già individuato per la raccolta di dati biometrici da parte delle forze dell'ordine, in conformità ai diritti previsti dagli artt. 7-8 e ai criteri di necessità e proporzionalità dell'art. 52 della Carta europea dei diritti fondamentali, e tenendo in debito conto anche il tipo di tecnologia biometrica utilizzata, nonché la durata della conservazione dei dati biometrici e le categorie di soggetti coinvolti⁹⁸.

Sul punto una recente pronuncia della Corte di giustizia ha ribadito come la mera sussistenza di una o più ragioni plausibili di sospetto reato non è sufficiente a giustificare la raccolta di dati biometrici, che non può mai rivestire carattere sistematico⁹⁹. Per la Corte, inoltre, questa raccolta laddove legittimamente operata secondo le disposizioni nazionali, può non essere soggetta ad un periodo massimo di conservazione, purché siano fissati termini periodici per verificare la permanenza della necessità di conservare tali dati¹⁰⁰.

Quanto sopra delinea un quadro frastagliato che forse avrebbe imposto, per le peculiarità dei sistemi di AI in attività di contrasto, l'adozione

di previsioni apposite o di specifici meccanismi di raccordo con la disciplina europea sul trattamento dati, come precisata dalla giurisprudenza sovranazionale e dalle Autorità di controllo: l'*over-regulation*, infatti, "è sempre un'arma a doppio taglio, nella misura in cui, se è vero che garantisce l'esistenza di più normative che da fronti diversi proteggono gli stessi diritti, dall'altro, se non ben regolato, rischia di ottenere l'effetto opposto alla finalità iniziale, mettendo a rischio quegli stessi diritti che si prefiggeva di tutelare"¹⁰¹.

4.1. Il riconoscimento facciale tra impieghi ed eccezioni "proporzionali"

Questa esigenza di equilibri "dinamici" tra sicurezza e diritti fondamentali è rinvenibile anche alla base della disciplina europea sui sistemi d'identificazione biometrica. Per comprendere a pieno le differenze di regolamentazione adottate, bisogna partire dalla distinzione tra sistemi di riconoscimento facciale in tempo reale e quelli da remoto (*enterprise*). Nel primo caso la comparazione con i contenuti di una banca dati predefinita avviene contestualmente alla cattura delle immagini, mentre nella seconda versione è svolta a posteriori.

Pur non generando forme di sorveglianza di massa, i sistemi di riconoscimento facciale *enterprise* non sono indenni da rischi o da margini di errore; per questo, in base al combinato disposto degli artt. 5, lett. h), e 26 del regolamento europeo¹⁰², sono consentiti, ma nel rispetto di precise condizioni.

In particolare, previa autorizzazione dell'autorità competente, risultano, oltre che soggetti ai requisiti generali previsti per tutti i sistemi ad

96. MOLLO 2024, p. 108, che precisa che l'*AI Act* non può costituire in ogni caso il fondamento giuridico per il trattamento dei dati personali.

97. Per il considerando 94 dell'*AI Act* l'uso in attività di contrasto soggiace a tutti i principi di cui all'articolo 4, paragrafo 1, della Direttiva (UE) 2016/680, tra cui liceità, correttezza e trasparenza, determinazione delle finalità, esattezza e limitazione della conservazione.

98. Sugli orientamenti adottati sul punto dalla Corte EDU vedi PIZZOLANTE 2025, p. 182.

99. Corte di giustizia, 19 marzo 2026, C-371/24.

100. Corte di giustizia, 20 novembre 2025, C57/23.

101. FALLETTA-MARSANO 2024, p. 11.

102. L'art. 26 dell'*AI Act* precisa che "in nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa".

alto rischio, impiegabili solo nell'ambito d'indagini su uno specifico reato per la ricerca mirata di una persona che sia stata per questo condannata o sia sospettata di averlo commesso¹⁰³. Alla luce del considerando 95 il carattere mirato comporta, inoltre, limiti sia sul luogo e sull'ambito temporale di utilizzo sia sugli input che possono alimentare il sistema, da individuare in un set di dati chiuso di filmati acquisiti legalmente. Aspetto ulteriormente interessante è quello relativo alla fissazione da parte del regolamento di quella che è stata definita “una regola di utilizzabilità degli output di questi sistemi di identificazione biometrica”¹⁰⁴, in forza della quale nessuna decisione che produce effetti giuridici negativi in capo a una persona può fondarsi esclusivamente su di essi.

Ne fuoriesce così un modello *rights driven*¹⁰⁵ particolarmente stringente e munito di un livello di specificità tale da impattare direttamente sul piano nazionale. Invero, in questa prospettiva, questione che andrebbe preliminarmente chiarita è se, salva l'ipotesi d'identificazione iniziale di un sospettato che tale sia in base a previi fattori oggettivi, negli altri casi l'assenza di autorizzazione si traduca sempre nel divieto di utilizzabilità¹⁰⁶. La risposta positiva a questo quesito travolgerebbe anche impieghi del nostro sistema SARI *enterprise* ammessi dal

nostro Garante privacy sul presupposto che questo strumento coadiuva e non sostituisce l'attività dell'operatore di polizia in processi d'identificazione, come quelli ai sensi dell'art. 349 c.p.p.¹⁰⁷ Un tale esito può sembrare eccessivo, a maggior ragione se pensiamo che il regolamento funge da “statuto minimo”, che sarebbe derogabile a livello nazionale solo con disposizioni più restrittive¹⁰⁸.

Questo aspetto va a maggior ragione tenuto presente con riguardo alla disciplina europea sui sistemi di identificazione biometrica in tempo reale in spazi accessibili al pubblico: ferma l'immediata operatività del divieto in sé, per le ipotesi d'impiego eccezionalmente ammesse la disciplina sovranazionale non è immediatamente applicabile, ma fissa degli standard che per la valenza garantistica assiologica sono già vincolanti.

La delega al legislatore dello Stato membro per l'adozione della relativa disciplina nazionale conforme a questi standard, è, infatti, una delega “limitata”, che può operare nel *range* dei requisiti abilitativi sovranazionali fissati dall'art. 5 dell'*AI Act*¹⁰⁹. Questi requisiti, peraltro, ancorando il principio di proporzionalità ad un fondamento legale, migliorano, in forza della predetta formalizzazione, la capacità di resistenza dei diritti contro

103. Questa norma prevede, peraltro, a favore di una parziale *disclosure*, che ciascun uso di tali sistemi di IA ad alto rischio è documentato nel relativo fascicolo di polizia e messo a disposizione della pertinente autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati, su richiesta, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto.

104. VASTA 2024, p. 284.

105. Per la differenza con il modello cinese *state driven* e con quello americano *market driven* vedi BOTTARI-CURRAO 2026, p. 4 ss.

106. CESARI 2026, p. 185.

107. VELE 2026, p. 30.

108. DE MARTIS 2025, p. 183.

109. Esplicito in questo senso è il paragrafo 5 dell'art. 5 dell'*AI Act*, che stabilisce quanto segue: “Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota ‘in tempo reale’ in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, primo comma, lettera h), e ai paragrafi 2 e 3. Gli Stati membri interessati stabiliscono nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, primo comma, lettera h), compresi i reati di cui alla lettera h), punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto. Gli Stati membri notificano tali regole alla Commissione al più tardi 30 giorni dopo la loro adozione. Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota”.

derive securitarie rispetto alle quali l'AI potrebbe segnare un punto di non ritorno.

Nello specifico, l'articolato impianto normativo in questo modo non intende solo evitare la compromissione dei già richiamati diritti alla privacy e alla non discriminazione, ma anche di quelle libertà universalmente riconosciute – da quella di movimento a quella manifestazione¹¹⁰ – che sono funzionali a preservare la dignità umana nel contesto di una società democratica¹¹¹.

Ciò comporta a livello nazionale che, nonostante la proroga fino al 31 dicembre 2027 del divieto di questi sistemi di riconoscimento *real time* con moratoria per quelli effettuati a certe condizioni dall'autorità giudiziaria¹¹², nel silenzio della legge n. 132/2025 questa moratoria sia travolta dal divieto sovranazionale fino all'emanazione di un'apposita disciplina che regolamenti gli usi eccezionali nel rispetto dei criteri fissati dal legislatore europeo.

Venendo ai contenuti di questi criteri, salvo situazioni di urgenza debitamente giustificate¹¹³, pre-condizione europea necessaria per gli impieghi ammessi dei sistemi di riconoscimento facciale *real time* in luoghi aperti al pubblico è che essi siano autorizzati, previa registrazione nella relativa banca dati e completamento della valutazione d'impatto sui diritti fondamentali¹¹⁴, da un'autorità giudiziaria o da un'autorità amministrativa

indipendente dello Stato membro sulla base di prove oggettive o indicazioni chiare. Su scia della giurisprudenza sovranazionale adottata per altri sistemi d'indagine tecnologica, è possibile ritenere che la legge nazionale, che dovrà prevedere nel dettaglio l'iter di autorizzazione, richieda il vaglio preventivo del giudice su richiesta del pm¹¹⁵.

In ogni caso, questo vaglio deve avvenire, sulla base del testo sovranazionale, nel rispetto delle regole degli Stati membri che fissano limitazioni temporali, geografiche e personali e deve avere ad oggetto la necessità e la proporzionalità della misura rispetto ad almeno una delle seguenti finalità: (a) la ricerca mirata di persone scomparse e di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale; (b) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; (c) la localizzazione o identificazione di una persona sospettata, indagata o ricercata per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

Queste tre ipotesi costituiscono delle ragioni giustificative eccessivamente ampie, richiamano

110. In relazione a questa libertà BORGIA 2021, p. 15, mette in luce il c.d. *chilling-effect* che può essere generato da questi sistemi di AI, quale effetto inibitore alla partecipazione a manifestazioni pubbliche per il timore di essere identificati.

111. CAVALIERE 2020, p. 8.

112. Proroga prevista dall'art. 2, comma 6-*quater*, del d.l. n. 200/2025, c.d. "Decreto Milleproroghe 2026", convertito nella legge n. 26/2026 del 27 febbraio 2026.

113. Il paragrafo 3, ultima parte, dell'art. 5 dell'*AI Act*, stabilisce, in presenza di situazioni di questo tipo, che è possibile iniziare ad usare il sistema senza autorizzazione, a condizione, però, che sia richiesta entro 24 ore. Se tale autorizzazione è respinta, l'uso deve essere interrotto con effetto immediato e cancellazione dei relativi dati.

114. Questa valutazione è prevista dall'art. 27 dell'*AI Act*, il quale indica tra gli elementi che devono essere considerati: "c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13; e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; f) le misure da adottare qualora tali rischi si concretizzino".

115. BORGIA 2021, p. 22. In questa prospettiva anche il paragrafo 10.2.2.2. delle *Guidelines*, per cui "l'indipendenza richiesta dall'articolo 5, paragrafo 3, dell'*AI Act* (...) implica che l'autorità che autorizza debba essere indipendente dall'autorità che utilizza il sistema RBI. Ciò si applicherebbe non solo alla polizia, ma anche ai casi di giudici istruttori o pubblici ministeri che supervisionano il lavoro della polizia e l'uso di sistemi RBI per i quali è richiesta un'autorizzazione".

“scenari emergenziali” che possono consentire praticamente sempre il ricorso “anche ai mezzi più controversi per conseguire lo scopo prefissato”¹¹⁶. In questo senso particolarmente rilevante è la condizione di cui alla lett. (b): i requisiti di attualità e realtà, previsti per la minaccia o l'attacco terroristico, ne impongono una considerazione *case by case*, alla luce delle specificità della situazione concreta, con possibilità, già ammessa per altri strumenti investigativi invasivi, di poterli ritenere sussistenti anche quando non si possa stabilire con sufficiente probabilità che la minaccia o l'attacco si concretizzeranno in futuro¹¹⁷.

Alla luce, poi del considerando 33 dell'*AI Act* il concetto di minaccia imminente alla vita o all'incolumità fisica delle persone è declinabile in modo da includere anche quella alle infrastrutture critiche, da cui possa discendere un grave danno alla popolazione o all'esercizio delle funzioni fondamentali dello Stato. Questa estensione appare ragionevole in considerazione di quelli che oggi costituiscono modalità frequenti, anche in forma, peraltro, *cyber*¹¹⁸ degli attacchi – di matrice terroristica o addirittura di *ius ad bellum*¹¹⁹ – rivolti alle infrastrutture di settori come sanità ed energia. Sembra rispondere alla medesima logica spiccata preventive-securitaria l'elencazione dei reati di cui all'allegato II¹²⁰ del regolamento, per cui è

ammesso ai sensi della lett. (c) la localizzazione o identificazione di condannato-sospettato mediante riconoscimento biometrico *real time*.

Come chiarito dalla Commissione si tratta o di “reati europei”, rientranti nelle ipotesi di cui all'articolo 83 TFUE, che legittimano una competenza penale europea concorrente¹²¹, o di quelli per cui può essere emesso un mandato d'arresto europeo¹²². La possibile, ulteriore considerazione di questi reati come gravi ai sensi anche della giurisprudenza sovranazionale¹²³ potrebbe non escludere censure, che, ad avviso di chi scrive, non afferiscono alla riconoscibile lesività degli stessi in astratto, quanto più che altro al rischio di (dis)armonizzazione applicative tra gli Stati. Nello specifico, l'indicazione nominale è operata mediante macro-categorie che si prestano più ad indicare forme di criminalità che reati, al fine di abbracciare la complessa “fenomenologia concreta dei comportamenti ‘criminologicamente rilevanti’”¹²⁴. Non sembra essere dirimente rispetto a ciò l'indicazione della soglia di pena di almeno quattro anni, nonostante si tratti di un parametro generalmente impiegato e certamente conforme al principio proporzionalità. Il riferimento alla pena ha, infatti, una valenza in termini, in particolare, di congruità che dovrebbe sussistere tra la sua entità e la gravità che si attribuisce alla sfera di lesività

116. COLACURCI 2022, p. 21.

117. FLOR 2015, p. 236.

118. Per un'analisi statica su attacchi di questo tipo nel corso del 2025 si rinvia al Rapporto Clusit 2026.

119. GABRIELLI 2025, p. 80 ss.

120. Questi reati sono: terrorismo, sfruttamento sessuale di minori e pornografia minorile, traffico illecito di stupefacenti o sostanze psicotrope, traffico illecito di armi, munizioni ed esplosivi, omicidio volontario, lesioni gravi, traffico illecito di organi e tessuti umani, traffico illecito di materie nucleari e radioattive, sequestro, detenzione illegale e presa di ostaggi, reati che rientrano nella competenza giurisdizionale della Corte penale internazionale, illecita cattura di aeromobile o nave, violenza sessuale, reato ambientale, rapina organizzata o a mano armata, sabotaggio, partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati.

121. Questa competenza è anche definita indiretta, in quanto è devoluto al legislatore europeo un giudizio di meritevolezza di pena senza diretta potestà punitiva, dovendo le “norme minime” relative alla definizione dei reati e delle sanzioni passare attraverso il contributo di recepimento del singolo Stato membro. Senza alcuna pretesa di esaustività, in proposito, vedi PICOTTI 2011, p. 207 ss.; GRASSO 2011, p. 2324 ss.; PAONESSA 2009, p. 237 ss.

122. In proposito il paragrafo 9.3.4. delle *Guidelines*.

123. Sulle pronunce della Corte di giustizia, che – con specifico riferimento alla *data retention* – hanno esemplificato le fattispecie rientranti nella nozione di criminalità grave, riferendosi alla criminalità organizzata e al terrorismo, vedi LUBERTO 2025, p. 74.

124. Così, con riguardo all'allora normazione comunitaria di diritto penale dell'economia, PALIERO 2000, p. 489.

selezionata¹²⁵, quale manifestazione della ragionevolezza intrinseca della fattispecie. Da quanto sopra, consegue, pertanto, che se è corretto il riferimento al limite massimo, perché espressione del disvalore del tipo di reato, non è condivisibile il *quantum* di questo limite (quattro anni), che appare eccessivamente basso; confrontato con il nostro ordinamento, potrebbe consentire di ritenere operante l'eccezione in esame per reati, per cui non sarebbe ammissibile procedere nemmeno alle intercettazioni.

Di tutt'altra valenza è la funzione garantistica attribuibile, invece, all'ulteriore condizione di una prognosi *ex ante* che l'autorità è chiamata a svolgere in ordine sia ai danni che deriverebbero dall'omesso impiego di questi sistemi di *AI real time*, sia alle conseguenze discendenti, di contro, dal suo utilizzo per i diritti e le libertà di tutte le persone interessate. In entrambi i casi questi effetti vanno valutati in termini di gravità, probabilità ed entità.

La prima parte di questo duplice giudizio controfattuale è, soprattutto, valorizzabile per far emergere quella dimensione di lesività effettiva, che rischia di essere dispersa dalla elencazione dei sopra definiti macro-reati rispetto ai quali può operare la finalità di cui alla lett. (c).

Si evidenzia che questi reati sono, peraltro, connotati da un marcata anticipazione dell'intervento penale¹²⁶, con la conseguenza che la verifica in esame potrebbe fungere da utile argine operativo.

In questa direzione si segnala, inoltre, che il richiamo all'offensività in concreto, operando qui come fattore di ammissione o esclusione del sistema intelligente di sorveglianza, non si espone a quelle censure che gli sono riferite quando funge, invece, da criterio di riduzione del "penale", consentendo al giudice di escludere dalla sfera d'azione della fattispecie le condotte inoffensive che vi rientrerebbero¹²⁷. Quest'ultimo uso entra in tensione con la formalità della legalità penale,

nella sua funzione di presidio anche sostanziale, che opera sia a "limitazione dell'attività valutativa del giudice nell'identificazione dei fatti rilevanti", sia ad "orientamento del comportamento del cittadino"¹²⁸.

Questa tensione non si registra, invece, per la offensività qui in esame: laddove ricorra la condizione cui alla lett. (c) la valutazione di dannosità sociale va riferita, infatti, ad una cornice d'interessi o beni che, anche se con i limiti segnalati, è stata delineata dal legislatore europeo, con la selezione dei reati di cui all'allegato II.

In realtà, anche in ordine alle altre finalità che consentono il ricorso al riconoscimento facciale *real time* (ricerca vittime-minaccia, attacco terroristico), il duplice giudizio controfattuale funge, comunque, da criterio esegetico applicativo, che non è estraneo al substrato di fondo che anima il principio di offensività¹²⁹.

La verifica imposta, pur non essendo riferibile alla prospettiva tradizionale del bene giuridico, meno in linea con l'*acquis* comunitario¹³⁰, spostata, di fatto, l'attenzione sul sacrificio dei diritti e delle libertà di tutte i soggetti coinvolti, compresi i terzi estranei, anche se in termini probabilistici-potenziati.

La considerazione di questo sacrificio non è avulsa dell'art. 52 della Carta europea dei diritti fondamentali. Stando alla formulazione testuale di questa previsione, la valutazione di necessità e idoneità della misura limitativa va infatti, condotta, secondo il criterio alternativo delle "finalità di interesse generale riconosciute dall'Unione" e della "esigenza di proteggere i diritti e le libertà altrui". Rispetto ad entrambi i criteri, il giudizio controfattuale qualitativo-quantitativo previsto dal regolamento consente il ricorso al mezzo investigativo intelligente in condizioni oggettive che devono essere particolarmente pregnanti.

In senso critico si potrebbe obiettare sul punto che, in realtà, con questo duplice accertamento

125. BRICOLA 1965, p. 311.

126. Sull'anticipazione dell'intervento penale con riguardo ai reati di terrorismo si rinvia a RISICATO 2019, p. 50 ss.

127. CADOPPI 2022, p. 258.

128. PAONESSA 2017, p. 308.

129. A favore di questa omogeneità di fondo tra l'offensività e i parametri di proporzionalità e ragionevolezza FORNASARI 2018, p. 1529.

130. Diffusamente su questi aspetti DE LIA 2019, p. 34.

controfattuale (danno da non impiego – compromissione dei diritti e le libertà di tutte le persone interessate dall'impiego) vengano semplicemente esplicitati i fattori di quello che rimane, comunque, un giudizio discrezionale di bilanciamento tra valori, tradizionalmente riferibile al principio di proporzionalità.

È vero che l'*AI Act* non muta la valenza sostanziale di questo principio, ma nel chiamarlo in causa nel suo ruolo di "conciliatore" tra "i due grandi criteri dell'ordine sociale: la libertà individuale e

la sicurezza sociale, l'individuo e lo Stato"¹³¹, gli conferisce, però, una consistenza propriamente fattuale.

Questa consistenza opera a favore di tutti i soggetti interessati, dal potenziale reo alle vittime, perché con riferimento agli "occulti" ed "imprevedibili" sistemi intelligenti comporta una maggiore ponderazione della decisione umana, con ricadute in termini di trasparenza e controllabilità della stessa e a favore di un diritto penale umano e contenibile.

Riferimenti bibliografici

- L. ALGIERI (2021), *Intelligenza artificiale e polizia predittiva*, in "Diritto penale e processo", 2021, n. 6
- A.C. AMATO MANGIAMELI (2023), *Tecno-diritto/regolazione*, in A.C. Amato Mangiameli, G. Saraceni (a cura di), "Cento e una voce di informatica giuridica", Giappichelli, 2023
- G.M. BACCARI, C. CONTI (2021), *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in "Diritto penale e processo", 2021, n. 6
- S. BARONA VILAR (2019), *Justicia penal desde la globalización y la postmodernidad hasta la neomodernidad*, in "Revista Boliviana de Derecho", 2019, n. 27
- G. BARONE (2024), *Artificial Intelligence Act: un primo sguardo al regolamento che verrà*, in "Cassazione penale", 2024, n. 3
- F. BASILE (2022), *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in G. Balbi, F. De Simone, A. Esposito, S. Manacorda (a cura di), "Diritto penale e intelligenza artificiale. Nuovi scenari", Giappichelli, 2022
- L. BELVINI (2026), *La disciplina dei software di riconoscimento facciale: rischi e prospettive*, in "Processo penale e giustizia", 2026, n. 1
- C. BERNASCONI (2022), *Dalla vittimologia al vittimocentrismo: cosa resta della tradizione reocentrica?*, in "discrimen.it", 15 marzo 2022
- C. BERNASCONI (2019), *A proposito di Caino*, in "discrimen.it", 25 settembre 2019
- K. BLOUNT (2021), *Applying the presumption of innocence to policing with AI*, in G. Vermeulen, N. Peršak, N. Recchia (Eds.), "Artificial Intelligence, Big Data and Automated Decision-Making in Criminal Justice", Maklu Publishers, 2021
- R. BORGES BLÁZQUEZ (2021), *Inteligencia artificial y proceso penal*, Cizur Menor, 2021
- G. BORGIA (2021), *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurolunitario*, in "legislazionepenale.it", 11 dicembre 2021
- M. BOTTARI, E. CURRAO (2026), *Riconoscimento facciale: tecnologie che corrono, diritti che frenano. Il caso italiano del Faceboarding*, in "federalismi.it", 25 marzo 2026
- F. BRICOLA (1973), *Teoria generale del reato*, in "Novissimo Digesto italiano", XIX, 1973
- F. BRICOLA (1965), *La discrezionalità nel diritto penale*, Giuffrè, 1965

131. FALATO 2018, p. 27.

- A. CADOPPI (2022), *Il “reato penale”. Teorie e strategie di riduzione della criminalizzazione*, Edizioni Scientifiche Italiane, 2022
- L. CAMALDO (2024), *Intelligenza Artificiale e investigazione penale predittiva*, in “Rivista Italiana di Diritto e Procedura Penale”, 2024, n. 1
- A. CAMON (2025), *Intelligenza artificiale, indagini preliminari e diritti di libertà*, in “Cassazione penale”, 2025, n. 10
- M.C. CANATO (2024), *Verso il superamento del “legal rick” europeo: Intelligenza artificiale e approccio proporzionale al rischio*, in “legislazionepenale.it”, 31 luglio 2024
- O. CARAMASCHI (2025), *Il costituzionalismo al cospetto dell’intelligenza artificiale: nuove sfide, quali soluzioni?*, in “Rivista italiana di informatica e diritto”, 2025, n. 1
- C. CASTELS RENARD (2022), *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (Eds.), “Constitutional Challenges in the Algorithmic society”, Cambridge University Press, 2022
- S. CAVALIERE (2020), *Il concetto di dignità umana nel diritto internazionale ed europeo: una breve nota ricostruttiva*, in “Euro-Balkan Law and Economics Review”, 2020, n. 2
- C. CESARI (2026), *Nuove tecnologie, dati biometrici e procedimento penale*, Cedam, 2026
- A. CHELO (2025), *Tutela della libertà morale nella formazione della prova penale*, Cedam, 2025
- C.M. CHRISTENSEN, M.E. RAYNOR, R. McDONALD (2015), *What Is Disruptive Innovation? Twenty years after the introduction of the theory, we revisit what it does – and doesn’t – explain*, in “Harvard Business Review”, 2015, n. 12
- M. COLACURCI (2022), *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in “sistemapenale.it”, 12 settembre 2022
- L.M. COLONE, M. ESPOSITO, L. MEGLIO, G. PAGNANELLI (2023), *Reati “spia” di femminicidio e pratiche locali di contrasto alla violenza di genere*, in “Sicurezza e scienze sociali”, 2023, n. 3
- F. CONSULICH (2024), *Il diritto penale al tempo dell’intelligenza artificiale. Prospettive punitive nazionali dopo l’AI ACT*, in “dirittodidifesa.eu”, 17 dicembre 2024
- A. DE LIA (2019), *“Ossi di seppia”? Appunti sul principio di offensività*, in “Archivio penale”, 2019, n. 2
- F. DE MARTIS (2025), *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, Cedam, 2025
- P. DI NICOLA TRAVAGLINI (2025), *Il femminicidio esiste ed è un delitto di potere*, in “Sistema penale”, 2025, n. 3
- M. DONINI, M. PAPA (2007), *Diritto penale del nemico*, Giuffrè, 2007
- F. FALATO (2018), *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall’ordine europeo di indagine penale*, in “Archivio penale”, 2018, n.1
- P. FALLETTA, A. MARSANO (2024), *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull’intelligenza artificiale e GDPR*, in “Rivista italiana di informatica e diritto”, 2024, n. 1
- A. FERRARA (2025), *The error in predictive justice systems. Challenges for justice, freedom, and human-centrism under EU law*, in “Freedom, Security & Justice: European Legal Studies”, 2025, n. 2
- R. FLOR (2022), *Data retention, accertamento e repressione dei reati e tutela dei diritti fondamentali dell’individuo: fiat iustitia ruat caelum*, in R. Flor, S. Marcolini (a cura di), “Dalla data retention alle indagini ad alto contenuto tecnologico”, Giappichelli, 2022
- R. FLOR (2015), *Dalla ‘Data retention’ al diritto all’oblio. dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive ‘de jure*

- condendo?*, in G. Resta, V. Zeno-Zencovich, "Il diritto all'oblio su Internet dopo la sentenza Google Spain", Roma TrE-Press, 2015
- R. FLOR (2012), *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in "Diritto penale contemporaneo", 20 settembre 2012
- G. FORNASARI (2018), *Offensività e post modernità: un binomio inconciliabile?*, in "Rivista Italiana di Diritto e Procedura Penale", 2018, n. 3
- G. GABRIELLI (2025), *La governance internazionale della cybersicurezza: cyber attacchi contro infrastrutture critiche nella prospettiva dello jus ad bellum*, in R. Brighi, G. Adinolfi (a cura di), "Governare la sicurezza degli (eco)sistemi cyberfisici. Regolamentazione, diritti e politiche", Giappichelli, 2025
- B. GALGANI (2019), *Giudizio penale, habeas data e garanzie fondamentali*, in "Archivio penale", 2019, n. 1
- F. GALLI (2022), *Law enforcement and Data driven Predictions at National and EU Level*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (Eds.), "Constitutional Challenges in the Algorithmic society", Cambridge University Press, 2022
- A. GIRALDI (2020), *Intelligenza artificiale e predictive policing nella rinnovata fase d'indagine*, in A. Massaro (a cura di), "Intelligenza artificiale e giustizia penale", 2020
- G. GRASSO (2011), *Il Trattato di Lisbona e le nuove competenze penali dell'Unione europea*, in "Studi in onore di Mario Romano", Iovene, 2011
- S. HASSAN, P. DE FILIPPI (2017), *The Expansion of Algorithmic Governance: From Code is Law to Law is Code*, in "Field Actions Science Reports", Special Issue, 2017, n. 17
- F. LAZZERI (2025), *In G.U. la L. 2 dicembre 2025, n. 181 (c.d. Legge sul femminicidio): una panoramica dei profili penalistici sostanziali e processuali*, in "sistemapenale.it", 3 dicembre 2025
- L. LESSING (2000), *Code is law. On liberty in cyberspace*, in "Harvard magazine", 2000
- M. LUBERTO (2025), *La riforma della data retention a fini di contrasto della criminalità Tra evoluzione tecnologica e garanzia dei diritti*, in "i-lex – Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale", 2025, n. 2
- L. LUPARIA, G. FIORELLI (2022), *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in "Diritto penale contemporaneo", 2022, n. 2
- L. MACRÌ (2025), *I primi passi dell'Italia verso l'impiego dell'IA nel processo penale e il calcolo del rischio di recidiva*, in "Giurisprudenza Penale", 2025, n. 2
- P. MAGGIO (2017), *Giustizia penale e tratta di esseri umani: i risvolti processuali della "vulnerabilità"*, in "Rivista di medicina legale", 2017, n. 2
- V. MANES (2020), *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in "discrimen.it", 15 maggio 2020
- F. MANTOVANI (1992), *Principi Fondamentali del Diritto Penale della Libertà*, in "Derecho Penal y Criminologia", 1992, n. 14
- A. MASSARO (2025), *Riflessioni sul disegno di legge in materia di femminicidio*, in "sistemapenale.it", 25 giugno 2025
- E. MENSA, D. COLLA, M. DALMASSO, M. GIUSTINI, C. MAMO, A. PITIDIS, D.P. RADICIONI (2020), *Violence detection explanation via semantic roles embeddings*, in "BMC Medical Informatics and Decision Making", 2020, n. 1
- M. MERLER (2023), *La corte costituzionale tedesca si pronuncia sul trattamento automatizzato dei dati in contesti di polizia*, in "Giornale di diritto amministrativo", 2023, n. 5

- F. MOLLO (2024), *Il trattamento dei dati biometrici nell'IA Act: intersezioni tra la normativa di protezione dei dati e la nuova disciplina europea dell'intelligenza artificiale*, in "federalismi.it", 28 novembre 2024
- D. MORONDO TARAMUNDI (2025), *Prevenzione versus predizione del rischio: l'uso del programma semi-automatizzato di decisione VioGén in Spagna*, in "Diritto & Questioni pubbliche", 2025, n. XXV
- D. NEGRI (2016), *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in "Archivio penale", 2016, n. 2
- W. NOCERINO (2020), *Le nuove tecniche di investigazione proattiva e le ricadute processuali – prima parte*, in "Studium iuris", 2020, n. 7-8
- C. PALIERO (2000), *La fabbrica del Golem. Progettualità e metodologia per la «Parte Generale» di un Codice Penale dell'Unione Europea*, in "Rivista Italiana di Diritto e Procedura Penale", 2000
- A.U. PALMA (2020), *Le "prove di verità" e la libertà morale del dichiarante*, in "Archivio penale", 2020, n. 1
- C. PAONESSA (2017), *Parola e Linguaggio nel diritto penale: la garanzia della forma oltre il formalismo*, in "Studi Senesi", vol. CXXIX, 2017
- C. PAONESSA (2009), *Gli obblighi di tutela penale. La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari*, Edizioni ETS, 2009
- L. PARODI (2025), *La "gravità dell'ingerenza" nel prisma della proporzionalità: nuovi equilibri in tema di data retention*, in "sistemapenale.it", 7 marzo 2025
- G. PAVAN (2013), *Tutela penale della vittima nel diritto penale*, in "Digesto delle discipline penalistiche", agg. VII, Utet Giuridica, 2013
- C. PECORELLA (2025), *Perché può essere utile una fattispecie di femminicidio*, in "sistemapenale.it", 2 giugno 2025
- D. PERRONE (2022), *La prognosi postuma tra distorsioni cognitive e software predittivi. Limiti e possibilità del ricorso alla "giustizia digitale integrata" in sede di accertamento della colpa*, Giappichelli, 2022
- L. PICOTTI (2011), *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in G. Grasso, L. Picotti, R. Sicurella (a cura di), "L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona", Giuffrè, 2011
- E. PIETROCARLO (2023), *Predictive policing: criticità e prospettive dei sistemi di identificazione dei potenziali criminali*, in "sistemapenale.it", 28 settembre 2023
- G. PIZZOLANTE (2025), *Il quadro giuridico europeo sulla sorveglianza biometrica*, in "Rivista di diritti comparati", 2025, n. 3
- L. PULITO (2025), *Algoritmi predittivi e valutazione della pericolosità sociale: livelli di rischio alla luce dell'AI Act e prospettive interne di impiego*, in "Archivio penale", 2025, n. 3
- L. PULITO (2024), *Il contributo dell'intelligenza artificiale simbiotica nella protezione delle vittime vulnerabili e nel contrasto della violenza di genere*, in "BioLaw Journal", 2024, n. 1
- S. QUATTROCOLO (2025), *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in "Diritto di difesa", 16 gennaio 2025
- L. RISICATO (2019), *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Giappichelli, 2019
- S. RODOTÀ (2010), *Una Costituzione per Internet?*, in "Politica del diritto", 2010, n. 3
- G. RUGGIERO (2023), *I principi del diritto penale: controlimiti nel tempo del "disagio della democrazia"*, in "Rivista Italiana di Diritto e Procedura Penale", 2023, n. 4
- F. SGUBBI (2019), *Diritto penale totale. Punire senza legge, senza verità, senza colpa. Venti tesi*, Il Mulino, 2019

- S. SIGNORATO (2016), *Tipologie e caratteristiche delle cyber investigations in un mondo globalizzato*, in “Diritto penale contemporaneo”, 2016, n. 3
- P. SORBELLO (2019), *Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto*, in “Diritto penale contemporaneo”, 2019, n. 2
- I. SPEZIALE (2025), *Le linee guida della Commissione europea in materia di pratiche di intelligenza artificiale vietate*, in “Contratto e impresa”, 2025, n. 2
- M. TORRE (2019), *Indagini informatiche e principio di proporzionalità*, in “Processo penale e giustizia”, 2019, n. 6
- P. TROISI (2019), *Passenger Name Records, privacy e accertamento penale*, in “Processo penale e giustizia”, 2019, n. 1
- M.A. UTSET (2021), *Predictive policing and criminal law*, Taylor e Francis ebook, 2021
- V. VASTA (2024), *Diritto dell’Unione Europea e Intelligenza Artificiale. Riflessi sul procedimento penale*, in “Rivista Italiana di Diritto e Procedura Penale”, 2024, n. 1
- M. VENTUROLI (2022), *Le misure sospensivo-probatorie nella fase esecutiva della pena tra criticità e prospettive di riforma*, in “Rivista Italiana di Diritto e Procedura Penale” 2022, n. 1
- M. VENTUROLI (2021), *La “centralizzazione” della vittima nel sistema penale contemporaneo tra impulsi sovranazionali e spinte populistiche*, in “Archivio penale”, 2021, n. 1
- M. VENTUROLI (2017), *Vittima. Profili di diritto penale*, in Treccani–Diritto on line, 2017
- A. VELE (2026), *Identificazione, intelligenza artificiale e riconoscimento facciale ai sensi dell’art. 349 c.p.p.*, in “Archivio penale”, 2026, n. 1
- F. VIGANÒ (2023), *Diritto penale e diritti della persona*, in “sistemapenale.it”, 13 marzo 2023
- A. ZIROLDI (2019), *Intelligenza artificiale e processo penale tra norme, prassi e prospettive*, in “questione-giustizia.it”, 18 ottobre 2019

Studi e ricerche

Sistemi e applicazioni

Note e discussioni



UMBERTO NIZZA

Ridurre la complessità, ricostruire la fiducia: dalla retorica della semplificazione alla teoria della chiarezza

Il presente saggio propone una formalizzazione teorica e computazionale della chiarezza amministrativa come parametro misurabile di efficienza e legittimità dell'azione pubblica. La ricerca individua nella complessità linguistica e procedurale una forma di asimmetria informativa istituzionale che mina la trasparenza e l'equità sostanziale, generando costi di transazione e disuguaglianze cognitive. Attraverso un modello dinamico multilivello, il lavoro mostra come la semplificazione non possa essere ricondotta alla mera riduzione di oneri o adempimenti burocratici, ma debba, invece, configurarsi come un nuovo equilibrio tra chiarezza espressiva, semplicità procedurale e capacità di apprendimento istituzionale. Per mezzo di simulazioni Monte Carlo questo contributo mostra, in termini probabilistici, qual è l'impatto delle politiche di semplificazione sull'accessibilità normativa e sul contenzioso, evidenzia come il linguaggio amministrativo possa agire come elemento di efficienza sistemica e di giustizia distributiva. Il saggio, in conclusione, colloca la chiarezza tra i principi immanenti del buon andamento amministrativo, delineandone una misurabilità empirica e una funzione di riequilibrio cognitivo fra amministrazione e destinatari finali delle norme.

Complessità normativa – Modelli computazionali – Linguaggio giuridico – Chiarezza regolatoria

Reducing administrative complexity, restoring public trust: From the rhetoric of simplification to the theory of clarity

This essay advances a theoretical and computational formalization of administrative clarity as a measurable parameter of efficiency and legitimacy in public action. The research identifies linguistic and procedural complexity as a form of institutional information asymmetry that undermines transparency and substantive equity, generating transaction costs and cognitive inequalities. Through a dynamic multilevel model, the study demonstrates that simplification cannot be reduced to the mere lowering of regulatory burdens or administrative requirements but must instead be conceived as a new equilibrium among expressive clarity, procedural simplicity, and institutional learning capacity. By means of Monte Carlo simulations, this contribution probabilistically assesses the impact of simplification policies on regulatory accessibility and litigation, highlighting how administrative language may function as a driver of systemic efficiency and distributive justice. In conclusion, the essay situates clarity among the immanent principles of sound administrative performance, outlining its empirical measurability and its role in restoring cognitive balance between public administrations and the ultimate addressees of legal norms.

Regulatory complexity – Computational models – Legal language – Regulatory clarity

L'Autore è *Transatlantic Technology Law Forum affiliate* presso l'Università di Stanford, *adjunct professor* presso l'Università di Bologna e assegnista di ricerca in diritto dell'economia presso l'Università di Torino

Questo lavoro si inserisce nell'ambito del progetto di eccellenza, del dipartimento di giurisprudenza di Torino, *Turin Tech & Law: a Lab for Social Good* (TuTeLa)

SOMMARIO: 1. Introduzione – 2. Inquadramento della problematica: la chiarezza come valore sociale non ancora pienamente realizzato. – 3. Una teorizzazione formale delle dinamiche di semplificazione amministrativa. – 4. Validazione empirica e test computazionale del modello di semplificazione amministrativa. – 4.1. Simulazione di scenario: un'analisi comparativa dell'impatto di potenziali configurazioni amministrative eterogenee sulla semplificazione normativa. – 4.2. Analisi di sensibilità dei pesi decisionali introdotti nel modello: verso un bilanciamento ottimale delle componenti della semplificazione. – 4.3. Proiezioni dinamiche in tema di accessibilità amministrativa e livello di semplificazione del linguaggio amministrativo: dalla teoria alla prassi. – 5. Implicazioni sistemiche e ragioni giuseconomiche in tema di riduzione della complessità del linguaggio amministrativo. – 6. Conclusioni.

1. Introduzione

Il linguaggio amministrativo contemporaneo è attraversato da una tensione strutturale fra l'esigenza di garantire la certezza giuridica e quella, non meno fondamentale, di rendere l'azione pubblica intelligibile, accessibile e proporzionata rispetto alle capacità cognitive, linguistiche e digitali dei destinatari¹. Tale tensione rappresenta una delle principali fonti di disfunzione dei rapporti tra cittadini e pubbliche amministrazioni, con un divario crescente tra il linguaggio normativo e regolatorio – spesso connotato da ambiguità e da uno stile di scrittura particolarmente faticoso – e i destinatari finali delle norme o disposizioni impartite dall'amministrazione medesima. Il divario tra il linguaggio normativo, spesso caratterizzato da iper-tecnicità, stratificazione e ambiguità semantica, e le capacità interpretative dei destinatari produce un divario di accessibilità che si traduce, nella prassi, in richieste di chiarimenti, ritardi procedurali e aumento del contenzioso². Lo scollamento tra la comprensione degli utenti e delle regole a cui

questi devono uniformarsi è particolarmente marcato nella “antilingua” amministrativa, che investe una dimensione qualitativa della comunicazione giuridico-amministrativa, ovvero la capacità degli atti pubblici di mostrare una complessità illocutiva che ne inficia la comprensibilità, l'eseguibilità e la contestazione consapevole³.

Questo divario di accessibilità si manifesta come una forma specifica di *asimmetria informativa istituzionale*, nella quale l'amministrazione dispone di risorse interpretative e conoscitive infinitamente superiori a quelle dei cittadini, i quali, a loro volta, si trovano a operare in un contesto di crescente complessità normativa e procedurale, che impedisce loro di fronteggiare, in quanto destinatari di tale linguaggio, la distanza sociale, culturale e tecnica che ne limita la capacità di comprensione e partecipazione all'intero procedimento amministrativo⁴. La semplificazione amministrativa, frequentemente intesa dal legislatore in senso meramente quantitativo, come riduzione di adempimenti o di oneri burocratici⁵, potrebbe non

1. BONETTI-TROILO 2016.

2. LIBERTINI 2020.

3. CORTELLAZZO 2021.

4. GIANNOTTI 2007.

5. Si vedano, su questo aspetto, le evoluzioni della disciplina, dai meccanismi taglia-oneri amministrativi introdotti dal legislatore con l'articolo 25 del d.l. 112/2008, sino ad arrivare ai principi di trasparenza, riorganizzazione e semplificazione introdotti con il d.lgs. 33/2013.

essere, di per sé, sufficiente a ristabilire un buon equilibrio comunicativo e cognitivo tra i soggetti coinvolti nel rapporto amministrativo⁶. Come si vedrà nel prosieguo, un'accessibilità normativa effettiva richiede un radicale mutamento di paradigma, passando dall'attuale modello di amministrazione autoritativa, basata sull'unidirezionalità dell'atto, a un modello relazionale e adattivo, nel quale la produzione amministrativa può essere concepita in modo maggiormente dinamico, ovvero come un processo iterativo di co-progettazione e dialogo tra amministrazione e cittadini. In tal senso, questo scritto non si limita alla mera analisi della scarsa intelligibilità degli atti amministrativi, ma si spinge oltre la mera retorica della semplificazione normativa, interrogandosi su quali fondamenta linguistiche, sintattiche e cognitive possa evolvere il diritto, nell'intento di individuare un modello virtuoso che possa servire al consolidamento – nel solco del principio di buon andamento e trasparenza, *ex art. 97 Cost.* – e sistematizzazione di un principio di *chiarezza amministrativa*, inteso come obbligo di rendere l'atto non soltanto come formalmente valido ma, in via più ampia e non necessariamente mediata, come *sostanzialmente comprensibile*. Tale principio, pur implicito nelle più recenti politiche di digitalizzazione e *open government*, resta subordinato alle note esigenze di autotutela amministrativa e di coerenza formale del testo giuridico. Ciononostante, la chiarezza e l'accessibilità del linguaggio amministrativo non sono meri attributi estetici o comunicativi, ma costituiscono, come si vedrà *infra*, condizioni epistemiche di efficacia dell'azione pubblica oltretutto requisiti di legittimazione democratica delle stesse istituzioni coinvolte in tali processi di efficientamento e semplificazione⁷.

In una prospettiva di stampo giuseconomico, la complessità amministrativa genera, all'interno dell'ordinamento, dei *costi di transazione* che si impongono, surrettiziamente, sull'intero ciclo regolatorio, con riflessi che si estendono, in maniera altrettanto importante, sull'intero ciclo di vita dell'atto normativo sotteso: nella fase di adozione – in virtù di maggiori oneri di redazione e revisione –, in quella di esecuzione – in ragione di

eventuali errori interpretativi, ritardi, richieste di chiarimento – e, infine, anche nell'eventuale stadio patologico – con l'aumento del contenzioso finalizzato ad ottenere chiarimenti o interpretazioni alternative di stampo giurisprudenziale⁸. Tali costi si distribuiscono in modo asimmetrico, gravando prevalentemente sui cittadini, sulle piccole imprese e sui soggetti a più bassa alfabetizzazione giuridica e digitale. Ne deriva un effetto regressivo sul piano dell'equità sostanziale: l'accesso al diritto amministrativo non risulta, in ragione di tali *asimmetrie di informazione* e dei *costi di transazione* sottostanti, eguale per tutti, ma è strettamente dipendente dalle capacità cognitive o dalla pregressa esperienza giuridica dei destinatari. Il risultato complessivo è che il divario di accessibilità amministrativa si configura come un fenomeno complesso e multidimensionale: giuridico, linguistico, organizzativo e tecnologico. Sul piano giuridico, esso riflette la tensione fra il principio di legalità e il principio di proporzionalità comunicativa, mentre, sul piano linguistico, si manifesta nella tendenza alla tecnicizzazione e ipertrofia lessicale degli atti, che li rende spesso indecifrabili per i non addetti ai lavori. Da un punto di vista organizzativo, tale complessità è il prodotto di filiere decisionali stratificate e di processi di controllo formale che privilegiano la conformità al modello rispetto alla chiarezza sostanziale. Infine, sul piano tecnologico, vi è ancora difficoltà nel tradurre l'atto amministrativo in formati digitali interoperabili e semanticamente accessibili, nonostante le potenzialità offerte dall'informatica giuridica e dai sistemi di intelligenza artificiale per la semantizzazione e l'analisi automatica del linguaggio normativo.

In questa prospettiva, un miglioramento della *chiarezza amministrativa* – con la conseguente riduzione del divario di accessibilità amministrativa – non può ottenersi attraverso riforme puramente lineari e statiche, ma richiede, a ben vedere, un approccio multilivello e integrato, capace di modellare e monitorare nel tempo l'interazione tra la qualità linguistica degli atti, il comportamento degli utenti e le decisioni interne dell'amministrazione. In altri termini, la *semplificazione amministrativa* dovrebbe concepirsi come

6. FIORENTINO 2007.

7. DUCCI 2013.

8. Si veda, per un esempio empirico, RASKOLNIKOV 2007.

un *processo dinamico* di regolazione, nel quale l'amministrazione può apprendere dai feedback ricevuti e modificare progressivamente le proprie pratiche redazionali e procedurali alla luce dei suggerimenti ricevuti e dalle mutate condizioni di tempo⁹. Tale processo di co-regolamentazione efficace può essere formalizzato attraverso modelli dinamici che rappresentano la coevoluzione tra complessità istituzionale e accessibilità cognitiva, introducendo variabili di stato – ovvero, come si vedrà nel prosieguo, da elementi quali il livello di chiarezza, i tempi procedurali, il tasso di ricorsi, il grado di fiducia istituzionale – e da regole di aggiornamento che descrivono come le decisioni di semplificazione o revisione incidano sui risultati complessivi del sistema amministrativo.

In questa prospettiva, anche attraverso modellizzazioni quantitative e simulazioni computazionali – che non sono strumenti del tutto estranei al sillogismo applicato al diritto¹⁰ – si possono rendere osservabili e misurabili fenomeni di natura complessa che sfuggono alle tradizionali categorie dogmatiche tipiche del diritto. Queste tecniche permettono di formalizzare le modalità di intervento con cui il legislatore – e, per conto di questi, la stessa pubblica amministrazione – migliora la chiarezza espositiva del proprio impianto normativo, valutando, al contempo, con strumenti empirici, quali fattori possono risultare di maggiore impatto nel garantire un intervento regolatorio o organizzativo efficace, capace di migliorare, in definitiva, la comprensibilità e l'efficienza amministrativa. In tal modo, la dimensione informatica e quella giuridica convergono nella costruzione di un quadro teorico che riconosce la normazione amministrativa come sistema aperto e suscettibile di apprendimento.

Nel corso di questo scritto si costruiranno le basi teoriche per tale attività di rimodulazione dell'azione amministrativa, fondando l'analisi su due presupposti normativi e metodologici: da

un lato, il riconoscimento della chiarezza e della comprensibilità come beni pubblici e condizioni di legittimità dell'azione amministrativa; dall'altro, la possibilità di trattare la complessità istituzionale come variabile governabile attraverso strumenti di analisi e simulazione. Il contributo teorico di questa impostazione risiede nel superamento della dicotomia tra diritto e tecnologia, restituendo al diritto amministrativo e al diritto dell'economia una dimensione sperimentale, coerente con i principi dell'amministrazione digitale e con le esigenze di trasparenza e partecipazione previste dal legislatore europeo e nazionale per i mercati regolati. Nel corso di questo scritto, gli elementi teorici individuati vengono testati per mezzo di alcune simulazioni Monte Carlo, così da vagliare la sensibilità a cambi di parametri o di impostazione generale¹¹, per poi trarne, in ultima analisi, delle conclusioni che permettano di formulare raccomandazioni operative orientate alla creazione di quel modello di amministrazione relazionale e partecipativa¹² che è visto come unico impianto normativo efficace nel ridurre le asimmetrie informative esistenti e migliorare la comprensione dei cittadini rispetto al proprio *agere*.

2. Inquadramento della problematica: la chiarezza come valore sociale non ancora pienamente realizzato

La chiarezza e la coerenza delle fonti tendono sempre più a configurarsi principi immanenti al canone di buon andamento sancito all'art. 97 Cost.¹³, in ragione della necessità, per la pubblica amministrazione, di dare seguito al principio di legalità formale e, contemporaneamente, di giustificare sia l'*agere* pubblico che, più in generale, rendere chiaro, coerente e trasparente il comportamento richiesto ai destinatari delle norme medesime¹⁴. L'esercizio dei poteri pubblici non potrebbe, infatti, dirsi conforme ai principi costituzionali se non risultasse anche intellegibile per i suoi destinatari¹⁵,

9. ODDENINO 2024.

10. NIZZA 2022.

11. WANG 2012.

12. CIRILLO 2011.

13. PICCHI 2013.

14. BOMBARDELLI 2015.

15. DOGLIANI 2008.

con il risultato che la chiarezza si pone come condizione stessa di effettività e di legittimità dell'azione amministrativa: una pubblica amministrazione che non si fa pienamente comprendere dal cittadino, o che redige i propri atti in modo tale da richiedere una continua interpretazione autentica, mediata, o specialistica¹⁶, viola le esigenze di trasparenza – in quanto rende opaca l'azione amministrativa, impedendo ai cittadini di comprendere le ragioni e le finalità dell'azione pubblica – e di imparzialità – giacché crea spazi di discrezionalità interpretativa non giustificati – e pregiudica, in ultima analisi, la possibilità che l'azione amministrativa espliciti i propri effetti utili in termini di conoscibilità, esecuzione e controllo¹⁷.

In questo contesto, la comprensibilità degli atti, la linearità dei procedimenti e la chiarezza delle norme costituiscono non soltanto elementi essenziali per l'effettività del rapporto fiduciario tra istituzione e cittadino – poiché senza chiarezza non esiste capacità di controllo, né possibilità effettiva di partecipazione o di esecuzione conforme¹⁸ – ma assumono una rilevanza sociale ed economica, data l'influenza su costi di transazione e sugli assetti di mercato. Il risultato è che, in mancanza di chiarezza, si mina la funzione precipua del diritto di organizzazione della vita sociale e di limitazione dei conflitti tra i consociati¹⁹. La chiarezza, in questo senso, non è un mero attributo ornamentale di forma, ma una condizione epistemica di accesso al diritto, come tale capace di incidere direttamente sull'efficacia e sulla legittimità sostanziale di tutta l'azione amministrativa.

Nonostante la crescente attenzione, sia in dottrina che in giurisprudenza²⁰, alla tematica della chiarezza e della semplicità dei testi prodotti dal

legislatore e dalle sue ramificazioni amministrative, le iniziative in favore di una maggiore chiarezza in termini di linguaggio risultano sporadiche²¹, nonostante vi siano numerose evidenze, anche empiriche, che dimostrano la persistenza di un carattere tipicamente burocratico che aumenta la complessità e la distanza tra cittadino e pubblica amministrazione²². Il legislatore italiano ha dedicato alla chiarezza e alla semplificazione linguistica strumenti di *soft law* – come il *Codice di stile delle comunicazioni scritte* del 1993 e la *Direttiva sulla semplificazione del linguaggio amministrativo* del 2002 – i quali, tuttavia, non avendo forza vincolante, rendono ancor più lampante la discrepanza fra la proclamazione del principio di chiarezza, riconosciuto come valore e come finalità pubblica, e l'assenza di meccanismi normativi e organizzativi idonei a tradurlo in obbligo effettivo. La conseguenza è che la chiarezza resta affidata alla mera buona volontà, oscillando tra prassi virtuose e rigidità burocratiche, senza criteri omogenei di misurazione o di responsabilità.

Su questo terreno si è innestata una più ampia riflessione sulla semplificazione amministrativa, che negli ultimi anni ha oscillato tra due approcci distinti: uno di natura normativa, teso a ridurre il numero di procedimenti, a semplificare gli adempimenti e a razionalizzare le fonti²³, e uno di natura sistemica, volto a ripensare complessivamente la cultura amministrativa in chiave cognitiva, partecipativa e digitale²⁴. Nel primo caso, la semplificazione è stata intesa come sottrazione: meno atti, meno vincoli, meno passaggi; nel secondo, come riorganizzazione intelligente del processo decisionale. Tuttavia, va notato che la mera riduzione dei passaggi procedurali non conduce

16. Tipico è il caso, infatti, della necessità di rivolgersi ad un avvocato o ad altro giurista per l'interpretazione di "fossili linguistici" che dovrebbero, invece, essere pienamente comprensibili anche dal "cittadino qualunque", come suggerito in BREGGIA 2013, p. 23.

17. FORTIS 2011.

18. MARGIOTTA 2021.

19. DE BENEDETTO–RANGONE 2019.

20. Cfr., *inter alia*, sul principio di *clare loqui*, Consiglio di Stato sentenze 2226/2021, 2709/2021, 3253/2025, oltreché, sulle tematiche di semplificazione del linguaggio amministrativo, FOÀ 2025, COLLEO 2022.

21. CARBONE–FIAMMA–MARCELLI et al. 2016.

22. BRUNATO 2014.

23. SALOMONI 2023.

24. MATTARELLA 2019.

necessariamente ad una maggiore chiarezza del testo o efficienza della procedura²⁵, giacché un atto può essere breve ma oscuro, oppure formalmente semplificato ma di difficile interpretazione per il cittadino medio²⁶. Nonostante i tentativi di semplificazione formale e di informatizzazione di tutte le attività che coinvolgono gli enti centrali, permane una significativa discrasia tra la modernità dei mezzi impiegati e il livello di arcaicità della lingua con la quale si veicolano precetti, informazioni, comunicazioni e decisioni amministrative. In questa prospettiva, il rischio è di non raggiungere la semplificazione sostanziale e la piena realizzazione di una pubblica amministrazione realmente trasparente e accessibile, così come ambita dal legislatore. Tra le ragioni di fondo che determinano questa oscurità di fondo vi è la compresenza di norme ambigue, una concezione eccessivamente formalistica di procedure e testi, una stesura poco accurata e incapace di rispondere ai bisogni degli utenti finali, o la presenza di stereotipi consolidati e di un linguaggio burocratico, che appesantiscono la leggibilità e l'adeguatezza del testo rispetto ai fini di comprensibilità, trasparenza e intelligibilità²⁷.

Il problema più generale della qualità della comunicazione istituzionale, che incide, in via diretta o mediata, sul *diritto a capire* del cittadino²⁸, impone una riflessione su quale modello possa essere adottato dalla pubblica amministrazione per far propria la *w*, come obiettivo perseguibile e variabile misurabile. La chiarezza, in questo senso, pur risultando concettualmente riconosciuta come bene pubblico, manca di un quadro analitico che ne consenta di definire con precisione indicatori, standard operativi e responsabilità organizzative, trasformandola in un mero principio etico ed aspirazionale che risulta ben lontano dall'essere obiettivo concreto, i cui esiti possono essere misurabili per mezzo di precisi indicatori e analisi empiriche. La carenza di strumenti metodologici adeguati rende difficile verificare se le politiche di semplificazione linguistica e procedurale producano effetti

tangibili sulla comprensibilità degli atti, sulla partecipazione dei cittadini e sulla riduzione dei costi di transazione. Il risultato è la creazione di un vuoto tra le intenzioni riformatrici e risultati concreti osservabili in tema di linguaggio burocratico²⁹. Senza criteri chiari di misurazione, gli interventi rischiano di rimanere episodici e frammentari, incapaci di generare una trasformazione strutturale della pubblica amministrazione. La difficoltà di valutare gli effetti di eventuali riforme semplificatorie – così come avvenuto con i vari interventi del legislatore – deriva, in buona parte, dalla natura complessa del concetto di chiarezza, che non si riduce alla mera brevità o semplicità formale dei testi, ma richiede di analizzare aspetti cognitivi, culturali e contestuali legati alla comprensione da parte di destinatari eterogenei.

Alla luce di quanto precede, questo contributo teorizza e testa un modello formale di chiarezza amministrativa, concependo tale elemento come strumento analitico, capace di tradurre questo principio aspirazionale in un vero e proprio parametro operativo suscettibile di misurazione e valutazione empirica. Il modello si fonda sulla considerazione secondo cui la chiarezza non possa essere identificata esclusivamente con la semplicità linguistica o con la brevità dei testi, ma debba essere intesa come un fenomeno multidimensionale che coinvolge: leggibilità dei documenti, coerenza interna di norme e procedimenti, capacità dei destinatari di comprendere e interpretare il contenuto e, infine, tener conto delle finalità precipe dell'azione amministrativa. In questa prospettiva, la chiarezza del linguaggio normativo si configura come condizione necessaria per l'effettività del rapporto fiduciario tra amministrazione e cittadino, influenzando sulla partecipazione attiva e sulla riduzione dei costi di transazione legati all'interazione con l'ente pubblico. Il senso complessivo del modello teorico presentato in questo scritto risiede nella capacità di costruire un quadro analitico che trasforma gli elementi qualitativi, e spesso

25. Medesime criticità si applicano alla sinteticità processuale richiesta dalla “riforma Cartabia”, giacché, se esistono questioni dibattute, queste permangono anche con minori passaggi. Così DE GIORGIS 2023.

26. AINIS 1997.

27. CORTELLAZZO 2015.

28. PIEMONTESE 1996.

29. ZANNI ROSIELLO 2015.

soggettivi, in criteri misurabili e standardizzabili. In questo modo si può stimare, in termini quantitativi, la correttezza formale e procedurale degli atti, così da valutare l'efficacia comunicativa e cognitiva rispetto ai destinatari reali. In tal modo, si mira a colmare la discrepanza tra il riconoscimento teorico della chiarezza, quale valore costituzionale, e la concreta difficoltà di implementarla nella prassi amministrativa, fornendo nuovi strumenti, capaci di guidare l'elaborazione di testi e procedure più trasparenti, coerenti e accessibili, e di orientare la gestione organizzativa e normativa verso una reale responsabilizzazione degli uffici pubblici nei confronti della qualità comunicativa istituzionale.

3. Una teorizzazione formale delle dinamiche di semplificazione amministrativa

Come anticipato *supra*, l'ipotesi di fondo che orienta la presente ricerca è che la complessità amministrativa non costituisca una mera proprietà statica dell'ordinamento, né un dato fisiologico inevitabile, ma possa essere trattata come una variabile dinamica, integrando componenti giuridiche, con dinamiche linguistiche e organizzative, in modo tale da rappresentare in termini quantitativi il processo di semplificazione a cui il legislatore sembra voler tendere senza successo. La *chiarezza del linguaggio normativo* viene intesa, in questa prospettiva, come il risultato di un'interazione complessa tra fattori linguistici, procedurali e organizzativi, che incidono in modo differenziato sull'accessibilità effettiva dell'azione amministrativa. A tal fine, il modello proposto assume che l'ordinamento venga considerato come un sistema composito di agenti eterogenei che interagiscono in orizzonte temporale discreto $t = 0, 1, 2, \dots, T$. Gli agenti principali sono:

- l'amministrazione, intesa come soggetto collettivo che produce atti e adotta decisioni di revisione o semplificazione;
- i destinatari degli atti, rappresentati come una popolazione distribuita in base a differenti livelli di alfabetizzazione giuridica, competenze digitali e capacità interpretative.

In ogni periodo temporale t lo stato del sistema è descritto da un vettore di variabili $X_t = (L_t, P_t, C_t, R_t)$ dove:

- L_t rappresenta l'indice di leggibilità o chiarezza testuale degli atti prodotti in quel periodo;
- P_t misura la complessità procedurale, espressa in termini di passaggi amministrativi medi o di densità normativa;
- C_t indica il tasso di contenzioso o di ricorso, assunto come proxy³⁰ della non-accessibilità cognitiva o procedurale;
- R_t rappresenta il flusso di feedback proveniente dagli utenti, sotto forma di richieste di chiarimento, segnalazioni o errori procedurali.

Il vettore X_t evolve secondo una legge di transizione che combina dinamiche naturali (inerzia burocratica, accumulo normativo) e decisioni di policy dell'amministrazione D_t , sicché:

$$X_{t+1} = \mathcal{F}(X_t, D_t, \varepsilon_t)$$

dove $\mathcal{F}$ è una funzione di aggiornamento che incorpora gli effetti diretti delle scelte amministrative e le perturbazioni stocastiche ε_t (shock esogeni, mutamenti legislativi, variazioni del contesto politico). La componente più rilevante del modello risiede nella possibilità di specificare D_t come vettore di decisioni di semplificazione, che possono assumere natura discreta (introduzione di modelli testuali, nuove linee guida) o continua (intensità di revisione, livello di investimento in formazione e digitalizzazione). Ciascuna di queste variabili evolve nel tempo in base a relazioni interne coerenti con la logica del sistema.

A fini esplicativi si considerino le seguenti equazioni semplificate:

$$\begin{aligned} L_{t+1} &= L_t + \gamma_1 \cdot Rev_t - \gamma_2 \cdot Comp_t + \xi_t \\ P_{t+1} &= P_t + \delta_1 \cdot Simpl_t - \delta_2 \cdot NewReg_t + \eta_t \\ C_{t+1} &= \alpha_0 + \alpha_1 P_t + \alpha_2 L_t - \alpha_3 \cdot Hetero_t + \theta_t \end{aligned}$$

in cui:

- Rev_t rappresenta l'intensità media degli interventi di revisione o chiarificazione degli atti;
- $Comp_t$ è una misura sintetica della complessità linguistica interna al corpus normativo vigente;
- $Simpl_t$ indica la portata delle azioni di semplificazione procedurale;
- $NewReg_t$ esprime l'impatto di nuove normative che incrementano la densità regolatoria;
- $Hetero_t$ misura l'eterogeneità della popolazione dei destinatari (in termini di alfabetizzazione giuridica e digitale).

30. Una variabile *proxy* è un indicatore indiretto utilizzato quando la variabile concettualmente rilevante non risulti direttamente osservabile o misurabile mediante dati empirici. WOOLDRIDGE 2016, p. 279 ss.

Le costanti γ , δ , α rappresentano i parametri di sensitività, ossia l'intensità con cui le decisioni amministrative e i fattori esterni incidono sulle variabili di stato. Le componenti ξ , η , θ sono rumori stocastici che rappresentano variazioni casuali o shock imprevisti, simulati tramite distribuzioni probabilistiche calibrate a seconda del contesto. Si comprenderà, in questo quadro, che il tasso di contenzioso C_t funga da *variabile-obiettivo*, ovvero come *proxy* di *accessibilità* del linguaggio: un suo incremento segnala inefficienza comunicativa o procedurale, mentre una riduzione stabile nel tempo indica una maggiore chiarezza e prevedibilità dell'azione amministrativa.

Tutto ciò premesso e considerato, l'amministrazione può essere concepita, in termini di modellizzazione, come un decisore che agisce entro vincoli cognitivi, organizzativi e normativi, e che tende a bilanciare due obiettivi complementari ma potenzialmente confliggenti: da un lato, l'efficienza interna dei propri processi; dall'altro, l'accessibilità esterna delle proprie decisioni e dei propri atti. In questo contesto, ogni scelta di semplificazione comporta un costo e produce un beneficio, nonostante i due parametri non si manifestino simultaneamente ma, contrariamente, si distribuiscono nel tempo. Il modello assume pertanto che l'amministrazione persegua una funzione di equilibrio dinamico, volta a minimizzare il costo complessivo derivante da: scarsa chiarezza, complessità procedurale e risorse necessarie per attuare gli interventi correttivi. Formalmente, ciò può essere indicato come una funzione di obiettivo che bilancia l'efficienza interna e l'accessibilità esterna:

$$\min_{\{D_t\}} \mathbb{E} \left[\sum_{t=0}^T \rho^t (\kappa_C C_t + \kappa_P P_t + \kappa_R \text{CostRev}_t) \right]$$

dove D_t indica il vettore delle decisioni prese dall'amministrazione in un dato periodo t , $\mathbb{E}$ rappresenta i costi valutati in termini attesi (*expected values*), $\sum_{t=0}^T (\cdot)$ è una sommatoria che individua l'orizzonte temporale di intervento, dal tempo t pari a zero sino al tempo T , ρ è un fattore di sconto intertemporale che riflette l'orizzonte di pianificazione dell'amministrazione, nonché il grado di avversione al ritardo nei benefici, mentre C_t rappresenta il costo della funzione, sintetizzando la quota di utenti che non comprendono l'atto o che promuovono ricorso o avviano una segnalazione

al tempo t . Infine, P_t indica la complessità procedurale, ovvero la "densità" di passaggi, punti decisionali e requisiti formali medi di un procedimento nel tempo t , mentre CostRev rappresenta il costo effettivo sostenuto dall'amministrazione per le attività di miglioramento, tra cui si possono indicare, a fini esemplificativi, i costi di revisione testuale, formazione, e aggiornamento dell'infrastruttura tecnologica. Da ultimo, i vari coefficienti κ esprimono il peso politico e organizzativo attribuito ai diversi costi:

- κ_C quantifica il costo sociale della non-accessibilità (contenzioso, sfiducia, inefficienza relazionale);
- κ_P misura il costo interno della complessità procedurale (tempi lunghi, duplicazioni, errori amministrativi);
- κ_R rappresenta il costo diretto degli interventi di revisione e formazione.

Si noti che la soluzione ottimale che l'amministrazione dovrebbe perseguire, in questa prospettiva, non coincide necessariamente con il massimo grado di semplificazione, poiché un eccesso di riduzione della complessità potrebbe generare una perdita di informazione essenziale o un'eccessiva semplificazione giuridica, cosa che non necessariamente coincide con una migliore condizione dell'attività amministrativa. Il modello consente di individuare un punto di equilibrio dinamico tra chiarezza e specificità, tra accessibilità e correttezza tecnica dell'atto.

Un ulteriore elemento della proposta teorica proposta in questo scritto consiste nella formalizzazione di meccanismi di retroazione (anche noti come *feedback loops*) che permettono al legislatore di apprendere dai propri errori sulla base delle indicazioni fornite dalla platea di beneficiari e destinatari finali dell'atto (in termini di chiarezza, burocrazia, chiarezza testuale, oneri amministrativi percepiti, complessità procedurale, coerenza normativa, accessibilità digitale e comprensibilità del linguaggio amministrativo, solo per fare alcuni esempi). Ogni periodo genera, coerentemente, delle informazioni empiriche – ovvero dei *feedback*, che sopra avevamo indicato con R_t , che incidono a loro volta sul tasso di contenzioso e sugli esiti delle revisioni – che influenzano le decisioni successive. Tali politiche di semplificazione possono essere rappresentate come funzioni adattive dello stato osservato nel periodo precedente, indicandole

con un vettore D_t che indichi le decisioni adottate dall'amministrazione al tempo t (ad esempio, l'intensità della revisione testuale, il numero di fasi procedurali eliminate o il grado di standardizzazione introdotto). Queste decisioni derivano da una funzione di risposta dinamica ottimale:

$$D_t = \Phi(R_{t-1}, C_{t-1}, L_{t-1}, P_{t-1})$$

dove R_{t-1} , C_{t-1} , L_{t-1} , P_{t-1} rappresentano, rispettivamente, il livello di feedback ricevuto, il tasso di contenzioso, la leggibilità media e la complessità procedurale osservati nel periodo precedente. La funzione $\Phi(\cdot)$ traduce queste informazioni in scelte operative, incorporando soglie di intervento, regole di priorità e strategie di apprendimento incrementale. In altre parole, il comportamento dell'amministrazione non risulta, in questa luce, come fisso e predeterminato, ma si adatta nel tempo in base alla qualità dei risultati ottenuti.

Un esempio tipico di questo stampo può individuarsi in una politica reattiva, in cui l'intensità degli interventi di revisione linguistica aumenta automaticamente quando il contenzioso supera una soglia critica $\bar{C}$. Tale meccanismo può essere espresso, in termini più formali nella forma:

$$\text{se } C_{t-1} > \bar{C}, \text{ allora } Rev_t = Rev_{t-1} + \Delta$$

dove Δ rappresenta l'incremento proporzionale di risorse o sforzi dedicati alla semplificazione.

Si tratta di un sistema che riflette un'amministrazione capace di apprendere dai dati e riconoscere eventuali inefficienze comunicative, reagire all'aumento del contenzioso e, sulla base delle diverse iterazioni, ridurre la complessità normativa e linguistica.

All'interno del modello dinamico proposto, la funzione di obiettivo rappresenta la tensione costante che l'amministrazione deve gestire fra tre dimensioni fondamentali: la *chiarezza degli atti* (o accessibilità esterna), l'*efficienza interna* dei procedimenti e la *sostenibilità economica* delle misure di semplificazione. Tale equilibrio si realizza lungo un percorso evolutivo, ovvero attraverso una sequenza di decisioni intertemporali che definiscono ciò che, nel linguaggio del modello, viene chiamata *traiettoria ottimale* D_t^* delle decisioni amministrative. In termini concettuali, questa traiettoria non è altro che la serie ordinata di scelte che l'amministrazione compie nel tempo per

raggiungere il miglior compromesso possibile tra riduzione del contenzioso, snellimento procedurale e contenimento dei costi organizzativi. È "ottimale" non nel senso astratto di perfetta razionalità – che il modello esplicitamente esclude, postulando una razionalità limitata – ma perché minimizza il costo complessivo atteso del sistema amministrativo, ponderato nel tempo.

L'amministrazione viene rappresentata, in questo contesto, come un *decisore dinamico*: in ogni periodo t , essa osserva lo stato del sistema (vale a dire i livelli di leggibilità, complessità e contenzioso), elabora tali informazioni e adotta una decisione D_t che incide sullo stato futuro. Questo meccanismo riflette il funzionamento reale delle politiche pubbliche, dove le scelte non sono isolate ma si accumulano e retroagiscono sugli esiti futuri. In termini formali, si può dire che la decisione ottimale in D_t – cioè D_t^* – è una funzione dello stato corrente, ovvero:

$$D_t^* = \Phi(S_t)$$

dove, come sappiamo da quanto indicato *supra*, $S_t = (L_t, P_t, C_t, R_t)$ rappresenta lo stato osservato del sistema. Ciò significa che l'amministrazione non sceglie in astratto, ma reagisce ai propri risultati: più aumenta il contenzioso (C_t), maggiore sarà l'intensità di revisione o di chiarificazione (Rev_t); se invece il sistema mostra un'eccessiva semplificazione che compromette la precisione tecnica, la decisione ottimale potrebbe essere quella di stabilizzare o correggere. Il concetto di *traiettoria* consente dunque di spostare l'attenzione dalla singola misura di semplificazione – come atto puntuale o riforma isolata – al processo complessivo di apprendimento istituzionale. Ogni decisione non si limita a produrre un effetto immediato, ma modifica le condizioni di partenza per le decisioni successive. La funzione di obiettivo incorpora proprio questo meccanismo di retroazione: essa valuta non solo l'efficacia momentanea di un intervento, ma anche le sue conseguenze cumulative e intertemporali.

In altri termini, la traiettoria ottimale, presentata nel modello, costituisce la linea di politica amministrativa più efficiente nel tempo, data una configurazione iniziale di risorse, competenze e vincoli normativi. Nel contesto delle simulazioni Monte Carlo che si faranno di qui a poco nel testo, tale traiettoria si può manifestare empiricamente

come quella sequenza di politiche che, in media, genera i valori più bassi della funzione di costo cumulata, ossia i livelli più equilibrati di chiarezza, semplicità e stabilità organizzativa. Questa impostazione consente di reinterpretare la buona amministrazione in chiave dinamica, ovvero come ente che non si conforma istantaneamente ad un determinato parametro di efficienza, ma come soggetto con la capacità di muoversi lungo un percorso di apprendimento e aggiustamento continuo, capace di minimizzare nel tempo il disallineamento tra linguaggio amministrativo e comprensione dei cittadini. In tal senso, la traiettoria ottimale non è solo il risultato di un calcolo, ma la rappresentazione formale di un processo virtuoso di razionalizzazione dell'azione pubblica.

4. Validazione empirica e test computazionale del modello di semplificazione amministrativa

Per verificare la coerenza interna e la capacità esplicativa del modello di chiarezza linguistica e semplificazione amministrativa, è stato sviluppato un codice di simulazione in linguaggio *Python*, che consente di riprodurre, in ambiente controllato e riproducibile, l'evoluzione dinamica di un'amministrazione pubblica sottoposta a politiche di semplificazione e chiarificazione dei propri atti. Le simulazioni, realizzate mediante tecniche Monte Carlo³¹, hanno lo scopo di rappresentare il comportamento del sistema amministrativo alla luce delle diverse condizioni istituzionali, linguistiche e organizzative presentate nel modello. Tale scelta metodologica nasce dalla constatazione che, nel diritto amministrativo contemporaneo, le riforme non producono effetti lineari, ma generano dinamiche di adattamento progressivo, spesso difficili da osservare empiricamente nel breve periodo. Le simulazioni consentono di esplorare, in ambiente virtuale, l'effetto di tali dinamiche in condizioni differenti, e di comprendere come variabili giuridiche e organizzative interagiscano nel tempo. Si tratta di un approccio sperimentale che, anziché basarsi su dati storici o osservazioni *ex post*, costruisce un ambiente amministrativo virtuale,

in cui le variabili fondamentali del sistema (leggibilità, complessità, contenzioso, costi di revisione) vengono fatte evolvere secondo le relazioni individuate nel modello teorico. In altre parole, la simulazione consente di osservare – in modo controllato – come l'amministrazione reagirebbe a diversi scenari decisionali, costituendo un'estensione analitica del modello teorico, che permette di analizzare scenari ipotetici e di osservare tendenze emergenti, traducendo concetti giuridicamente complessi (come chiarezza, prevedibilità, trasparenza) in variabili formalizzate, osservabili, quantificabili e confrontabili nel tempo. In questo modo, si traduce in termini quantitativi l'idea, eminentemente giuridica, che la chiarezza normativa non derivi da un singolo intervento, ma da un processo cumulativo di adattamento e apprendimento istituzionale. Per testare la coerenza del modello, sono state realizzate tre simulazioni, ciascuna con una funzione cognitiva distinta: un'analisi di scenario – che esplora il comportamento del sistema in contesti ipotetici –, un'analisi di sensibilità – che verifica quanto i risultati del modello dipendano dai pesi attribuiti alle diverse dimensioni (ovvero leggibilità, semplificazione, stabilità) – e una simulazione evolutiva, che rappresenta nel tempo le possibili traiettorie di adattamento dell'amministrazione.

Nel passaggio dal modello teorico al modello simulato, le quattro variabili dinamiche originarie – leggibilità (L), complessità procedurale (P), contenzioso (C) e feedback (R) – sono state tradotte in un insieme più ridotto di parametri operativi, destinati a esprimere la medesima logica relazionale in forma aggregata. In particolare, la variabile C_p , che nel modello teorico misura il livello di contenzioso e funge da indicatore di non-accessibilità, non compare nel codice come variabile autonoma, ma è incorporata in una funzione di penalità, o *penalty factor*, che riduce proporzionalmente il valore dell'indice di chiarezza amministrativa complessiva C^* , quale risultato dalla combinazione bilanciata dei tre fattori principali (leggibilità, semplicità e stabilità) e dall'effetto correttivo delle inefficienze relazionali (contenzioso e feedback

31. La simulazione Monte Carlo è una tecnica computazionale che, variando casualmente i parametri di un modello matematico secondo distribuzioni di probabilità, permette di analizzare la distribuzione dei risultati e stimarne le probabilità, semplificando sistemi complessi in iterazioni numeriche ripetute. Si veda, *ex multis*, RUBINSTEIN-KROESE 2014.

negativo). Formalmente, si può descrivere questa relazione come:

$$C^* = f(L_t, P_t, R_t) - \phi(C_t)$$

dove $\phi(C_t)$ rappresenta la penalità derivante dal livello di contenzioso e di opacità sistemica.

In tal modo, il modello computazionale non sostituisce ma “compatta” la dinamica delle quattro variabili originarie in una funzione sintetica osservabile, utile per la validazione empirica del comportamento amministrativo di efficientamento e miglioramento della comprensibilità e chiarezza del proprio operato e delle direttive normative impartite.

4.1. Simulazione di scenario: un’analisi comparativa dell’impatto di potenziali configurazioni amministrative eterogenee sulla semplificazione normativa

Nel primo blocco del codice vengono testati un insieme di scenari ipotetici, con parametri differenti di leggibilità linguistica (L), semplicità procedurale (P) e stabilità organizzativa (R). Si tratta di sei ideali di chiarezza amministrativa, determinati da altrettanti possibili scenari di fatto: “burocrazia elevata”, “burocrazia ridotta”, “comunicazione opaca”, “comunicazione chiara”, “correzione lenta” e “correzione rapida”. Per ciascun scenario, il programma genera centomila iterazioni casuali dei parametri, simulando l’eterogeneità e l’incertezza tipiche dei processi amministrativi reali. Per fornire un esempio, un’amministrazione considerata “burocratica” viene rappresentata, nella simulazione, con valori medi di semplicità (P) elevati – indicativi di complessità – e con valori più bassi di leggibilità (L), mentre una “burocrazia ridotta” presenta valori opposti. Il codice combina poi questi parametri all’interno della già richiamata funzione di penalità della chiarezza amministrativa ottimale (C^*), calcolata come rapporto fra fattori positivi – e.g., leggibilità, stabilità, continuità amministrativa – ed eventuali elementi negativi – e.g., fattori di complessità, rigidità procedurale, costi di coordinamento. I risultati, riportati in Figura 1, mostrano la distribuzione di probabilità di C^* per ciascuno di questi scenari.

I risultati mostrano differenze sostanziali nella collocazione e nella dispersione dei valori simulati. La diversa forma che assumono le distribuzioni di C^* nei sei scenari simulati dipende dal modo in cui mutano congiuntamente L , P , R , ovvero

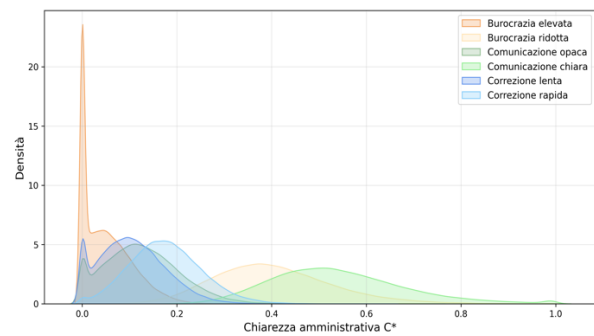


FIG. 1 — Distribuzione dell’indice di chiarezza amministrativa nei diversi scenari analizzati
(La figura mostra la distribuzione stimata dell’indice di chiarezza amministrativa C^* attraverso simulazioni Monte Carlo per sei diverse configurazioni istituzionali, caratterizzate da combinazioni differenti di leggibilità testuale, semplicità procedurale e stabilità organizzativa)

dei pesi relativi che l’ordinamento attribuisce, in ciascuna configurazione ideale, alla leggibilità degli atti, alla densità procedurale e alla capacità di risposta ai feedback esterni. Nel modello, L incrementa direttamente il numeratore dell’indice di chiarezza, riducendo gli oneri cognitivi associati alla decodifica del testo; P , al contrario, contribuisce negativamente in duplice modo, poiché incrementa la complessità procedimentale percepita, aumentando la probabilità di errore, ritardo o fraintendimento; R , infine, agisce come variabile di retroazione positiva, attenuando nel tempo le imperfezioni strutturali del sistema e consentendo una riallocazione progressiva degli sforzi organizzativi verso una semplificazione effettiva. In termini più propriamente giuridici, ciò significa che la qualità della produzione amministrativa non viene determinata da un unico attributo, ma dall’interazione dinamica tra testo, struttura e apprendimento istituzionale, sulla base dei quali le simulazioni riportate graficamente in Figura 1 operano una valutazione statistica dei possibili scenari. Nello scenario di *burocrazia elevata*, ovvero nella curva in rosso, a sinistra, il valore di P è impostato su livelli relativamente alti, mentre L non cresce proporzionalmente e R rimane su valori medi. Questa combinazione produce un duplice effetto normativo: da un lato, la complessità procedurale erode la capacità del destinatario di accedere alla funzione informativa dell’atto; dall’altro, una capacità di correzione non particolarmente reattiva impedisce di recuperare l’opacità accumulata. Il risultato, come si può osservare in Figura 1, è una distribuzione schiacciata verso lo zero e prossima a valori persino

negativi, che esprime scarsa chiarezza e alta concentrazione di casi in cui l'atto resta, nella sostanza, incomprensibile ai destinatari finali. Tale fenomeno è coerente con le categorie classiche del diritto amministrativo, dove forme rigide, stratificazione e iper-formalismo possono generare un contenzioso endemico³² e, in prospettiva costituzionale ed europea, erodono il diritto al buon andamento della pubblica amministrazione e la parità di accesso ai procedimenti³³. Interessante è osservare il caso di *burocrazia ridotta* che mostra come intervenire soltanto su *P*, ovvero sulla semplificazione procedurale, non basti: nonostante la densità dei passaggi amministrativi venga compressa efficacemente, se non cresce *L* e se *R* non entra in retroazione, permane una dispersione residua molto ampia, giacché l'ordinamento non riesce a garantire un'uniformità dei guadagni cognitivi tra i vari destinatari della norma (si noti, in questa luce, come la curva *giallo chiaro*, in Figura 1, risulti molto schiacciata verso il basso e con una distribuzione molto dispersa). Il risultato della simulazione offre un messaggio molto chiaro al legislatore, mostrando come la mera semplificazione procedurale non sia, da sola, sinonimo di maggiore accessibilità, perché permangono ancora forti dispersioni all'interno di tutto il campione.

Un discorso a parte si può fare per le questioni comunicative, che costituiscono il banco di prova per la centralità della leggibilità. Lo scenario di *comunicazione opaca* – curva in *verde scuro*, schiacciata a sinistra in Figura 1 – conferma la centralità specifica di *L*: qui la leggibilità testuale è ridotta, e *R* non è, da sola, sufficiente ad assorbire l'opacità. La distribuzione si mantiene, infatti, su valori molto bassi – prossimi allo zero o persino negativi – ed altamente dispersivi, riflettendo il fatto che gli utenti finali che risultano più alfabetizzati da un punto di vista giuridico sopravvivono al carico interpretativo, mentre coloro che dispongono di minori strumenti cognitivi ne rimangono esclusi. Ciò che emerge è, pertanto, una differenziazione sistemica di accesso e comprensibilità dell'atto, con un effetto regressivo sul piano della capacità di fruizione dell'atto da parte di chi risulta avere minori strumenti per comprenderne le finalità³⁴. Nel caso

di *comunicazione chiara* da parte del legislatore – curva in verde chiaro, in Figura 1 – *L* è fissata su valori ridotti, mentre *P* e *R* rimangono alti. In questa configurazione, la distribuzione si sposta verso destra, ovvero verso valori più alti di chiarezza amministrativa (si noti un picco di valori che si registra in prossimità di uno, ovvero della massima chiarezza amministrativa) ma che diviene a mano a mano più omogenea. Ciò significa che la chiarezza testuale – ovvero il termine *L*, che rappresenta la leggibilità linguistica – normalizza la distribuzione, riducendo l'asimmetria cognitiva tra utenti esperti e inesperti, con l'effetto giuridico sostanziale di una diminuzione drastica della selettività di fatto nell'accesso al linguaggio amministrativo ed una caducazione della necessità di alfabetizzazione giuridica. In altri termini, con una maggiore leggibilità linguistica, un'evidente semplicità procedurale, che si accompagnano a stabilità organizzativa, più persone possono orientarsi in sicurezza e comprendere il linguaggio degli atti amministrativi in questione, riducendo le zone grigie in cui si annida l'incertezza interpretativa.

Infine, se si osservano più da vicino gli scenari di *correzione lenta* rispetto a quelli di *correzione rapida*, in cui si introduce una dimensione temporale, risulta evidente come *R* operi su un diverso asse rispetto a *L* e *P*. Anche a parità di leggibilità iniziale e complessità procedurale, la rapidità di feedback spinge porzioni significative della distribuzione verso valori più alti di chiarezza amministrativa, mostrando come, in termini dinamici, questo significhi che l'ordinamento apprende e corregge le proprie inefficienze, trasformando *C** in una variabile evolutiva. La ragione di questo risultato può essere individuata in un'amministrazione capace di integrare meccanismi di ascolto, riesame e revisione generale del testo amministrativo, capace di ridurre l'opacità normativa non perché originariamente chiara, ma in quanto maggiormente intelligibile alla luce dei *feedback* ricevuti. L'effetto sulla distribuzione non è dunque lineare, ma morfologico: non si alza solo la media, ma si accorcia la coda dei casi patologici. Ciò significa che un *regolatore* incapace di apprendere rapidamente dai *feedback* dei soggetti *regolati* può soltanto produrre dei

32. ALBERSTEIN 2012.

33. CELONE 2016.

34. BONETTI 2016.

miglioramenti incrementali, diluiti nel tempo e scarsamente redistributivi. Una correzione efficace, invece, deve espandersi verso valori intermedi e presentare, graficamente, una “coda” a destra più pronunciata. Si tratta, in questo senso, di un effetto di *densificazione dei casi positivi*: più iterazioni riescono a raggiungere soglie di chiarezza stabile, con la conseguenza di *chiudere falle sistemiche*; ridurre errori diffusi tra utenti ed amministrazione, consolidare prassi amministrative corrette e aumentare la prevedibilità dell’azione amministrativa.

Nel confronto sinottico, si nota chiaramente che gli scenari che lavorano su una sola dimensione producono distribuzioni fragili: la semplificazione procedurale senza leggibilità genera un plateau limitato; la leggibilità senza correzione rapida migliora la comprensione ma non elimina i casi patologici; la correzione lenta non riesce ad incidere sulle modalità di produzione degli atti e rimane inefficace nelle zone di bassa chiarezza. Solo negli scenari in cui due dimensioni convergono la curva si sposta visibilmente e migliora la propria distribuzione. La geometria delle curve riportate in Figura 1 suggerisce una lezione di policy profonda: la chiarezza amministrativa è una variabile *distributiva* prima che una media. I valori medi potrebbero ingannare, perché gli effetti normativi più dannosi emergono nelle code: quando molte oscillazioni simulano esiti vicini allo zero, l’impatto reale ricade sui soggetti meno equipaggiati. Da qui deriva la *ratio* del modello: *L* riduce gli ostacoli cognitivi individuali, *P* diminuisce gli ostacoli sistemici, mentre *R* limita gli ostacoli temporali. Se una di queste dimensioni non viene trattata, i fenomeni di opacità permangono in forma concentrata nella parte bassa della distribuzione, producendo contenzioso, incertezza, errori procedurali e regressività dell’accesso. Una curva che “si distribuisce” significa, da un punto di vista sistemico, un ordinamento più comprensibile, equo e prevedibile. Una curva che, invece, “collassa” sullo zero mostra un ordinamento sostanzialmente inaccessibile ai più.

4.2. Analisi di sensibilità dei pesi decisionali introdotti nel modello: verso un bilanciamento ottimale delle componenti della semplificazione

Il secondo blocco di simulazioni è inteso ad eseguire delle analisi di sensibilità, in base alle quali

non si valutano potenziali scenari alternativi, ma si valutano i pesi delle diverse configurazioni che i valori medi di chiarezza amministrativa C^* possono assumere sull’osservazione complessiva dei fenomeni qui studiati, rispondendo alla domanda su quali leve incidano, maggiormente, sulla comprensibilità dell’azione amministrativa. In particolare, la simulazione di sensibilità valuta proprio il “peso” attribuito alla *leggibilità linguistica* (λ) e alla *semplificazione procedurale* (σ), mantenendo costante una quota residua ($\delta = 1 - \lambda - \sigma$), che esprime la stabilità organizzativa e la *coerenza istituzionale* complessiva, ovvero incorpora la capacità di correzione, revisione e adattamento sistemico. Da un punto di vista operativo, l’algoritmo costruito con linguaggio *Python* identifica una griglia di valori per i pesi λ e σ (da 0.1 a 0.8) e calcola, per ogni combinazione, il corrispondente valore medio di chiarezza C^* . La superficie è costruita calcolando C^* per ciascuna combinazione di λ e σ , mantenendo δ come variabile derivata. Alla luce delle simulazioni, C^* cresce se il numeratore della funzione riduce la pressione cognitiva e aumenta la trasparenza, e decresce quando il denominatore aumenta i costi di decodifica. Si ottiene così una sorta di “panoramica” della comprensibilità istituzionale, che è visivamente riportata in Figura 2.

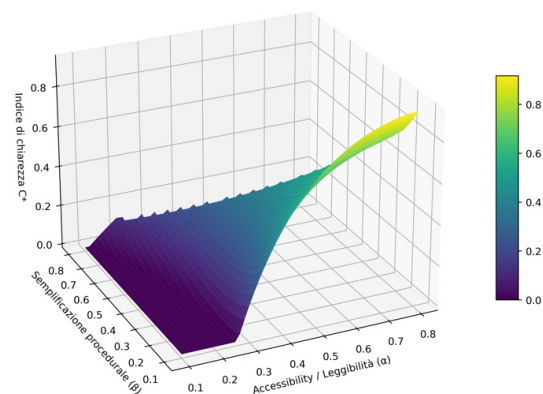


FIG. 2 — Superficie di sensibilità dell’indice di chiarezza amministrativa C^* al variare dei pesi attribuiti alla leggibilità linguistica (α) e alla semplificazione procedurale (la figura mostra, con una resa tridimensionale, la risposta dell’indice di chiarezza amministrativa C^* a fronte di variazioni parametriche dei pesi assegnati alle dimensioni della leggibilità e della semplificazione).

Il profilo emergente dai risultati riportati in Figura 2 non è simmetrico. La superficie tende ad assumere valori elevati nelle regioni in cui λ raggiunge intensità medio-alte, suggerendo che

la leggibilità costituisce il fattore maggiormente incisivo sulla compressione degli oneri cognitivi. Al contrario, un mero aumento di σ non produce un miglioramento ripido, evidenziando, invece, un effetto marginale differenziale rispetto alla chiarezza testuale. Le zone più depresse della superficie indicano configurazioni di sbilanciamento nella ponderazione dei pesi, che rivelano un'eccessiva enfasi sulla sola semplificazione procedurale, in assenza di un parallelo incremento di chiarezza linguistica, non produce miglioramenti significativi della comprensibilità. Il modello rende visibile una condizione ricorrente nell'esperienza giurisprudenziale italiana, in cui l'opacità semantica può talvolta generare interpretazioni antagoniste, alimentare il contenzioso e produrre un'erosione progressiva della capacità di comprensione degli utenti finali della norma³⁵. Ciò che emerge dalla Figura 2, pertanto, è che tanto più aumenta λ , maggiore è la crescita dei parametri, mostrando che intervenire sul linguaggio produce ritorni marginali elevati, soprattutto nelle fasi in cui il testo rischia di essere troppo tecnico o costruito in forme giuridiche che vengono individuate, troppo spesso, come teleologicamente prolisse³⁶.

Come già anticipato *supra*, invece, lungo l'asse σ , la superficie sale più lentamente. La semplificazione procedurale riduce tempi e costi, ma non incide sulla qualità inferenziale che il destinatario deve compiere per comprendere l'atto in questione. Nel modello, dopo una certa soglia, ridurre ulteriormente le fasi non migliora ulteriormente C^* : la comprensione non aumenta oltre un limite se il linguaggio rimane opaco. Si tratta, a ben vedere, di una condizione nella quale un procedimento più breve conduce comunque ad atti non leggibili. Se ne deduce, conseguentemente, un ruolo particolarmente sofisticato per la variabile residua δ , che diminuisce quando λ e σ aumentano contestualmente. In questo modo, il modello segnala che nonostante sia vero che ridurre le ridondanze procedurali possa giovare, è altrettanto vero che ciò significa eliminare anche i punti di verifica, gli audit informativi e le opportunità di intervento correttivo. Il grafico cattura esattamente questa tensione:

esiste un plateau in cui ulteriori incrementi dei pesi primari non incrementano C^* , proprio perché senza capacità di revisione la chiarezza rischia di non essere sostenibile nel lungo periodo. La chiarezza, in questo senso, è una qualità emergente che non deriva dalla sola leggibilità, né dalla sola semplificazione procedurale, ma dalla interazione di questi fattori con una forma di manutenzione istituzionale, profonda e radicale³⁷. Ciò rispecchia l'affidamento del cittadino, la necessità di controllo successivo degli atti e la fisiologia del buon andamento della pubblica amministrazione³⁸. Il grafico mostra inoltre che gli incrementi di leggibilità hanno rendimenti marginali non decrescenti fino a una soglia alta, mentre quelli procedurali raggiungono presto un livello di "saturazione" che mostra come il mero taglio di passaggi burocratici possa comportare effetti deludenti, giacché si semplifica l'iter senza ridurre l'ambiguità epistemica dell'atto. Infine, i risultati mostrano come sono altrettanto evidenti i rischi di politiche monoculari: un ordinamento che investe solo in leggibilità, senza riserva di revisione, rischia di fossilizzarsi; uno che investe solo nella semplificazione, senza cura del testo, rischia di accelerare la produzione normativa al prezzo di una crescente incomprensibilità diffusa; uno che investe solo nella revisione, senza aggredire né la lingua né le procedure, ricorre a rimedi *ex post ad infinitum*. In sintesi, il grafico non suggerisce solo che cosa funzioni meglio, ma *perché* la comprensione giuridica richieda un equilibrio tra chiarezza espressiva, snellimento funzionale e capacità di correzione, essendo necessaria che la maggior chiarezza si generi nella testa del destinatario, non nell'atto in sé. È qui che il modello matematico incontra la dogmatica: l'accessibilità degli atti andrebbe considerata come un bene pubblico e la sua produzione dipende fortemente da scelte linguistiche, organizzative e istituzionali governate da *trade-off* non lineari per le quali la superficie tridimensionale, di cui alla Figura 2, ne rende, in maniera lampante, la topografia.

35. CIVITARESE MATTEUCCI 2006.

36. CONTE 2013.

37. TORCHIA 1997.

38. LUCIANI 2016.

4.3. Proiezioni dinamiche in tema di accessibilità amministrativa e livello di semplificazione del linguaggio amministrativo: dalla teoria alla prassi

Il terzo blocco di simulazioni che è stato condotto a mezzo *Python* valuta, in termini dinamici, come cambi il livello di accessibilità rispetto al livello di semplificazione che si vuole introdurre nel sistema. Per procedere all'analisi dell'impatto che una maggiore semplificazione può comportare sulla intellegibilità degli atti, si è costruita una proiezione dinamica di una funzione, che possiamo chiamare $A(x)$, che simula l'andamento dell'accessibilità amministrativa al variare del livello di semplificazione x . Il modello su cui è fondata la simulazione assume la presenza di una serie di variabili casuali L_0, P_0, ϕ, θ in cui L e P sono parametri stocastici che rappresentano, da un lato, la dotazione iniziale di leggibilità testuale – ovvero il livello di chiarezza e intellegibilità del linguaggio amministrativo pre-esistente all'intervento di semplificazione – mentre, dall'altro lato, P descrive una forma di densità e rigidità procedurale – ovvero una misura sintetica dell'onere burocratico iniziale, ovvero della quantità di passaggi, verifiche e approvazioni che si rendono necessarie per l'intervento riformatore.

Entrambi gli indicatori altro non rappresentano che delle forme sintetiche dei noti *principi di trasparenza e comprensibilità degli atti* (artt. 1 e 3, legge n. 241 del 1990, nonché art. 97 Cost.), oltretutto del più generale *principio di proporzionalità organizzativa e di buon andamento della p.a.* (art. 97 Cost.). In questa prospettiva, la simulazione mostra come l'introduzione di condizioni iniziali differenziate consenta di modellare l'eterogeneità strutturale delle pubbliche amministrazioni, che, per ragioni istituzionali partono da diversi livelli di chiarezza o di carico procedurale, con chiare differenze sull'efficacia delle politiche di semplificazione. I parametri ϕ e θ rappresentano, in questa luce, il grado di resistenza interna che un'amministrazione oppone a ogni variazione strutturale del proprio modo di operare, per cui tanto più ϕ risulta alto, tanto più si rappresentano rigidità istituzionali che assorbono gran parte dell'efficacia della semplificazione. Al contempo, definiamo θ quale parametro di inerzia istituzionale che opera su un piano dinamico e

temporale, con la conseguenza diretta che un valore più alto di θ indica che la struttura amministrativa tende a mantenere più a lungo gli effetti delle proprie configurazioni passate. In questa prospettiva, la variazione di accessibilità $A(x)$, in risposta a un aumento di x , sarà più lenta e più attenuata.

Nella simulazione Monte Carlo, la combinazione di ϕ e θ consente di introdurre, in forma probabilistica, la dinamica della razionalità limitata e patologica della pubblica amministrazione³⁹. In contropartita, la dotazione iniziale di leggibilità e la pressione procedurale fungono, in contemporanea, da vincoli sistemici e frizioni al cambiamento. Tutti e quattro i parametri concorrono a determinare la traiettoria della funzione di accessibilità amministrativa $A(x)$ e della chiarezza complessiva C^* , permettendo di osservare come il sistema reagisca, nel tempo, a strategie diverse di semplificazione e revisione. Si ottiene così una sorta di “panoramica” della comprensibilità istituzionale, visivamente riportata in Figura 3.

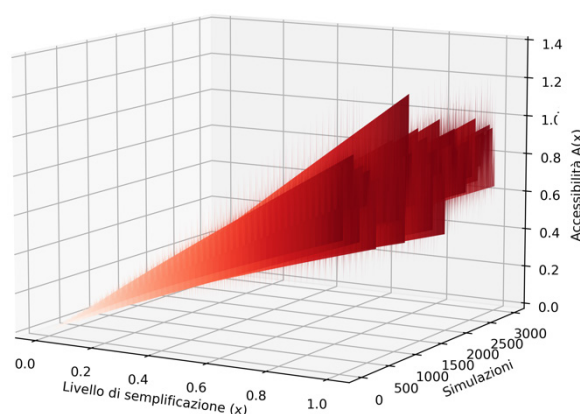


FIG. 3 — Proiezione dinamica simulata dell'accessibilità amministrativa $A(x)$ generata tramite tecniche Monte Carlo al variare del livello di semplificazione procedurale (la figura rappresenta l'evoluzione dell'accessibilità amministrativa $A(x)$ lungo diverse iterazioni, al variare del livello di semplificazione x compreso tra 0 e 1. La superficie mostra l'effetto congiunto di variabili latenti quali leggibilità iniziale, complessità procedurale e coefficienti di dispersione, che contribuiscono a modulare l'impatto incrementale degli interventi di semplificazione).

I risultati mostrano una relazione complessivamente positiva tra il livello di semplificazione x e l'accessibilità amministrativa $A(x)$. In particolare, la superficie evidenzia una crescita inizialmente marcata dell'accessibilità al crescere della

39. In questa prospettiva, si veda VIALE 2016.

semplificazione, cui segue una progressiva attenuazione degli incrementi marginali, riconducibile a fenomeni di rendimenti decrescenti. L'andamento complessivo risulta pertanto mediamente monotono, ma non lineare. Dal punto di vista tecnico, il grafico mostra una crescita mediamente monotona dell'accessibilità amministrativa in funzione del livello di semplificazione, accompagnata da oscillazioni locali e discontinuità, soprattutto nelle fasi intermedie del processo. Tali irregolarità non costituiscono anomalie del modello o errori di calcolo, bensì espressioni della struttura stocastica delle simulazioni, segnalando la presenza di zone di instabilità, nelle quali piccoli interventi marginali di semplificazione possono generare effetti sensibilmente diversi, talora amplificati, talora inefficaci o trascurabili. In alcuni contesti simulati, l'aumento di x determina miglioramenti rapidi e persistenti dell'accessibilità al testo normativo; in altri casi, invece, gli effetti risultano contenuti o temporanei, a causa dell'elevata inerzia istituzionale incorporata nei parametri del modello. Ciò conferma l'ipotesi secondo cui la semplificazione amministrativa non generi incrementi proporzionali e automatici di accessibilità, ma operi attraverso dinamiche non lineari, da soglie critiche e da effetti cumulativi. Una più approfondita lettura di questa simulazione suggerisce che la qualità dell'accesso amministrativo non dipende esclusivamente dalla quantità di semplificazione introdotta – nella forma di norme eliminate o accorpate – bensì dal modo in cui le riforme incidono sulle strutture sottostanti del sistema. Quando persistono elevati livelli di attrito amministrativo – a causa di prassi interpretative, rigidità organizzative o frammentazione delle competenze – l'effetto della semplificazione risulta attenuato, producendo una traiettoria di crescita lenta e irregolare. Viceversa, in contesti in cui la semplificazione è accompagnata da una revisione delle logiche procedurali e da un efficace coordinamento istituzionale, l'incremento di x si traduce in un'accelerazione tangibile dell'accessibilità, rappresentato dalla fascia superiore della superficie.

Sempre da un punto di vista tecnico, le oscillazioni osservate nella superficie possono essere interpretate come l'effetto della propagazione delle variazioni nei parametri stocastici del modello. In particolare, i termini di leggibilità normativa (L_0) e di pressione procedurale (P_0) sono estratti da distribuzioni normali centrate su valori medi,

con deviazioni standard calibrate in modo da riflettere l'eterogeneità del tessuto amministrativo. Tale impostazione fa sì che, a parità di incremento del livello di semplificazione, gli esiti in termini di accessibilità possano differire sensibilmente tra le diverse simulazioni. Ne consegue che, in alcuni scenari, l'aumento del livello di semplificazione generi miglioramenti rapidi ma relativamente stabili dell'accessibilità amministrativa; in altri casi, la medesima variazione produce effetti più contenuti o persino regressivi, in ragione dell'interazione con il coefficiente di attrito amministrativo (ϕ) elevato e/o con il parametro di inerzia istituzionale (θ) significativo. In termini dinamici, ciascuna simulazione rappresenta un equilibrio contingente tra forze di accelerazione – legate, ad esempio, alla digitalizzazione o alla riduzione degli oneri procedurali – e forze di resistenza – riconducibili, per fare un esempio, a prassi burocratiche sedimentate, rigidità organizzative o deficit di coordinamento inter-organico. Questa variabilità rende visibile una proprietà strutturale e sistemica dell'ordinamento: la semplificazione non opera come un processo puramente additivo, bensì come un campo di forze soggetto a effetti di soglia e potenziali *feedback* endogeni, degli utenti finali della norma in questione. Oltre un certo livello, la riduzione della complessità normativa può infatti indebolire la capacità di controllo e di coerenza decisionale del sistema, generando fenomeni di frammentazione dell'azione amministrativa. Al contrario, il mantenimento di un grado minimo di articolazione regolatoria preserva un "tessuto connettivo" istituzionale, funzionale alla garanzia di uniformità, prevedibilità e affidabilità delle decisioni. Da un punto di vista visivo, infine, la parte superiore della superficie – dove la funzione $A(x)$ tende alla saturazione – rappresenta precisamente questa soglia ottimale, nella quale l'accessibilità dei cittadini risulta massimizzata senza compromettere la stabilità istituzionale. In una prospettiva sistemica, il modello suggerisce che la semplificazione più efficiente sia quella che elimina la complessità superflua senza intaccare la complessità necessaria, ossia quella che sostiene trasparenza, motivazione, tracciabilità di fondo e legittimo affidamento. Il punto di equilibrio individuato empiricamente dalla simulazione può essere interpretato, in tal senso, come una forma di proporzionalità istituzionale, nella quale la

riduzione del carico regolatorio deve essere calibrata in funzione della capacità istituzionale di assorbire e rielaborare il necessario cambiamento.

5. Implicazioni sistemiche e ragioni giuseconomiche in tema di riduzione della complessità del linguaggio amministrativo

La ricostruzione teorica e le evidenze computazionali espone nei paragrafi precedenti consentono di formulare alcune considerazioni di sintesi, che si collocano nel solco dell'impostazione proposta e ne rappresentano il punto di convergenza sistemica. La formalizzazione del processo di semplificazione amministrativa, unitamente alla sua verifica simulativo-computazionale, mostra come l'architrave di tale processo di semplificazione risieda nell'interdipendenza di tre fattori principali: una maggiore chiarezza linguistica, una spiccata semplicità procedurale e una rinnovata ed efficiente stabilità organizzativa, capace di determinare un coordinamento istituzionale tra tutti gli attori coinvolti e gli *stakeholder* – che altro non sono che i consociati a cui si rivolge la amministrazione medesima – con la costruzione di un equilibrio in cui la riduzione della complessità amministrativa non assume un carattere di mero obiettivo di politica regolatoria o di efficienza gestionale, bensì come ampio intervento di razionalizzazione del rapporto tra ordinamento e destinatari, nel quale si ridefiniscono le condizioni stesse dell'effettività dell'azione dei pubblici poteri⁴⁰.

L'adozione di un *indice di chiarezza amministrativa* e la sua manipolazione parametrica rendono empiricamente osservabili i legami che intercorrono fra struttura normativa e qualità del linguaggio istituzionale⁴¹, mostrando come entrambe le caratteristiche incidano, in ultima analisi, sul comportamento degli attori che le norme intendono regolare⁴². Ciò che emerge dall'analisi è l'esistenza di una relazione sistemica tra la qualità linguistica

degli atti amministrativi e la distribuzione dei costi di interazione tra amministrazione e destinatari finali dell'atto. Un documento redatto in forma opaca, oltre a compromettere la trasparenza dell'azione pubblica, determina un incremento dei costi cognitivi e interpretativi che si riflettono sull'intero ciclo di vita dell'atto: dalla fase dell'adozione a quella di esecuzione, fino all'eventuale fase patologica del contenzioso. La complessità amministrativa si traduce, in questo modo, in nuove forme di inefficienza strutturale, poiché la difficoltà di decodifica linguistica accresce il fabbisogno di mediazione specialistica, amplifica le asimmetrie informative e rallenta i flussi decisionali, con effetti negativi che si riverberano sull'equilibrio complessivo del sistema. In una chiave di lettura più ampia, i risultati ottenuti consentono di interpretare la chiarezza non come semplice requisito formale, bensì come variabile di ottimizzazione istituzionale, in cui il linguaggio amministrativo, lungi dal rappresentare una mera modalità espressiva, diviene un fattore produttivo del sistema regolatorio, la cui qualità incide sulla prevedibilità delle condotte, sull'efficienza allocativa delle risorse pubbliche e sulla riduzione dei costi di transazione nei rapporti tra amministrazione ed amministrati. I risultati empirici mostrano, infatti, che l'indice di chiarezza può essere letto come un parametro di efficienza sistemica, in quanto misura la capacità dell'ordinamento di generare informazione utile e ridurre, in ultima istanza, l'incertezza giuridica che, come noto, comporta innumerevoli esternalità negative ed un aggravamento generale dei costi di transazione⁴³. All'aumentare della chiarezza amministrativa, infatti, corrisponde una diminuzione della dispersione interpretativa ed una conseguente riduzione di ciò che potremmo definire come "entropia normativa"⁴⁴, con effetti tangibili di disallineamento ed eterogeneità tra le rappresentazioni cognitive che i destinatari elaborano rispetto al contenuto del medesimo atto⁴⁵.

40. PELLIZZARI 2012.

41. Cfr. RASO 2005 e CORTELAZZO-PELLEGRINO 2003.

42. TODOROV 2005.

43. Cfr. DARI-MATTIACCI-DEFFAINS 2007, HADFIELD 1994, WEISS 2019, BEHRENDT 2025.

44. SIMONATI 2013.

45. È chiaro che un disallineamento tra interpretazioni del medesimo atto è problematico per diverse ragioni, giacché la pluralità di letture possibili può generare un margine di indeterminatezza che mina la prevedibilità

In tal senso, la chiarezza si configura come una condizione strutturale di stabilità e affidabilità dell'azione amministrativa e del buon funzionamento dell'ordinamento, in quanto fattore decisivo per la comprensibilità dei precetti normativi che il sistema istituzionale, nel suo complesso, è chiamato a produrre e applicare. La *chiarezza normativa*, in questa prospettiva, incide direttamente sulla capacità dei destinatari di orientare le proprie condotte in modo conforme alle richieste del legislatore, riducendo l'area di incertezza interpretativa e rafforzando il principio di prevedibilità dell'azione pubblica. In assenza di un adeguato livello di chiarezza, infatti, si è visto che il contenuto normativo tende a frammentarsi con effetti distorsivi tanto sull'effettività della regolamentazione quanto sulla legittimazione dell'intervento amministrativo. La chiarezza amministrativa opera, in questa prospettiva, come meccanismo di allineamento cognitivo tra amministrazione e cittadini, contribuendo a stabilizzare le aspettative e a contenere i costi di coordinamento che gravano sull'intero sistema. La semplificazione non può essere intesa, in tal senso, come mera sottrazione di regole, ma come un processo qualitativo di riorganizzazione del linguaggio, delle procedure e delle strutture decisionali, volto a rendere intellegibile e coerente l'esercizio del potere pubblico. Ne deriva che molte delle politiche di semplificazione – quali quelle legate alle procedure di semplificazione normativa in ambito finanziario di cui ai vari “pacchetti Omnibus” europei – risultano disancorate da un vero e proprio investimento sulla chiarezza, rischiando di produrre effetti solo apparenti, lasciando invariati – o addirittura aggravando – i livelli di complessità percepita dai destinatari finali della norma, siano essi imprese, consumatori, o semplici utenti finali.

Tutte le simulazioni presentate mostrano, infatti, come la semplificazione procedurale – che è stata, negli ultimi decenni, obiettivo primario e complementare rispetto alla trasparenza propugnata dal legislatore⁴⁶ – non produca effetti duraturi in termini di accessibilità se non accompagnata da

un corrispondente miglioramento della leggibilità degli atti. Ciò dipende dal fatto che la complessità amministrativa non è riconducibile esclusivamente alla sequenza formale dei passaggi decisionali, ma risiede anche nella densità semantica del linguaggio impiegato e nella sua capacità di orientare in modo efficace le condotte dei destinatari⁴⁷. In una prospettiva sistemica, la semplificazione deve essere intesa come un processo di riequilibrio interno tra complessità necessaria e complessità patologica. La prima risulta funzionale alla tutela di principi strutturali quali la trasparenza, la tracciabilità e l'obbligo di motivazione; la seconda, invece, è il prodotto di inerzie organizzative e retaggi linguistici che amplificano l'opacità regolatoria degli atti, senza apportare benefici in termini di garanzie sostanziali. Le risultanze quantitative emerse dalle simulazioni Monte Carlo consentono, tuttavia, di individuare un punto ottimale di equilibrio tra queste due dimensioni. Da un lato, un'eccessiva contrazione delle fasi procedurali può compromettere i livelli di controllo interno e di garanzia formale; dall'altro lato, una proliferazione non selettiva delle procedure determina un aumento significativo dei costi di accesso e di comprensione degli atti da parte dei destinatari. Il modello conferma dunque che l'efficacia della semplificazione dipende dalla sua calibrazione, e non dalla sua intensità, ponendo in evidenza la necessità di interventi mirati, capaci di ridurre la complessità superflua senza indebolire l'architettura complessiva dell'ordinamento.

Da un punto di vista distributivo, le evidenze empiriche rivelano una dinamica di rilievo sorprendente – anche se non del tutto inaspettata – nella misura in cui l'opacità linguistica non si limita a generare inefficienze complessive, ma produce effetti regressivi che incidono in modo sproporzionato sui destinatari dotati di minori competenze giuridiche e, più in generale, linguistiche. Si delinea così una forma di *diseguaglianza cognitiva* che, pur non essendo intenzionale né esplicitamente prevista, introduce una selettività

dell'agire pubblico e la fiducia dei cittadini nelle istituzioni, anche in ragione della introduzione di elementi di discrezionalità applicativa non riconducibili a scelte di merito, ma a differenze puramente linguistiche o concettuali.

46. Cfr., per degli esempi concreti, PAGANO 2024 e CAPORALE 2021.

47. CIRILLO 2017.

sostanziale nell'accesso all'ordinamento⁴⁸, compromettendo l'uniformità delle condizioni di comprensione e di partecipazione alle dinamiche sociali previste dall'ordinamento. In questa luce, la chiarezza amministrativa non si configura soltanto come presupposto più generale di maggiore trasparenza ed efficienza normativa, ma come uno strumento di equità sostanziale, in quanto consente di rimuovere le barriere cognitive che ostacolano un'effettiva parità di accesso ai diritti e agli obblighi pubblici. Ne deriva che la chiarezza non può più essere intesa come un mero indicatore di efficienza amministrativa, ma assume la valenza di fattore causale di giustizia distributiva, poiché incide sulla capacità dei cittadini di comprendere le regole, di conformarvisi e di partecipare consapevolmente allo spazio pubblico regolato.

Sul piano dogmatico, tale conclusione sollecita una riflessione sullo statuto della chiarezza quale principio di efficacia sostanziale dell'azione pubblica. Un atto oscuro o ambiguo, pur formalmente legittimo, rischia infatti di tradire la propria funzione di orientamento e di garanzia, ponendosi in contrasto con i principi di buon andamento e di imparzialità sanciti a livello costituzionale⁴⁹. Le evidenze riportate in questo scritto contribuiscono a rendere empiricamente osservabile la nozione di chiarezza, mostrando come questa rivesta una natura funzionale e non meramente ornamentale, sia in termini di aumento della fiducia istituzionale che di miglior allocazione di tutte le risorse che si intendono investire in attività di semplificazione e di maggiore accessibilità del diritto da parte dei consociati. La chiarezza, da un punto di vista di teoria economica, emerge come un elemento costitutivo dell'efficienza complessiva dell'ordinamento, nella misura in cui riduce il fabbisogno di interpretazione mediata, attenua le frizioni informative e rafforza la funzione predittiva delle regole, così da ridurre le esternalità negative che possono insidiarsi in norme poco chiare⁵⁰ e migliorare la qualità della governance pubblica⁵¹. La conseguente riduzione del contenzioso, evidenziata nei

modelli simulati attraverso la diminuzione delle penalità sistemiche, non rappresenta soltanto un esito empirico contingente, ma conferma il valore economico della certezza e della chiarezza giuridica. Quanto più tali dimensioni vengono perseguite in modo coerente ed efficace, tanto più si riducono i costi collettivi di coordinamento e si accresce la produttività istituzionale complessiva. In questo senso, la chiarezza amministrativa si colloca al centro di una trasformazione più profonda del modo di concepire l'amministrazione non già come mero apparato di produzione normativa, bensì come sistema di comunicazione giuridica orientato alla comprensione, all'equilibrio regolatorio e rivolto ad una più elevata responsabilità del regolatore nei confronti dei regolati.

6. Conclusioni

Il presente lavoro si è proposto di delineare un quadro coerente di analisi volto a mostrare come la chiarezza del linguaggio non solo possa favorire una più efficace semplificazione amministrativa – in linea con gli auspici e gli obiettivi perseguiti del legislatore – ma consenta altresì di riportare al centro il principio di effettività e di giustizia sostanziale fulcro delle disposizioni costituzionali in tema di buon andamento della pubblica amministrazione e, più in generale, di efficienza sistemica⁵². Il percorso argomentativo sviluppato sin qui ha evidenziato come la riduzione della complessità amministrativa non coincida affatto con una mera eliminazione di norme o procedimenti, bensì con la ricostruzione di un equilibrio funzionale tra chiarezza linguistica, semplicità procedurale e stabilità organizzativa, capace di tradurre la semplificazione in una dimensione cognitiva, comunicativa e, finanche, democratica. La chiarezza assume, in questa veste, il valore di un vero e proprio bene pubblico, da perseguire e tutelare, configurandosi come condizione epistemica di legalità di tutto l'ordinamento. Laddove il legislatore, anche per mezzo delle proprie articolazioni amministrative, non sia in grado di rendere intellegibili le proprie prescrizioni, viene

48. Su questo aspetto si veda DICIOTTI 2015.

49. DI MARTINO 2023.

50. Per alcuni esempi, in ambito finanziario, si veda MACEY 2005.

51. FARINA-NEWHART-BLAKE 2014.

52. Cfr., sul punto, SPASIANO 2011 e DE MAGLIE 2022.

meno la possibilità, per i destinatari, di comprendere pienamente quale sia il comportamento richiesto e, più in generale, il precetto a cui conformarsi. Ne discende la necessità di ripensare il rapporto tra istituzioni e cittadini come un più ampio progetto di rifondazione del rapporto tra diritto e società, nella consapevolezza che un'amministrazione più chiara è, al tempo stesso, più giusta, più efficiente e più democratica.

Sotto il profilo metodologico, il lavoro ha dapprima formalizzato un modello teorico di integrazione della chiarezza nell'articolato amministrativo, per poi fornire una misurabilità empirica dell'impatto che i parametri considerati esercitano sulla qualità complessiva delle regole che l'amministrazione comunica, impone, e applica ai propri destinatari. Tale modello, costruito su un impianto teorico-formale, è stato successivamente sottoposto a verifiche mediante simulazioni Monte Carlo che, nelle loro diverse articolazioni, hanno confermato come una semplificazione realmente efficace si manifesti solo allorquando la riduzione dei passaggi procedurali sia accompagnata da un parallelo incremento della leggibilità e da un'adeguata capacità di correzione reattiva da parte dell'ordinamento. La chiarezza, in questa prospettiva, non si presenta come un risultato istantaneo, bensì come un processo evolutivo di apprendimento istituzionale, nel quale il sistema amministrativo adatta progressivamente le proprie pratiche secondo dinamiche non lineari, caratterizzate dall'esistenza di soglie oltre le quali la mera riformulazione del linguaggio o la semplificazione procedurale non producono benefici ulteriori e possono, anzi, compromettere la coerenza sistemica delle regole imposte dal legislatore. Si è osservato, nel corso di questo scritto, come un incremento della chiarezza linguistica contribuisca in modo significativo alla riduzione dei costi di transazione e al rafforzamento della fiducia istituzionale, traducendosi in una maggiore prevedibilità delle decisioni e in una più equa distribuzione delle informazioni. In termini sostanziali, la chiarezza realizza una forma di *uguaglianza cognitiva*, giacché consente a tutti i cittadini – indipendentemente dal loro capitale linguistico o giuridico – di accedere in modo effettivo alla sfera del diritto e di comprendere le ragioni e le finalità delle decisioni che li riguardano.

L'impianto teorico e le risultanze empiriche contenute nel presente lavoro suggeriscono, pertanto, una riformulazione del principio di semplificazione a tendere verso un *principio di comprensibilità amministrativa*, dotato di autonoma valenza dogmatica e operativa. In questa prospettiva, il legislatore e la pubblica amministrazione dovrebbero orientare le politiche di riforma del linguaggio normativo non soltanto verso una maggiore digitalizzazione o una riduzione formale degli oneri, ma verso l'instaurazione di un processo autenticamente dialogico, fondato su una comunicazione chiara, coerente e intelligibile tra istituzione e cittadini. In un momento storico in cui aumenta il divario di alfabetizzazione all'interno della popolazione⁵³ è evidente che tale impostazione implichi un mutamento di paradigma. La semplificazione non può essere più concepita come mera riduzione del numero di norme vigenti, bensì come un processo qualitativo che aiuti il cittadino ad "apprendere" e "comprendere" ciò che gli viene richiesto dagli organi pubblici in termini di doveri e quanto gli spetta in termini di diritti. In tal senso, la comprensibilità amministrativa si configura come una condizione precipua per l'effettività del sistema regolatorio, per la riduzione delle asimmetrie informative eventualmente presenti sul mercato e per il rafforzamento della fiducia tra cittadini e istituzioni, contribuendo a trasformare l'azione collettiva da mero esercizio di autorità a pratica di governo orientata a responsabilità, partecipazione allargata e legittimità sostanziale.

In questa prospettiva, il legislatore e la pubblica amministrazione sono chiamati a promuovere strumenti normativi e tecnici efficaci che rendano l'ordinamento non soltanto più accessibile, ma anche più efficiente nel permettere ai cittadini di interagire coerentemente e consapevolmente con lo Stato e con le sue articolazioni amministrative. La semplificazione normativa, in questo quadro, dovrebbe configurarsi come strumento di riduzione dei divari linguistici e cognitivi esistenti, così da rendere la regolamentazione di mercati, imprese e cittadini maggiormente comprensibile e intellegibile per la più ampia gamma di destinatari, inclusi coloro che non possiedono competenze giuridiche o tecniche avanzate. La transizione da un criterio di fittizia semplificazione – fondato su criteri

53. Si vedano, su questo tema, assolutamente non secondario, i dati riportati in LAMBOGLIA 2021.

meramente quantitativi di riduzione del numero delle norme o dei passaggi procedurali – non rispecchia il principio di chiarezza e comprensibilità amministrativa che è stato richiamato a più riprese in questo scritto, anche per mezzo della formazione della stessa pubblica amministrazione riguardo alle diverse esigenze della cittadinanza. In tale ottica, la semplificazione si traduce in un processo inclusivo, volto a garantire che ogni individuo possa accedere in modo effettivo al diritto, senza essere escluso o penalizzato dalla complessità del linguaggio normativo. Ne consegue che la chiave di volta per un'efficace semplificazione normativa

non risieda soltanto nell'adozione di tecnologie più avanzate o nell'eliminazione di passaggi burocratici superflui, ma in una trasformazione più profonda della cultura amministrativa, chiamata a porre la comprensibilità al centro della propria attività dialogica con i destinatari finali dei propri atti. Un simile approccio non solo rafforzerebbe la trasparenza e l'efficienza dell'azione pubblica, ma contribuirebbe, in modo decisivo, ad accrescere la fiducia dei cittadini nelle istituzioni e nel sistema normativo nel suo complesso, favorendo una partecipazione più attiva, informata e responsabile di tutti gli attori coinvolti.

Riferimenti bibliografici

- M. AINIS (1997), *La legge oscura: come e perché non funziona*, Laterza, 1997
- M. ALBERSTEIN (2012), *Measuring legal formalism: Reading hard cases with soft frames*, in A. Sarat (ed.), "Studies in Law, Politics, and Society", Emerald, 2012, pp. 161-199
- J. BEHRENDT (2025), *Uncertainty-Related Transaction Costs in EU Law for Entrepreneurs Developing and Operating Microgrids*, in K.B. Atici, A.B. Semerci, H. Kabakci, P. Shrestha (eds.), "Energy Entrepreneurship, Sustainability, Innovation and Financing: Practical Applications and Future Directions", Springer Nature Switzerland, 2025, pp. 221-241
- M. BOMBARDELLI (2015), *Semplificazione normativa e complessità del diritto amministrativo*, in "Diritto pubblico", 2015, n. 3, pp. 985-1064
- P. BONETTI (2016), *L'uso della lingua negli atti concernenti l'ingresso, il soggiorno e l'allontanamento degli stranieri e nell'accesso al diritto di asilo*, in P. Bonetti (a cura di), "L'uso della lingua negli atti e nella comunicazione dei poteri pubblici italiani", Giappichelli, 2016, pp. 571-623
- P. BONETTI, S. TROILO (2016), *L'uso della lingua negli atti e nella comunicazione dei poteri pubblici italiani*, in P. Bonetti (a cura di), "L'uso della lingua negli atti e nella comunicazione dei poteri pubblici italiani", Giappichelli, 2016, pp. 113-160
- L. BREGGIA (2013), *La semplificazione del linguaggio giuridico negli atti processuali*, in F. Bambi, A. Mariani Marini (a cura di), "Lingua e diritto: scritto e parlato nelle professioni legali", Pisa University Press, 2013, pp. 15-25
- D. BRUNATO (2014), *Complessità necessaria o stereotipi del "burocratese"? Un'indagine sulla leggibilità del linguaggio amministrativo da una prospettiva linguistico-computazionale*, in "Atti del XIII Congresso della Società Internazionale di Linguistica e Filologia Italiana (SILFI)" (Palermo, 22-24 settembre 2014), 2014
- S. CARBONE, F. FIAMMA, T. MARCELLI, V. MIRRA, D. ZAOTTINI (2016), *La qualità della regolazione nell'esperienza della Consob: Dalla misurazione degli oneri amministrativi al ciclo della valutazione. Il caso dell'equity crowdfunding*, CONSOB Discussion papers, 2016, n. 6, pp. 1-79
- C. CELONE (2016), *Il diritto alla buona amministrazione tra ordinamento europeo ed italiano*, in "Diritto dell'economia", 2016, n. 3, pp. 669-703
- A. CIRILLO (2017), *Parole in comune: il linguaggio della pubblica amministrazione tra conservazione e innovazione*, Franco Angeli, 2017

- A. CIRILLO (2011), *L'amministrazione relazionale: modelli comunicativi di Public Governance*, in "Rivista trimestrale di scienza della amministrazione", 2011, pp. 59-78
- S. CIVITARESE MATTEUCCI (2006), *Miseria del positivismo giuridico? Giuspositivismo e scienza del diritto pubblico*, in "Diritto pubblico", 2006, n. 3, pp. 685-750
- N. COLLEO (2022), *Il principio di legalità nel diritto amministrativo in evoluzione. Riflessioni sulla sua attualità e sul suo avvenire, tra fattori di crisi e rapporti con il potere normativo delle autorità amministrative indipendenti*, in "PA Persona e Amministrazione", 2022, n. 2, pp. 487-532
- G. CONTE (2013), *Il linguaggio della difesa civile*, in F. Bambi, A. Mariani Marini (a cura di), "Lingua e diritto: scritto e parlato nelle professioni legali", Pisa University Press, 2013, pp. 35-67
- M.A. CORTELAZZO (2021), *Il linguaggio amministrativo. Principi e pratiche di modernizzazione*, Carocci, 2021
- M.A. CORTELAZZO (2015), *Il cantiere del linguaggio istituzionale. A che punto siamo?*, in "LeGes", vol. 26, 2015, pp. 135-150
- M.A. CORTELAZZO, F. PELLEGRINO (2003), *Guida alla scrittura istituzionale*, Laterza, 2003
- G. DARI-MATTIACCI, B. DEFFAINS (2007), *Uncertainty of law and the legal process*, in "Journal of Institutional and Theoretical Economics (JITE) / Zeitschrift für die gesamte Staatswissenschaft", 2007, pp. 627-656
- M. DE BENEDETTO, N. RANGONE (2019), *La questione amministrativa dell'effettività: regole, decisioni e fatti*, in "Diritto pubblico", 2019, n. 3, pp. 747-792
- F. DE GIORGIS (2023), *Le disposizioni generali in materia di chiarezza e sinteticità degli atti processuali nella riforma Cartabia*, in "Judicium", 2023, pp. 1-13
- C. DE MAGLIE (2022), *Linguaggio del diritto penale e principio di effettività: spunti di riflessione*, in "Criminalia", 2022, pp. 43-50
- C. DI MARTINO (2023), *Il diritto costituzionale alla «non radicale inintelligibilità» delle disposizioni*, in "Consulta Online", 2023, n. 3, pp. 960-990
- E. DICIOTTI (2015), *Equivocità dei testi normativi, norme espresse e norme inesprese*, in "Analisi e diritto", 2015, n. 1, pp. 47-70
- M. DOGLIANI (2008), *Il principio di legalità dalla conquista del diritto all'ultima parola alla perdita del diritto alla prima*, in "Diritto pubblico", 2008, n. 1, pp. 1-28
- G. DUCCI (2013), *La comunicazione pubblica digitale per la trasparenza, l'accountability e il dialogo con i cittadini: verso una PA open e condivisa*, in "Autonomie locali e servizi sociali", 2013, n. 3, pp. 461-470
- C.R. FARINA, M.J. NEWHART, C. BLAKE (2014), *The Problem with Words: Plain Language and Public Participation in Rulemaking*, in "George Washington Law Review", vol. 83, 2014, pp. 1358-1409
- G. FIORENTINO (2007), *Web usability e semplificazione linguistica nella scrittura amministrativa*, in F. Venier (a cura di), "Rete Pubblica. Il dialogo tra Pubblica Amministrazione e cittadino: linguaggi e architettura dell'informazione", Guerra Edizioni, 2007, pp. 11-37
- S. FOA (2025), *Il nuovo merito amministrativo*, Giappichelli, 2025
- D. FORTIS (2005), *Il dovere della chiarezza. Quando farsi capire dal cittadino è prescritto da una norma*, in "Rivista italiana di comunicazione pubblica", 2005, n. 25, pp. 1000-1035
- B. GIANNOTTI (2007), *Il linguaggio delle istituzioni*, in "Studi Urbinati, B-Scienze umane e sociali", vol. 77, 2007, pp. 329-352
- G.K. HADFIELD (1994), *Weighing the value of vagueness: An economic perspective on precision in the law*, in "California Law Review", vol. 82, 1994

- R. LAMBROGLIA (2021), *Strumenti diagnostici del ROLL: i test di posizionamento per la misurazione del learning loss e la costruzione metacognitiva*, in E. Lastrucci, D. Milito, E. Surmonte (a cura di), "Analfabetismo funzionale e strategie di contrasto. Approcci, sperimentazioni, esperienze europee", Basili-cata University Press, 2021, pp. 328-358
- R. LIBERTINI (2020), *Perché scrivere chiaro. Dal semplicismo alla pertinenza del linguaggio giuridico (ai fini del discorso e dei suoi destinatari)*, in "Rivista italiana di informatica e diritto", 2020, n. 1, pp. 43-59
- M. LUCIANI (2016), *Il linguaggio dell'avvocato*, in "Revista do Instituto de Hermenêutica Jurídica", vol. 14, 2016, n. 20, pp. 73-87
- J. MACEY (2005), *The Limits of Legal Analysis: Using Externalities to Explain Legal Opinions in Structured Finance*, in "Texas Law Review", vol. 84, 2005, pp. 75-82
- S. MARGIOTTA (2021), *Certezza del diritto e diritto positivo*, in "Nomos, quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale", 2021, n. 1, pp. 1-37
- B.G. MATTARELLA (2019), *La semplificazione amministrativa come strumento di sviluppo economico*, in "Astrid Rassegna", 2019, n. 11, pp. 1-10
- U. NIZZA (2022), *Analisi quantitativa di dati giuridici*, in C. Rossi Chauvenet, S. Martinelli (a cura di), "Legal Tech, Big Data e contratti smart per professionisti e imprese", Wolters Kluwers, 2022
- A. ODDENINO (2024), *Pervasività, centralità geopolitica e molteplicità delle istanze di tutela della cybersicurezza: elementi introduttivi*, in "Teoria e Critica della Regolazione Sociale", 2024, n. 2, pp. 15-24
- E. PAGANO (2024), *Art. 50 D. Lgs. 36/23, un difficile equilibrio tra istanze di semplificazione procedurale ed interpretazione comunitariamente orientata*, in "Amministrativ@mente – Rivista di Ateneo dell'Università degli Studi di Roma 'Foro Italico'", 2024, n. 1, pp. 197-208
- S. PELLIZZARI (2012), *Make it better and simpler. Semplificazione amministrativa e principio di semplicità dell'azione dei pubblici poteri nell'ambito dell'ordinamento dell'Unione Europea*, in "Diritto pubblico", 2012, n. 1, pp. 265-298
- M. PICCHI (2013), *Tecniche normative e tutela del buon andamento della Pubblica Amministrazione: dalla Corte costituzionale un nuovo impulso per preservare la certezza del diritto (osservazioni a margine della sentenza n. 70/2013)*, in "federalismi.it", 2013, n. 21
- M.M. PIEMONTESE (1996), *Capire e farsi capire. Teorie e tecniche della scrittura controllata*, Tecnodid, 1996
- A. RASKOLNIKOV (2007), *The Cost of Norms: Tax Effects of Tacit Understandings*, in "University of Chicago Law Review", vol. 74, 2007
- T. RASO (2005), *La scrittura burocratica. La lingua e l'organizzazione del testo*, Carocci, 2005
- R.Y. RUBINSTEIN, D.P. KROESE (2016), *Simulation and the Monte Carlo Method*, John Wiley & Sons, 2016
- L. SALOMONI (2023), *Risposte nuove ad esigenze vecchie? Alla ricerca degli istituti di semplificazione nel nuovo Codice dei Contratti Pubblici*, in "Economia Pubblica", 2023, n. 2, pp. 233-251
- A. SIMONATI (2013), *La trasparenza amministrativa e il legislatore: un caso di entropia normativa?*, in "Diritto amministrativo", 2013, n. 4, pp. 749-788
- M.R. SPASIANO (2011), *Il principio di buon andamento: dal metagiuridico alla logica del risultato in senso giuridico*, in "Ius publicum network review", vol. 26, 2011, n. 39, pp. 1-34
- J.C. TODOROV (2005), *Laws and the complex control of behavior*, in "Behavior and Social Issues", vol. 14, 2005, n. 2, pp. 86-91
- L. TORCHIA (1997), *La modernizzazione del sistema amministrativo: semplificazione e decentramento*, in "Le regioni", vol. 25, 1997, n. 2-3, pp. 329-348

- R. VIALE (2016), *Razionalità limitata e forme di paternalismo libertario*, in “Sistemi intelligenti”, 2016, n. 1, pp. 181-194
- U. WEISS (2019), *The regressive effect of legal uncertainty*, in “Journal of Dispute Resolution”, 2019, n. 1, pp. 149-186
- Y. WANG (2012), *Uncertain parameter sensitivity in Monte Carlo simulation by sample reassembling*, in “Computers and Geotechnics”, vol. 46, 2012, pp. 39-47
- J.M. WOOLDRIDGE (2016), *Introductory econometrics a modern approach*, Cengage learning, 2016
- I. ZANNI ROSIELLO (2015), *Del linguaggio burocratico*, in “Le carte e la storia”, 2015, n. 2, pp. 11-24



STEFANO TORREGIANI

Gemelli digitali e diritto pubblico: tra questioni ricorrenti e nuove sfide

Il contributo analizza le prospettive e le questioni giuridiche legate alla realizzazione e alla diffusione dei “gemelli digitali” (*Digital Twins*), ossia di quell’agglomerato di tecnologie che consente una riproduzione virtuale “vivente” di oggetti, processi o individui. Il presente lavoro principia dall’approfondimento del profilo definitorio del gemello digitale, al fine di identificarne i tratti salienti e, conseguentemente, di comprendere quali questioni giuridiche (vecchie o nuove) potrebbero emergere a seguito della sua diffusione. Nello specifico, tale tecnologia è destinata ad accentuare le problematiche giuridiche in materia di *data governance*, giacché, da un lato, l’efficienza del gemello digitale richiede accesso e circolazione massiva di informazioni; mentre, dall’altro, rimane necessario garantire il pieno rispetto della normativa applicabile, specie in materia di protezione dei dati (personali e non) e di sicurezza informatica. Il contributo si pone come punto di partenza per avviare una profonda riflessione sul ruolo che può ricoprire il diritto pubblico nell’orientare lo sviluppo di tale tecnologia, secondo un approccio giuridico che, oltre a prevenire abusi e vulnerabilità, guidi la diffusione dei gemelli digitali in una direzione compatibile con i diritti fondamentali e il benessere collettivo, bilanciando protezione e innovazione.

Gemello digitale – Digital Twin – Governance dei dati – Diritto dei dati

Digital twins and public law: recurring issues and new challenges

This paper examines the legal perspectives and challenges related to the development and spread of “Digital Twins,” i.e., the mixture of technologies enabling the creation of a “living” virtual replica of objects, processes, or individuals. This paper begins with an in-depth analysis of the definition of Digital Twins, in order to identify their essential features and, therefore, to understand which legal issues (both recurring and novel) may arise from their implementation. This technology is likely to heighten data governance challenges: on the one hand, the efficiency of Digital Twins lies on broad access to and free flow of information; on the other hand, it is essential to ensure full compliance with applicable regulations, especially in relation to (personal and non-personal) data protection and cybersecurity. This paper is meant as a starting point for a deeper reflection on the purpose of Public Law in the development of this technology, according to a legal approach that not only prevents abuses and vulnerabilities, but also steers the spread of Digital Twins in accordance with fundamental rights and collective well-being, balancing protection and innovation.

Digital Twin – Data Governance – Data Law

L’Autore è assegnista di ricerca presso il Dipartimento di Scienze Giuridiche dell’Università degli Studi di Firenze (SSD_IUS/08)

Questo contributo è presentato nell’ambito del Progetto CRIPTUS – “Centro di Ricerca Interdisciplinare sulle Politiche Tecnologiche Urbane Sostenibili” (CUP: B13C23001280009)

SOMMARIO: 1. Introduzione. – 2. Definizioni ed elementi costitutivi del gemello digitale. – 3. L'unione fa la forza: il gemello digitale come agglomerato di tecnologie. – 4. Gemello digitale e diritto dei dati: tra vecchie e nuove questioni. – 5. Osservazioni conclusive: quali prospettive di regolazione?

1. Introduzione

Il “gemello digitale”, traduzione letterale della originaria versione anglosassone *Digital Twin*, rappresenta uno strumento destinato a rivoluzionare la società nella quale viviamo. La sua concezione affonda le radici negli anni Sessanta e Settanta del secolo scorso, quando, nell'ambito del programma Apollo, la *National Aeronautics and Space Administration* (NASA) iniziò a costruire veicoli identici a quelli mandati nello spazio al fine di assistere gli astronauti e gli ingegneri durante le fasi più delicate della missione¹. Con l'avvento della digitalizzazione, e ancor più della datificazione², l'idea di governare il mondo fisico attraverso una controparte simmetrica virtuale ha ricevuto una spinta propulsiva enorme.

L'utilizzo combinato delle più recenti tecnologie dell'informazione e della comunicazione – fra cui, come si vedrà, *cloud computing*³, *data analytics*⁴,

Intelligenza Artificiale⁵, e *Internet of Things*⁶ – consente infatti di creare una copia “vivente”, di precisione millimetrica, di una persona fisica, di un processo produttivo, di un oggetto o di un insieme di più oggetti, offrendo la possibilità di prendere decisioni migliori, anticipare eventi accidentali e pregiudizievoli, o testare in anticipo eventuali soluzioni migliorative.

Con il progresso delle tecnologie digitali, è progredito di pari passo il fenomeno del gemello digitale. Sono in costante aumento progetti aventi ad oggetto questa tecnologia che oggi trova applicazione, in particolare, nei settori della manifattura, dell'urbanistica, della salute, della tutela dell'ambiente e dell'energia⁷. La sua diffusione su larga scala è destinata a provocare un mutamento di paradigma tanto sociale quanto culturale, poiché diverrà il mezzo su cui si baseranno gran parte delle decisioni politiche, economiche, e finanche personali, riguardanti la nostra esistenza⁸.

1. PALENSKY-CVETKOVIC-GUSAIN-JOSEPH 2022.

2. VAN DIJCK 2014, p. 197 ss.

3. WINKLER-MOSCA 2015, p. 121 ss.

4. ZENO-ZENCOVICH-GIANNONE CODIGLIONE 2016, p. 34.

5. SIMONCINI-SUWEIS 2019, p. 87 ss.

6. MORO VISCONTI 2016, p. 536 ss.

7. SHEN-ARRAÑO-VARGAS-KONSTANTINOU 2023; FULLER-FAN-DAY-BARLOW 2020.

8. Basti in proposito osservare il percorso avviato da qualche anno dall'Unione europea che ha iniziato a promuovere numerosi progetti relativi a gemelli digitali, fra i quali si ricordano: *Destination Earth* (*DestinE*), concernente la creazione di un *Digital Twin* della Terra, lo *European Digital Twin Ocean* (*EU DTO*), per fornire una descrizione multidimensionale e ad alta risoluzione dell'oceano, il gemello digitale della rete elettrica europea, destinato a migliorare l'efficienza e l'intelligenza della rete in modo da rendere più intelligente il sistema energetico nel suo complesso e il *Virtual Human Twin* europeo, capace di riprodurre digitalmente il corpo umano. Sul punto, si veda la Comunicazione della Commissione, *Un'iniziativa*

Come ogni nuovo mezzo tecnologico le cui potenzialità non sono ancora del tutto note, lo sviluppo del *Digital Twin* porta con sé una serie di interrogativi, anche di carattere giuridico, che meritano adeguato approfondimento. Tuttavia, a fronte di simili – dirompenti – prospettive, la ricerca giuridica sul tema stenta ancora a decollare del tutto. Sebbene il gemello digitale sia già da tempo oggetto di studio in ambito scientifico⁹, arrivati a questo punto dello sviluppo pare necessario dedicare maggiore attenzione ai profili di diritto emergenti dalla sua applicazione, specie in un contesto come quello italiano dove stanno trovando sempre più spazio progetti incentrati sulla realizzazione di *Digital Twin*¹⁰.

Tale approfondimento si rivela quantomai necessario in riferimento a uno strumento come quello in esame, dove l'integrazione funzionale di più mezzi tecnologici potrebbe innescare un effetto moltiplicatore del suo impatto, arrivando a un livello di complessità ulteriore e, per certi versi, nuovo rispetto a quanto di regola avviene con le singole tecnologie considerate isolatamente. Appare pertanto opportuno domandarsi quale ruolo può rivestire il diritto nell'orientare un impiego proficuo di tale tecnologia, prevenendo le ricadute negative e predisponendo le migliori condizioni affinché i benefici siano massimizzati.

Fra le diverse prospettive giuridiche da cui può essere analizzato un fenomeno di simile portata, quella costituzionalistica consente di apprezzare più compiutamente la potenziale incidenza dei gemelli digitali sulla nostra esistenza. Essi sono destinati a trasformarsi nella infrastruttura tramite cui verrà esercitato il potere pubblico e privato e che plasmerà la libertà di autodeterminazione dell'individuo di domani. In tale ottica, il presente contributo tenterà di stimolare una riflessione più profonda sul tema, al preciso fine di individuare quali sono le opportunità e quali potrebbero essere

invece gli svantaggi derivanti dall'adozione di un approccio regolatorio¹¹.

I paragrafi che seguono esordiranno con un inquadramento descrittivo del tema, analizzando la terminologia e le principali caratteristiche riguardanti il *Digital Twin*. Successivamente, si passerà all'esame dell'articolazione tecnica di tale strumento, individuando le tecnologie utili a costruire una replica digitale e dinamica di un'entità fisica.

Tale illustrazione preliminare risulta propedeutica alla corretta identificazione di alcune fra le questioni giuridiche di maggiore momento che emergono nel contesto della realizzazione del *Digital Twin*: trattandosi di uno strumento che, in ragione della sua poliedricità, interseca numerosi ambiti normativi, ci si soffermerà nello specifico sulle questioni inerenti al diritto dei dati, in quanto funzionali a trovare una risposta alla domanda di ricerca che guida il presente studio: è necessaria una regolazione settoriale dedicata ai gemelli digitali?

2. Definizioni ed elementi costitutivi del gemello digitale

La comprensione del gemello digitale passa necessariamente dalla preventiva ricerca di una definizione di *Digital Twin* e dei suoi tratti caratterizzanti, specie al fine di distinguerlo da strumenti tecnologici che svolgono funzioni parzialmente simili.

In dottrina, la concettualizzazione del gemello digitale – ma non ancora la coniazione vera e propria del termine – viene generalmente fatta risalire ai primi anni Duemila, quando Michael Grieves introdusse l'idea di un equivalente digitale di un prodotto fisico reale durante il corso sul *Product Lifecycle Management* (PLM) alla *University of Michigan*¹².

Nella teoria di Grieves, il paradigma del *Product Lifecycle Management* consisteva in un approccio che, nell'ambito del processo produttivo manifatturiero, mirava a integrare in maniera

dell'UE sul web 4.0 e i mondi virtuali: muoversi in anticipo verso la prossima transizione tecnologica, doc. COM(2023) 442.

9. SEMERARO-LEZOCHE-PANETTO-DASSISTI 2021.

10. Ad esempio, con riferimento alle smart cities, si vedano i casi dei gemelli digitali urbani dell'Emilia-Romagna (cfr. *Esplorazione dei gemelli digitali: indagine sui casi d'uso in Emilia-Romagna*, Settembre 2024).

11. SIMONCINI 2021, p. 724 ss.

12. GRIEVES 2014.

onnicomprensiva tutte le informazioni relative a un prodotto, allo scopo di gestire in maniera puntuale ogni aspetto del suo ciclo di vita: dalla progettazione, alla realizzazione, dalla distribuzione alla manutenzione¹³.

In origine, Grieves si astiene volontariamente dal fornire una vera e propria definizione di PLM, in quanto ritenuta una operazione eccessivamente limitante per un paradigma ancora in fase di sviluppo embrionale. Egli, per converso, si affida a quelli che definisce *visual models*. Sebbene non fosse ancora comparso il termine *Digital Twin*, tali modelli visuali lasciavano già intravedere chiaramente le caratteristiche principali di quello che viene attualmente definito gemello digitale. Oltre all'idea di creare un *informational equivalent* di un oggetto reale, l'autore sviluppa il paradigma del PLM tramite il riferimento al cosiddetto *Mirrored Spaces Model* (MSM), ossia a un modello costituito dai tre elementi che ancora oggi contraddistinguono essenzialmente il *Digital Twin*: lo spazio reale, lo spazio virtuale e il meccanismo di collegamento tra questi due spazi¹⁴.

Dopo i primi riferimenti comparsi nella dottrina ingegneristica statunitense¹⁵, la locuzione *Digital Twin* è poi salita definitivamente alla ribalta nei primi anni Dieci¹⁶, quando i ricercatori della NASA e della U.S. Air Force si sono riferiti ad essa al fine di sollecitare un cambio di paradigma nello sviluppo della successiva generazione di veicoli aerei delle rispettive agenzie governative¹⁷.

Nel proprio lavoro, i ricercatori descrivono il *Digital Twin* come “an integrated multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin”. Fra i benefici derivanti dallo sviluppo di un simile modello vengono individuati la capacità di

prevedere continuativamente lo stato di salute del veicolo, la sua vita residua, la sua risposta a eventi critici, nonché quella di mitigare i danni o il deterioramento tramite meccanismi di auto-riparazione o modifiche *ad hoc*¹⁸.

Negli anni successivi, Grieves torna sulla nozione di *Digital Twin* e aggiorna la descrizione abbozzata in precedenza. Esso viene definito come “a set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level”¹⁹.

L'autore lo raffigura, dunque, come sistema funzionale a seguire dinamicamente l'intero ciclo di vita del prodotto che rispecchia, incentrando la descrizione sulla parte relativa al costrutto informativo, ma si astiene dal qualificarlo come vera e propria tecnologia a sé stante²⁰. In quest'ottica, la realizzazione del gemello prende avvio dalla fase di progettazione, quando il bene fisico non esiste ancora e viene plasmato sulla base di quello realizzato nello spazio virtuale, passa per le fasi di produzione e di operatività, caratterizzate dal costante flusso di dati tra i due versanti materiale e digitale, e arriva alla fase finale, quella di smaltimento, ove al sistema fisico sopravvive quello virtuale. In tal modo, la conoscenza esperienziale maturata durante il periodo di attività può anche essere utilizzata per perfezionare la messa a punto di nuovi prodotti, nonché di futuri gemelli digitali²¹.

In seguito, la dottrina, specie nei diversi ambiti della *hard science*, si è prodigata nello studio del *Digital Twin* arrivando a partorire una molteplicità di definizioni con l'intento di perimetrare semanticamente un fenomeno ontologicamente poliedrico. Si tratta di costrutti imperniati su un nucleo comune – costituito dalla riproduzione digitale di un oggetto fisico – ma al contempo caratterizzati

13. GRIEVES 2005, p. 71 ss.

14. *Ivi*.

15. TUEGEL-INGRAFFEA-EASON-SPOTTSWOOD 2011.

16. BARRICELLI-CASIRAGHI-FOGLI 2019, p. 167655.

17. GLAESSGEN-STARGEL 2013.

18. *Ivi*, pp. 7-8.

19. GRIEVES-VICKERS 2017, p. 85 ss.

20. ZHENG-YANG-CHENG 2019, p. 1141 ss.

21. GRIEVES-VICKERS 2017, p. 85 ss.

da lievi differenze spesso dipendenti dal diverso contesto di applicazione settoriale²².

In particolare, la definizione tende a cambiare a seconda dell'aspetto cui l'autore attribuisce maggiore rilevanza: alcuni fanno riferimento al concetto di rappresentazione virtuale del prodotto reale, intesa come controparte fisica capace di replicarne l'intero ciclo di vita²³, altri richiamano l'idea di un "modello vivente" che si adatta continuamente ai cambiamenti prodotti nello spazio fisico utilizzando dati sensoriali in tempo reale²⁴.

La descrizione che forse più di altre riesce a sintetizzare aspetti cardine e funzioni salienti del *Digital Twin*, e che consente di avere maggiore contezza dell'impatto travolgente che questo strumento potrebbe avere rispetto alle singole tecnologie che potrebbero comporlo, è quella fornita da Barricelli, Casiraghi e Fogli, secondo cui: "DTs can be defined as (physical and/or virtual) machines or computer-based models that are simulating, emulating, mirroring, or 'twinning' the life of a physical entity, which may be an object, a process, a human, or a human-related feature. Each DT is linked to its physical twin through a unique key [...], identifying the physical twin, and therefore allowing to establish a bijective relationship between the DT and its twin. A DT is more than a simple model or simulation [...]. A DT is a living, intelligent and evolving model, being the virtual counterpart of a physical entity or process. It follows the lifecycle of its physical twin to monitor, control, and optimize its processes and functions. It continuously predicts future statuses (e.g., defects, damages, failures), and allows simulating and testing novel configurations, in order to preventively apply maintenance operations. More specifically, the

twinning process is allowed by the continuous interaction, communication, and synchronization (closed-loop optimization) between the DT, its physical twin and the external, surrounding environment"²⁵.

Spostandosi dal piano dottrinale a quello istituzionale, più precisamente, quello europeo, una prima definizione di gemello digitale è stata fornita dalla Commissione europea all'inizio del 2020, nella comunicazione *Una strategia europea per i dati*²⁶, uno dei documenti cardine dell'attuale stagione politica avviata dall'Unione nell'ambito dell'economia dei dati²⁷.

Nella parte introduttiva della comunicazione, incentrata sull'enorme rilievo che hanno assunto i dati per lo sviluppo economico del continente, la Commissione dedica un riferimento anche al ruolo che siffatti dati svolgeranno per la diffusione dei gemelli digitali, specie nell'industria manifatturiera. In tale passaggio, viene affermato che essi "creano una copia virtuale di un prodotto, processo o sistema fisico che può ad esempio prevedere, sulla base dell'analisi dei dati, quando un'apparecchiatura avrà un guasto, consentendo di incrementare la produttività mediante una manutenzione predittiva"²⁸.

Ciò che emerge chiaramente dall'analisi della dottrina in materia è che il minimo comun denominatore che sottende qualsiasi tipologia di gemello digitale, indipendentemente dallo specifico settore di applicazione, risiede nel concetto di copia, replica, rappresentazione di carattere virtuale e legata da una stretta interconnessione con la controparte fisica che rispecchia.

Pertanto, le caratteristiche essenziali del fenomeno in parola possono ancora oggi riassumersi

22. SEMERARO-LEZOCHE-PANETTO-DASSISTI 2021.

23. SCHROEDER-STEINMETZ-PEREIRA-ESPINDOLA 2016, p. 12 ss.

24. LIU-MEYENDORF-MRAD 2018.

25. BARRICELLI-CASIRAGHI-FOGLI 2019, p. 167656.

26. Comunicazione della Commissione, *Una strategia europea per i dati*, doc. COM(2020) 66.

27. Proprio con tale comunicazione sono infatti stati concepiti quei provvedimenti normativi che sarebbero poi diventati il 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 (noto come Data Governance Act) e 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 (noto come Data Act).

28. Comunicazione della Commissione, *Una strategia europea per i dati*, cit., p. 3.

con quelle individuate da Grieves in riferimento al PLM: a) lo spazio reale contenente l'oggetto (o il processo) fisico; b) lo spazio virtuale dove viene replicato quanto presente nello spazio fisico; c) la connessione bidirezionale tra i due spazi²⁹.

Tale architettura qualifica univocamente il gemello digitale, ponendolo su un piano maggiormente innovativo rispetto ad altre metodologie sviluppate in passato, da considerarsi sue antesignane.

Il *Digital Twin* si pone infatti al culmine di un percorso evolutivo iniziato con lo sviluppo di altri ambiti di ricerca. Fra essi si ricordano, il *Virtual Manufacturing systems*, in cui viene riprodotta virtualmente una entità fisica, ma senza stabilire una connessione tra spazio fisico e spazio virtuale; il *Model-based Predictive control* in cui viene realizzato un sistema virtuale al preciso scopo di predire il comportamento di un sistema reale, ma senza quella perfetta sincronia reale-virtuale che contraddistingue il *Digital Twin*; il *Building Information Modelling* (BIM), in cui la costruzione di un modello digitale finalizzato a gestire e monitorare l'operatività di un bene fisico non viene compiuta ricorrendo ai dati prodotti in tempo reale³⁰.

Pertanto, il gemello digitale non deve essere confuso né con la semplice ricostruzione in versione digitale di una entità fisica esistente senza che ci sia alcuno scambio di dati tra entità reale e entità virtuale (nota come *Digital Model*), né soprattutto – e qui la distinzione appare più labile – con la cosiddetta *Digital Shadow*, in cui il flusso di dati rimane unidirezionale, dall'oggetto fisico verso quello virtuale, sicché qualsiasi alterazione dell'entità reale

produce un corrispondente cambiamento in quella digitale, ma non viceversa³¹.

Il gemello digitale – quantomeno come inteso nell'ambito del presente contributo – è uno strumento che, attraverso un complesso meccanismo di sensori e di attuatori, garantisce una costante comunicazione tra la dimensione reale e la dimensione virtuale, le quali vivono in una simbiosi biunivoca e interdipendente. In altri termini, come è stato osservato, “[t]ali gemelli digitali sono, dunque, molto più di una replica digitale di sistemi fisici, persone e ambienti. Essi vanno tenuti distinti da altri approcci di analisi e visualizzazione dei dati, proprio perché sono in grado di integrare dati provenienti da varie fonti in tempo reale e di valutare scenari futuri attraverso simulazioni avanzate”³².

Tale peculiarità rende unica, anche dal punto di vista giuridico, una tecnologia di questo tipo, laddove gli accadimenti del mondo fisico vengono dettati, direttamente o indirettamente, da eventi, scelte o azioni che avvengono nel mondo virtuale.

In questa prospettiva, stanti le ricadute che possono derivare dall'adozione dell'una o dell'altra delle alternative prospettate in dottrina, risulta dirimente giungere a una definizione giuridica chiara e univoca di gemello digitale³³: la qualificazione del *Digital Twin* incide infatti sulla delimitazione dell'oggetto tecnologico cui l'ordinamento deve riferirsi, sia per tutelare gli individui, che per orientarne il corretto sviluppo.

Una definizione incardinata sul rapporto biunivoco tra spazio reale e spazio virtuale – ove il gemello digitale viene tratteggiato come infrastruttura capace di incidere direttamente su beni

29. È bene segnalare che successivamente alle prime concettualizzazioni di Grieves, la dottrina è arrivata a individuare anche ulteriori dimensioni del gemello digitale. Si veda, in particolare, TAO-ZHANG-LIU-NEE 2018, pp. 169-172, dove all'architettura proposta da Grieves vengono aggiunte le dimensioni del *Services model* e del *Data Model*.

30. SEMERARO-LEZOCHE-PANETTO-DASSISTI 2021, p. 11. La distinzione tra *Digital Twin* e *Building Information Modelling* (BIM) assume particolare rilevanza nell'odierno contesto italiano, alla luce della recente entrata in vigore del Decreto legislativo 31 marzo 2023, n. 36 (cd. Codice dei contratti pubblici) che all'art. 43 prescrive l'obbligo, a decorrere dal 1° gennaio 2025, nell'ambito delle procedure pubbliche di affidamento di contratti, di adottare il modello BIM per la progettazione e la realizzazione di opere di nuova costruzione e per gli interventi su costruzioni esistenti per importo a base di gara superiore a 1 milione di euro. Per un approfondimento sulle implicazioni giuridiche derivanti dall'utilizzo di tale strumento si rinvia a COSTANZI 2020.

31. FULLER-FAN-DAY-BARLOW 2020, p. 108952 ss.

32. SPEZIALE-BASUNTI 2024, p. 582.

33. SUFFIA 2023, p. 122 ss.

giuridici di rango primario – non può che porre questioni profondamente diverse rispetto a una concezione normativa in cui esso viene inquadrato come modello puramente descrittivo con effetti operativi inevitabilmente più contenuti. La perimetrazione normativa del concetto di gemello digitale rappresenta pertanto una operazione tanto delicata quanto decisiva, dalla quale dipenderà la misura e l'estensione dell'intervento regolatorio necessario ad assicurare che il suo sviluppo avvenga nel pieno rispetto dei diritti fondamentali.

3. L'unione fa la forza: il gemello digitale come agglomerato di tecnologie

Dal punto di vista prettamente tecnico, il gemello digitale può essere sinteticamente descritto come un algoritmo in grado di replicare integralmente nel mondo digitale un oggetto o un processo reale³⁴.

Tuttavia, scendendo nel dettaglio, con il termine gemello digitale non si indica di norma una unica e specifica tecnologia. La rappresentazione virtuale di una entità fisica esistente viene infatti ottenuta tramite l'integrazione di più strumenti che, mettendo a fattor comune le proprie funzionalità individuali, riescono a dare vita al *Digital Twin*³⁵.

Sebbene non possa essere individuato *a priori* un insieme di mezzi la cui combinazione è da considerarsi essenziale per la realizzazione del gemello digitale, la prima delle cosiddette *enabling technologies* non può che essere quella che garantisce l'interconnessione tra il mondo reale e il mondo virtuale: l'*Internet of Things* (IoT)³⁶.

Si tratta di una tecnologia basata su una infrastruttura, materiale e immateriale, che consente il trasporto, l'archiviazione, l'elaborazione e l'accesso

ai dati generati (direttamente o tramite l'utilizzo degli utenti) da *smart devices* equipaggiati con sensori e attuatori tra loro collegati tramite un *network*³⁷.

Tale tecnologia ricopre una posizione chiave, per alcuni primaria³⁸, nell'organigramma del gemello digitale. L'IoT consente la raccolta in tempo reale di quei dati provenienti dall'ambiente fisico che risultano essenziali per la realizzazione di una replica virtuale fedele alla realtà e in costante aggiornamento. Per un verso, i sensori intelligenti acquisiscono dati relativi alle caratteristiche dell'oggetto fisico, al suo funzionamento, a eventuali anomalie e alle interazioni con l'ambiente circostante, al fine di procedere alla mappatura (dinamica) dello spazio reale. Per l'altro, proprio grazie ai *feedback* provenienti dallo spazio virtuale, gli attuatori consentiranno al corrispondente oggetto fisico di "reagire" tempestivamente secondo le istruzioni impartite, ad esempio prevenendo un guasto o modificando il processo di funzionamento³⁹.

L'IoT mette dunque a disposizione del gemello digitale dati altamente dettagliati e variegati, sulla cui base la realtà viene poi "ricostruita" nel mondo virtuale⁴⁰.

Le caratteristiche dei dati così raccolti, definiti *big in nature* in ragione della loro mole ed eterogeneità⁴¹, consentono di individuare una ulteriore tecnologia da integrare nell'ingranaggio del *Digital Twin*: i *big data*.

I dati vengono considerati *big* quando riescono a cumulare le tre caratteristiche – le cosiddette tre "v" – relative al *volume*, ossia alla quantità ingente di informazioni a disposizione, alla *variety*, in quanto di contenuto, provenienza e formato diversificati, e alla *velocity*, riferita alla grande velocità con cui le informazioni vengono prodotte e a cui dovrebbero

34. RATHORE-SHAH-SHUKLA et al. 2021, p. 32030.

35. *Ivi*, p. 32044.

36. Nel presente contributo, il riferimento comprende anche quello che parte della dottrina tecnica definisce come *Industrial Internet of Things* (IIoT), inteso quale applicazione del tradizionale IoT al processo manifatturiero e industriale. Per un approfondimento, si veda: BOYES-HALLAQ-CUNNINGHAM-WATSON 2018.

37. DORSEMAINE-GAULIER-WARY et al. 2015, p. 72 ss.

38. ATTARAN-CELIK 2023, p. 2.

39. ZHENG-YANG-CHENG 2019, p. 1141 ss.

40. KAUR-MISHRA-MAHESHWARI 2020, p. 3 ss.

41. RATHORE-SHAH-SHUKLA et al. 2021, p. 32039.

essere analizzate⁴². A queste, la dottrina ha aggiunto nel tempo altri aspetti, fra cui, la *veracity*, ossia la (non sempre ottimale) qualità e affidabilità delle informazioni e, infine, il *value*, che indica l'elevato valore che può essere estratto dalle stesse⁴³.

Quando si parla di *big data*, non ci si riferisce solamente ai dati che posseggono le caratteristiche (“v”) anzidette, ma anche alla strumentazione dotata della capacità di analizzare, in un tempo tollerabile, i dati in questione e di estrarne valore tramite l'individuazione di correlazioni e *pattern* nascosti⁴⁴. Capacità di cui sono invece sprovvisti i tradizionali strumenti informatici⁴⁵.

In tale ottica assume rilievo anche la *data analytics*, o meglio, alla luce di quanto appena esposto, la *big data analytics*, in quanto consente di trasformare la moltitudine di dati raccolti in informazioni di valore. Nello specifico, l'estrazione della “conoscenza” insita nei dati avviene attraverso un processo composto da operazioni di *data management* atte a gestire la raccolta di dati grezzi, la loro memorizzazione e la preparazione per lo svolgimento delle successive operazioni di *data analytics* vera e propria, nel contesto delle quali, attraverso l'impiego di appositi algoritmi, vengono estrapolate le informazioni essenziali per l'operatività del *Digital Twin*⁴⁶.

Per tale ragione, la necessità di replicare accuratamente lo spazio reale, specie in contesti in cui il *Digital Twin* rispecchia ambienti ampi e complessi, attribuisce una importanza capitale alla tecnologia *big data*, senza la quale il gemello sarebbe uno strumento inefficiente⁴⁷.

Peraltro, il volume, la varietà e la velocità di questi dati richiedono una piattaforma che possa fungere da adeguato supporto all'imponente flusso di informazioni raccolte e trattate. Tale esigenza può essere soddisfatta dal *cloud computing*⁴⁸.

Tale tecnologia abilitante garantisce accesso dinamico a un insieme di risorse costituite da network, server e applicazioni, sulla base di un modello condiviso e scalabile⁴⁹. Le sue peculiarità risultano particolarmente preziose per il *Digital Twin* dal momento che corredano il sistema della adeguata capacità di elaborazione e di archiviazione dei grandi volumi di dati, garantendo al contempo tempi di analisi ridotti e facoltà di accesso ubiqua⁵⁰.

Infine, fra le tecnologie che possono equipaggiare il gemello digitale non può di certo essere omessa quella che, attualmente, sta suscitando maggiore attenzione: l'Intelligenza Artificiale. È di per sé evidente il valore aggiunto che può derivare dall'apporto di “un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che [...] deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali”⁵¹.

L'impiego dell'Intelligenza Artificiale (IA), comprensiva di tutti i suoi sottoinsiemi come il Machine-Learning e il Deep Learning, può incrementare le potenzialità del gemello digitale rendendolo, per l'appunto, “intelligente” e dunque capace di analizzare i dati al fine, fra l'altro, di ottimizzare i processi decisionali, di fornire previsioni sul funzionamento del prodotto, nonché

42. BUZZACCHI 2016, p. 69 ss.

43. CALZOLAIO 2017, p. 599.

44. QI-TAO 2018, p. 3586.

45. AGCM, AGCOM, Garante per la protezione dei dati personali, *Indagine conoscitiva sui big data*, 2018, spec. pp. 7-8.

46. GANDOMI-HAIDER 2015, p. 137 ss.

47. QI-TAO 2018, p. 3591.

48. RATHORE-SHAH-SHUKLA et al. 2021, p. 32039.

49. BONCINELLI 2021, p. 29 ss.

50. ATTARAN-CELIK 2023, p. 2.

51. Questa la definizione normativa individuata dall'art. 3, p.to 1) del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008 (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

di valutare anticipatamente l'impatto derivante dall'implementazione di eventuali modifiche⁵².

Inoltre, l'integrazione dell'IA consente di combinare in modo ottimale i dati raccolti dallo spazio reale per colmare le lacune che, invece, spesso pregiudicano l'affidabilità dei sistemi di simulazione tradizionali: quella parte di informazioni che non può essere rilevata direttamente dalla strumentazione ICT viene, in un certo senso, "dedotta" dal *Digital Twin* dotato di intelligenza artificiale. Quindi, il valore aggiunto che contraddistingue il gemello digitale rispetto agli altri strumenti di simulazione già sperimentati risiede proprio nella capacità di compensare eventuali lacune nella rappresentazione virtuale attraverso una avanzata combinazione delle informazioni a disposizione⁵³.

In ogni caso, analogamente a quanto osservato con riferimento al profilo definitorio, anche la dimensione tecnologica del gemello digitale non è neutra sul piano giuridico. La combinazione delle tecnologie impiegate, pur non esaurendo le possibili modalità di realizzazione del sistema⁵⁴, assume rilievo giuridico in quanto, potendo ciascuna componente essere sussunta al di sotto di un differente regime normativo, l'assetto tecnico del gemello digitale finisce per incidere, in modo non trascurabile, sul perimetro delle tutele e degli istituti applicabili.

4. Gemello digitale e diritto dei dati: tra vecchie e nuove questioni

Il gemello digitale, termine metaforico sintatticamente imperniato su una dimensione virtuale diversa dalla realtà, sembra porsi su una direttrice opposta rispetto ad altri strumenti oggi maggiormente diffusi o attenzionati, come i social network o la realtà virtuale. Se questi ultimi sono programmati per spingerci continuamente in un mondo diverso da quello materiale, dove la percezione

fisica scolora giorno dopo giorno, con effetti tutt'altro che positivi⁵⁵, il *Digital Twin* sembra voler invertire questo esodo, della propria personalità individuale e del proprio ecosistema relazionale, verso lo spazio virtuale: il gemello digitale non promuove una migrazione verso la virtualità, ma mira a sfruttare lo spazio digitale per apportare benefici all'ambiente fisico, migliorando la qualità della vita dei consociati e (ri)attribuendo valore al mondo reale. Si tratta di uno strumento al servizio della realtà e non di una via di fuga da essa.

In questo senso, il *Digital Twin*, rappresentando la *practical innovation* per eccellenza, è capace di alterare significativamente il modo in cui le persone pensano e interagiscono⁵⁶.

Pertanto, se è vero che ai grandi benefici connessi all'utilizzo di nuove tecnologie fanno da contraltare le potenziali ripercussioni negative derivanti da un impiego illecito o incontrollato delle medesime, tale evidenza vale *a fortiori* per il caso del gemello digitale, in cui le problematiche giuridiche attinenti a ciascuna delle singole tecnologie abilitanti non solo si assommano, ma, integrandosi, rischiano di moltiplicarsi, giungendo a un livello di complessità nuovo.

La sua natura poli-tecnologica e, soprattutto, la sua capacità di modellare "in tempo reale" il mondo fisico rievocano questioni già note al diritto delle tecnologie, ponendole tuttavia in una prospettiva per certi versi inedita. Ciò rende immediatamente evidente l'importanza che può ricoprire il diritto nell'orientare il corretto impiego di tale strumento⁵⁷.

In tale ottica, appare necessario riconoscere preliminarmente quali questioni giuridiche possono emergere nel contesto della realizzazione e della operatività del gemello digitale. Tale operazione risulta utile a stabilire un punto di partenza da cui muovere per impostare una riflessione

52. SHEN-ARRAÑO-VARGAS-KONSTANTINO 2023.

53. GARSKE-HOLZ-EKARDT 2024.

54. Non esistendo allo stato attuale un gruppo predefinito di tecnologie la cui presenza è da considerarsi necessaria, quelle menzionate nel presente paragrafo non costituiscono un elenco minimo, né tantomeno esaustivo, di strumenti tecnologici necessari alla realizzazione del *Digital Twin*; si veda, ad esempio, ATTARAN-CELIK 2023, dove fra le *Digital twin technologies* viene inclusa anche la *Extended Reality*.

55. CALZOLAIO 2023-A, p. 281 e ss.; CALZOLAIO 2023-B, p. 291 ss.

56. SIMONCINI-LONGO 2021, p. 27 ss.

57. ZOLTICK-MAISEL 2023, p. 1167 ss.

più profonda in merito all'adeguatezza del quadro normativo vigente rispetto all'obiettivo di valorizzare i benefici del gemello digitale senza sacrificare illegittimamente i diritti e gli interessi dei singoli e della collettività⁵⁸.

Fra la moltitudine di problematiche che meritano l'attenzione del giurista⁵⁹, il presente studio si focalizza su quelle strettamente legate alla materia prima senza la quale il *Digital Twin* non potrebbe esistere: i dati⁶⁰.

Un percorso argomentativo improntato a una logica consequenziale impone di illustrare per prima la tematica della *data governance*, la quale, grazie al suo carattere onnicomprensivo, è in grado di inglobare ognuna delle varie dimensioni concernenti la gestione e il trattamento dei dati⁶¹.

Il gemello digitale è tanto più efficiente quanto più ottimale è la governance dei dati che lo alimentano⁶². Esso presuppone pertanto un insieme di policies, procedimenti, misure tecniche e organizzative che, da un lato, consentano di sfruttare al meglio il patrimonio informativo a disposizione⁶³, mentre dall'altro, garantiscano la conformità alle normative rilevanti in materia di diritto dei dati⁶⁴.

In altri termini, la governance dei dati del gemello digitale è chiamata a trovare un difficile equilibrio tra esigenze e interessi che spesso si trovano in contrapposizione. Frequentemente, alla necessità – dettata dal livello di dettaglio e di aggiornamento del gemello – di avere a disposizione la più elevata quantità possibile di dati e di farli circolare rapidamente si contrappone l'obbligo normativo di tutelare determinati tipi di informazioni, perché

di carattere personale o perché sottoposte a un regime di protezione specifico che ne impedisce, o comunque ne limita, l'accesso⁶⁵.

Per tale ragione, la data governance si intreccia, innanzitutto, con gli aspetti relativi alla protezione dei dati personali. La qualifica di diritto fondamentale all'interno del tessuto ordinamentale europeo rende la *personal data protection* una questione particolarmente delicata e meritevole di considerazione⁶⁶.

Basti in tal caso fare riferimento alle ipotesi di *Individual Digital Twin* in cui viene creata una replica virtuale della persona fisica attraverso la raccolta e l'elaborazione di tutte le informazioni di carattere personale che la riguardano. Sebbene tale evenienza abbia incommensurabili risvolti benefici per l'interessato, specialmente di natura medica, è evidente come la creazione di una copia virtuale in tutto e per tutto coincidente con un essere umano vivente e, addirittura, in grado di anticiparne il comportamento, pone serie preoccupazioni in punto di diritto alla autodeterminazione – non solo informativa – dell'individuo e di diritto all'identità personale⁶⁷. Come è stato acutamente osservato “The digital twin causes a ‘derealization’ of human experiences. The digitization and pixelization of the person disrupts our traditional conception of the person, which is no longer defined by his or her civil status but by the correlation of his or her data. So where does the virtual begin and where does the person stop?”⁶⁸.

Sebbene l'ipotesi di *Digital Twin* individuale lasci emergere maggiori preoccupazioni, ciò non

58. TELLER 2021.

59. Esistono infatti altre dimensioni giuridiche rilevanti con riguardo al gemello digitale, non riferite al diritto dei dati, come, ad esempio, quella relativa alle questioni di proprietà intellettuale o alla responsabilità giuridica di chi progetta, realizza e utilizza questa tecnologia, senza dimenticare quelle relative alla applicazione della normativa in materia di intelligenza artificiale. Per una breve elencazione delle problematiche giuridiche si veda, BUNDIN–MARTYNOV–SHIREEVA 2022, p. 77 ss.

60. DELLA MORTE 2018, p. 135.

61. TORREGIANI 2024, pp. 240-241.

62. GARSKE–HOLZ–EKARDT 2024.

63. IANNUZZI 2021, p. 39.

64. Per un approfondimento sul tema, si rinvia a STREINZ 2021, p. 902 ss.

65. GARSKE–HOLZ–EKARDT 2024.

66. ALLEGRI 2018, pp. 75-80; POLLICINO–BASSINI 2017, p. 132 ss.; ADAM 2000, p. 881 ss.

67. IANNUZZI 2024-B, p. 35 ss.

68. TELLER 2021, p. 5.

significa che il trattamento delle informazioni di carattere personale effettuato nell'ambito di altre tipologie di gemello digitale (non focalizzate sul singolo essere umano) desti minori problemi. I sistemi di IoT incorporati nel gemello ricorrono a dispositivi dotati di sensori capaci di raccogliere un'enorme quantità di informazioni di carattere sensibile e dettagliato sulle persone (localizzazioni, immagini, colloqui, parametri fisici), conducendo a un aumento esponenziale della quantità, nonché della qualità, dei dati relativi a ognuno di noi⁶⁹.

In tal senso, anche i "Gemelli Digitali Urbani", ossia quelli volti a replicare dinamicamente una intera città, non possono prescindere dalla raccolta di miriadi di dati personali dei cittadini e degli utenti che compongono il tessuto sociale e fruiscono dei servizi pubblici: la costante osservazione dei processi dinamici che interessano la città implica un trattamento su larga scala di dati, da un lato, direttamente personali e, dall'altro, di carattere non personale ma che, attraverso l'analisi incrociata, possono consentire di ricavare informazioni riguardanti persone fisiche identificabili⁷⁰. Il trattamento di tali informazioni deve obbligatoriamente essere condotto nel più rigoroso rispetto della normativa europea e nazionale in materia affinché i Gemelli Digitali Urbani siano impiegati per la creazione di smart cities efficienti e non per attuare forme di sorveglianza non democratica o per lo sfruttamento a fini commerciali⁷¹.

Tuttavia, la immanente complessità del *Digital Twin* rende il raggiungimento dell'anzidetta conformità normativa un traguardo tutt'altro che semplice: le soluzioni che si sono rivelate adeguate per le singole tecnologie isolatamente considerate, potrebbero non risultare adatte a garantire la

conformità normativa in un contesto integrato e complesso come il *Digital Twin*⁷².

Un'altra questione inerente al profilo relativo alla protezione, invero, non solo dei dati, ma anche delle reti e del sistema nel suo complesso, riguarda la cybersicurezza del gemello digitale. Le grandi capacità e potenzialità che connotano il *Digital Twin* lo espongono a un significativo "rischio digitale"⁷³. La maggiore distribuzione e la conseguente "dispersione" dello strumentario che lo compone, unite alla sua elevata interconnessione, portano inevitabilmente a un incremento della vulnerabilità del sistema⁷⁴.

Oltretutto, man mano che i *Digital Twin* otterranno maggiore impiego e diffusione, è destinato ad aumentare anche l'interesse di coloro che vorrebbero utilizzarlo per finalità malevole e destabilizzanti: se solo si pensa agli effetti causati dalla manipolazione dei *new media* digitali⁷⁵, risulta preoccupante pensare a quali conseguenze devastanti potrebbero derivare dal deprecabile accesso non autorizzato al flusso di dati che alimentano il gemello digitale.

In questo senso, dalla grande potenza del gemello digitale discende, in un certo qual modo, anche la sua più grande fragilità: la concatenazione e la profonda integrazione dei suoi elementi costituenti fanno sì che la vulnerabilità di una singola parte possa ripercuotersi sull'intero sistema, compromettendone la sicurezza e la funzionalità⁷⁶.

Pertanto, per disinnescare tali rischi e assicurare altresì la compliance normativa anche in materia di cybersecurity⁷⁷, appare indispensabile equipaggiare il *Digital Twin* con misure tecniche e organizzative idonee – come, ad esempio, algoritmi di crittografia adeguati, sistemi di archiviazione sicura dei dati, gestione e supervisione degli accessi – tenendo sempre in debita considerazione le debolezze (nell'epoca attuale ancora ineliminabili) connaturate al sistema⁷⁸.

69. ATLAM–WILLS 2020, p. 123 ss.

70. Sia consentito in proposito rinviare a TORREGIANI 2020, p. 317 ss.

71. PAGNANELLI 2023, p. 188 ss.

72. ATLAM–ALENEZI–WALTERS–WILLS 2017, p. 254 ss.

73. LONGO, 2024-A, p. 53 ss.

74. KAUR–MISHRA–MAHESHWARI 2020, pp. 12-13.

75. COSSIRI 2023, p. 77 ss.

76. ATLAM–WILLS 2020, p. 123 ss.

77. LONGO 2024-B.

78. Eloquenti in tal senso, ATLAM–WILLS 2020, nella parte in cui sottolineano che "most IoT devices have limited processing and storage capabilities, due to small and lightweight features which make them run on lower energy."

Gli aspetti relativi alla protezione e alla sicurezza fin qui illustrati si trovano spesso in tensione con altre questioni giuridiche rilevanti per il gemello digitale. Si tratta di profili pur sempre riconducibili all'ambito della data governance, ma che non si riferiscono *stricto sensu* alla salvaguardia dei dati o dell'infrastruttura del *Digital Twin*. Essi riguardano piuttosto quei fattori che ne condizionano l'efficacia, l'efficienza e la diffusione su larga scala.

Come più volte ribadito, l'operatività del gemello digitale si basa essenzialmente sui dati, i quali devono fluire in maniera costante e in misura massiva da una vasta gamma di fonti interconnesse al medesimo *network*. Detto altrimenti, tale tecnologia dipende fortemente dalla circolazione delle informazioni: la rappresentazione dinamica e in costante aggiornamento dell'asset fisico, la *big data analytics*, l'addestramento dei sistemi di intelligenza artificiale, e ogni altra funzione latamente correlabile ai gemelli digitali, non sarebbero attuabili senza un adeguato flusso di dati in entrata e in uscita dal sistema⁷⁹.

Senza dimenticare che, al fine di migliorare le capacità predittive, il *Digital Twin* si nutre non solo dei dati *real-time* raccolti dai dispositivi e dai sensori, ma anche dei dati *offline* di carattere storico,

relativi, ad esempio, alle precedenti operazioni di manutenzione o al consumo energetico. Queste informazioni possono non fare parte del *network* di riferimento, ma trovarsi in database altrui.

Al riguardo, è bene notare che buona parte dei dati necessari alla realizzazione dei gemelli digitali esistono già e non richiedono una ulteriore raccolta⁸⁰. Si pensi allo "Spazio europeo dei dati sanitari" (*European Health Data Space*) per i gemelli digitali individuali in materia sanitaria⁸¹, alla Infrastruttura per l'informazione territoriale nella Comunità europea (Inspire) per la condivisione in ambito europeo delle informazioni territoriali e ambientali per gli *Urban Digital Twins*⁸², oppure ai dati raccolti e prodotti da altri gemelli digitali o altri mezzi ICTs: queste banche dati racchiudono tutte informazioni che possono incrementare notevolmente le capacità e il successo di questa tecnologia.

Il fatto che molti dei dati presenti in tali raccolte, detenute da enti pubblici o da soggetti privati, non siano liberamente disponibili induce a interrogarsi anche in merito al tema dell'accessibilità alle informazioni funzionali alla creazione del *Digital Twin*⁸³. Sebbene le recenti riforme del diritto dei dati europeo abbiano segnato importanti passi in avanti in questo ambito⁸⁴, nel caso di un sistema

Therefore, sophisticated security algorithms are not suitable for these constrained devices as they are not able to execute complex processing operations in real time. Instead, constrained devices typically only employ fast, lightweight encryption algorithms", così a p. 136.

79. Comunicazione della Commissione, *Verso una florida economia basata sui dati*, doc. COM(2014) 442, spec. pp. 12-13, ove la Commissione ha evidenziato che i requisiti in materia di ubicazione dei dati ostacolano la libera circolazione delle informazioni e producono un effetto frenante nei confronti dello sviluppo del *cloud computing* e dei *big data*.

80. Garske-Holz-Ekardt 2024, pp. 9-11.

81. Il riferimento è al 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, con cui l'Unione europea istituisce lo spazio europeo dei dati sanitari (*European Health Data Space* – EHDS) prevedendo 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.

82. Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (Inspire). Si tratta di una infrastruttura utile a raggiungere gli scopi delle politiche ambientali europee e delle politiche o delle attività che possono avere ripercussioni sull'ambiente.

83. Emergono in tali ipotesi le questioni sempre attuali relative alla sussistenza di un eventuale diritto di proprietà dei dati. Sul punto, si vedano DREXL 2016-A; DREXL 2016-B; WIEBE 2016; ZECH 2016.

84. Ci si riferisce, in particolare, 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 (Data Governance Act) e al Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023,

come il gemello digitale – la cui accuratezza cresce al crescere della mole di dati utilizzati – tale questione deve essere esaminata in una prospettiva differente, anche valutando l'opportunità di introdurre obblighi di messa a disposizione o diritti di accesso alle informazioni necessarie.

Peraltro, risultano legate all'incentivazione della circolazione anche le problematiche legate alla scarsa interoperabilità dei dati e dei sistemi a supporto del gemello digitale.

Con "interoperabilità" si indica, generalmente, la capacità di un sistema, prodotto o servizio di comunicare e funzionare con altri sistemi, prodotti o servizi tecnicamente diversi, nonché, con particolare riferimento al mondo dell'informazione digitale, alla capacità di trasferire e mettere a disposizione i dati attraverso differenti sistemi e applicazioni⁸⁵. È evidente che per una tecnologia caratterizzata dalla eterogeneità delle fonti di alimentazione e degli strumenti – cui solitamente è connessa anche una pluralità di fornitori delle singole componenti tecnologiche – quello dell'interoperabilità costituisce un tema centrale, o addirittura, secondo alcuni il "digital twins' biggest issue"⁸⁶.

Effettivamente, la propagazione del fenomeno dei gemelli digitali dipende fortemente dalla interoperabilità dei sistemi. Per tale ragione, da più

parti viene richiesta la creazione di un quadro di standard condivisi che funga da base tecnico-normativa solida per lo sviluppo di sistemi capaci di comunicare vicendevolmente⁸⁷. Infatti, malgrado i primi importanti progetti di *digital twinning* in ambito pubblico comincino a trovare applicazione anche in territorio continentale, non si è ancora giunti a un insieme di norme comuni e, soprattutto, intersettoriali, in grado di rendere meno farraginoso il flusso dei dati tra i diversi attori coinvolti nella catena di trattamento delle informazioni⁸⁸.

In conclusione, la corretta identificazione delle questioni giuridiche di maggiore rilievo appare fondamentale per comprendere fino in fondo quanto il *data law* europeo sia funzionale alla realizzazione di gemelli digitali "constitutionally oriented". Difatti, sebbene nell'attuale panorama unionale non esistano provvedimenti normativi aventi come oggetto specifico ed esclusivo della propria regolazione il gemello digitale⁸⁹, è indubbio che la aggrovigliata trama ordinamentale correntemente in vigore influenza già pesantemente lo sviluppo e la diffusione del *Digital Twin*⁹⁰: ognuna delle singole tecnologie che compongono il gemello digitale, nonché la tipologia di dati che vengono trasmessi per il loro tramite, potrebbe infatti rientrare nell'ambito di applicazione di uno fra gli svariati regolamenti e direttive europei oggi vigenti⁹¹.

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 (Data Act). Per un approfondimento su quest'ultimo provvedimento normativo, sia consentito rinviare a TORREGIANI 2023, p. 131 ss.

85. KERBER-SCHWEITZER 2017, p. 39 ss.

86. BOSTWICK 2023, p. 465.

87. *Ivi*, p. 440 ss.

88. RATHORE-SHAH-SHUKLA et al. 2021.

89. TELLER 2021.

90. SAPIENZA-PALMIRANI-GRECO 2024, p. 184 ss.

91. Tra gli atti normativi che, al momento, rilevano da questo punto di vista figurano sicuramente i seguenti: Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati (Database Directive); Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva ePrivacy); 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 (GDPR); 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 (Regolamento sui dati non personali); Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie

Solo in esito a siffatta analisi giuridica sarà possibile valutare, con cognizione di causa, le opportunità di un intervento settoriale da parte delle istituzioni europee orientato a regolamentare precipuamente il gemello digitale⁹², nella piena consapevolezza delle difficoltà connesse all'inserimento di un ulteriore provvedimento normativo all'interno del già affollato mosaico regolamentare della società digitale⁹³.

5. Osservazioni conclusive: quali prospettive di regolazione?

I gemelli digitali rappresentano uno strumento destinato ad assumere una importanza capitale nella nostra società. Le previsioni di crescita per il mercato dei *Digital Twin* sono particolarmente promettenti, con alcuni studi che prospettano una dimensione economica pari a 106,26 miliardi di dollari nel 2028⁹⁴.

Il sostegno di un ambiente virtuale in tutto e per tutto corrispondente a quello reale, se plasmato correttamente, non può che impattare positivamente sul benessere della collettività e degli individui: la possibilità di avere a disposizione un "banco di prova digitale", che permette di testare

eventuali alterazioni del sistema e di prevederne gli effetti, consentirebbe di trovare la soluzione più idonea a ogni problema in tempi ridotti e, soprattutto, con rischi contenuti.

Di fronte alla complessità e alle potenzialità di un fenomeno che si inserisce nel solco di quella rivoluzione tecnologica che sta stravolgendo la nostra epoca⁹⁵, sembra opportuno avviare una profonda riflessione finalizzata a indagare quale ruolo può avere il diritto nell'orientarne lo sviluppo nella direzione di una tecnologia che sia rispettosa dei diritti individuali e funzionale alla prosperità della società intera⁹⁶.

In proposito, si registra una certa propensione alla esplorazione di soluzioni regolatorie del gemello digitale da parte degli attori interessati, con i primi tentativi di normazione tecnico-giuridica sviluppati autonomamente da alcune istituzioni o, addirittura, dagli stessi operatori del settore che preferiscono muoversi in un contesto maggiormente chiaro e definito.

Fra gli indicatori di questa tendenza, degni di nota sono sicuramente i *Gemini Principles* elaborati nell'ambito di una partnership, avviata dal governo britannico, tra il *Department for Business*,

dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (Cybersecurity Act); 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 (Direttiva Open Data); 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 (Data Governance Act); Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersecurity nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (Direttiva NIS 2); 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 (Data Act); Regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio, del 13 marzo 2024, che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (Regolamento su un'Europa interoperabile); 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 (AI Act); Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersecurity 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 (Cyber Resilience Act).

92. SUFFIA 2023.

93. IANNUZZI 2024-A, p. 9 ss.

94. BOSTWICK 2023, pp. 463-464.

95. SIMONCINI 2019, p. 63 ss.

96. SIMONCINI 2023.

Energy & Industrial Strategy e l'Università di Cambridge, denominata *Centre for Digital Built Britain* (CDBB), con l'obiettivo di gestire, fra gli altri, il programma governativo *National Digital Twin Programme*⁹⁷.

In tale contesto, è stato elaborato un complesso di principi funzionali a supportare lo sviluppo di un gemello digitale di dimensione nazionale, inteso non come unico (macro)gemello digitale, ma, all'opposto, come insieme di gemelli digitali "federati" uniti tramite la condivisione sicura dei dati⁹⁸.

I nove principi enucleati dal CDBB sono suddivisi in tre grandi categorie, indicate come *Purpose*, *Trust* e *Function*.

Nella prima rientrano tre principi: quello di *Public good*, secondo cui il gemello deve sempre mantenere come fine ultimo il raggiungimento del bene pubblico e il soddisfacimento delle esigenze degli utenti; il principio di *Value creation*, relativo al valore che il gemello deve creare, promuovendo innovazione e concorrenza; e quello di *Insight*, che indirizza la tecnologia verso la generazione di elementi utili ad adottare decisioni migliori.

Nella seconda categoria figurano i principi di *Security*, secondo cui il *Twin* deve garantire la sicurezza, sia fisica che digitale, del sistema, sulla base di un approccio fondato sul rischio; quello di *Openness*, in linea con l'idea di un gemello più "aperto" possibile, ossia fondato su dati aperti, standard aperti e modelli *open source* collaborativi; e, per terzo, il principio di *Quality*, a mente del quale il *Twin* deve essere realizzato con dati di qualità appropriata per lo scopo previsto.

Nell'ultima categoria sono inclusi i principi di *Federation*, che si riferisce, come accennato in precedenza, alla condivisione di dati per abilitare la federazione di diversi gemelli digitali, consentita soprattutto per mezzo di una adeguata interoperabilità; quello di *Curation*, funzionale a stabilire le responsabilità delle diverse parti coinvolte, chiarendo le questioni relative alla *data ownership*; e, da ultimo, quello di *Evolution*, attraverso cui garantire l'adattabilità del gemello digitale ai cambiamenti della tecnologia, della società e dell'ambiente⁹⁹.

Malgrado si tratti di statuizioni, per l'appunto, di principio e dunque prive del carattere prescrittivo tipico delle norme giuridiche vincolanti, esse si pongono come prima linea guida utile a tracciare la rotta per un approccio trasversale che poi permetterà di affrontare con maggiore chiarezza ognuna delle singole questioni giuridiche che possono emergere in tale settore¹⁰⁰.

Proprio in risposta alla esigenza di standardizzazione manifestata dagli operatori e dalla dottrina, anche la *International Organization for Standardization* (ISO) ha elaborato alcune norme di carattere tecnico volte ad agevolare l'attività delle imprese interessate allo sviluppo di progetti relativi ai gemelli digitali. Nello specifico, la ISO, assieme alla *International Electrotechnical Commission* (IEC), ha costituito un sottocomitato nell'ambito del *Joint Technical Committee 1*, (nominato ISO/IEC JTC 1/SC 41) che si occupa, in particolare, del tema *Digital Twin*. Fra il materiale di maggiore rilevanza elaborato in ambito ISO e riguardante i gemelli digitali figurano: la ISO/IEC 30194:2024 (*Internet of things (IoT) and digital twin - Best practices for use case projects*) che illustra le migliori pratiche per chi intende sviluppare progetti di *Digital Twin*; la ISO/IEC 20924:2024 (*Internet of Things (IoT) and digital twin - Vocabulary*) e la ISO/IEC 30173:2023 (*Digital twin - Concepts and terminology*) che chiariscono alcuni aspetti terminologici di tale tecnologia; il rapporto tecnico ISO/IEC TR 30172:2023 (*Internet of things (IoT) - Digital twin - Use cases*) contenente una raccolta di *use cases* relativi ad applicazioni di gemelli digitali in diversi ambiti; e le ISO 23247 (1:2021, 2:2021, 3:2021, 4:2021), dedicate alla individuazione di standard comuni nel settore manifatturiero.

Una ulteriore iniziativa specificamente dedicata alla promozione di standard e finalizzata ad accelerare l'innovazione in ambito *Digital Twin* risponde al nome di "*Digital Twin Consortium*". Si tratta di una organizzazione che coadiuva industria, governo e mondo accademico per incentivare l'uniformità terminologica e lo sviluppo nell'architettura,

97. Per un approfondimento, si rinvia al sito internet del CDBB.

98. BOLTON-BUTLER-DABSON et al. 2018.

99. *Ibidem*.

100. ASLI 2022.

nella sicurezza e nell'interoperabilità della tecnologia dei gemelli digitali in vari settori¹⁰¹.

Fra i documenti prodotti dal *Digital Twin Consortium* assume particolarmente rilevanza il *Digital Twin System Interoperability Framework* che ha l'obiettivo di fornire un quadro di riferimento per l'interoperabilità di sistemi eterogenei integrati nei gemelli digitali¹⁰². Il *Framework* ricorre a sette diversi concetti chiave al fine di predisporre un meccanismo di interoperabilità comune in grado di adattarsi a varie tipologie di *Digital Twin*¹⁰³.

Le iniziative regolatorie del gemello digitale testé illustrate lasciano trasparire una crescente esigenza di disciplina della materia che, con la diffusione del fenomeno, è destinata a intensificarsi fino a fuoriuscire dal ristretto ambito della normazione tecnica. Con ogni probabilità, quando il gemello digitale arriverà a incidere in modo significativo sui diritti e sugli interessi di ampie fasce della collettività, il bisogno di regolazione si manifesterà in

maniera ancora più compiuta, tanto sul piano istituzionale quanto su quello sociale.

Del resto, ogniqualvolta una nuova tecnologia dotata di potenzialità dirompenti si affaccia all'orizzonte, riemerge un interrogativo di natura squisitamente costituzionalistica: come garantire che questi strumenti “non prendano il sopravvento sui diritti fondamentali della persona, sul buon funzionamento della democrazia e sulla libertà dei mercati?”¹⁰⁴.

Nel caso del gemello digitale, tuttavia, il ruolo del diritto non dovrebbe esaurirsi in una funzione meramente limitativa o difensiva, focalizzata sul solo contenimento dei rischi. Le significative potenzialità benefiche di tale strumento richiedono infatti un diritto “proattivo”, capace di guidarne lo sviluppo verso l'obiettivo del benessere individuale e collettivo, ricercando il giusto punto di equilibrio tra la protezione (delle persone e della società) e le esigenze dell'innovazione tecnologica.

Riferimenti bibliografici

- R. ADAM (2000), *Da Colonia a Nizza: la Carta dei diritti fondamentali dell'Unione europea*, in “Il Diritto dell'Unione Europea”, 2000, n. 4
- M.R. ALLEGRI (2018), *Ubi Social, Ibi Ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, 2018
- A. ASLI (2022), *A High-Tech Crystal Ball: The Digital Twin of a Ship and Data Issues in EU Law*, in “Lloyd's Shipping and Trade Law”, 2022
- H. ATLAM, A. ALENEZI, R. WALTERS, G. WILLS (2017), *An overview of risk estimation techniques in risk-based access control for the internet of things*, in “Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDs 2017)”, 2017
- H. ATLAM, G. WILLS (2020), *IoT Security, Privacy, Safety and Ethics*, in M. Farsi, A. Daneshkhah, A. Hosseini-Far, H. Jahankhani (eds.), “Digital Twin Technologies and Smart Cities”, Springer, 2020
- M. ATTARAN, B. CELIK (2023), *Digital Twin: Benefits, use cases, challenges, and opportunities*, in “Decision Analytics Journal”, vol. 6, 2023
- B.R. BARRICELLI, E. CASIRAGHI, D. FOGLI (2019), *A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications*, in “IEEE Access”, vol. 7, 2019

101. Per un approfondimento, si rinvia al sito internet del Digital Twin Consortium.

102. BUDIARDJO-MIGLIORI 2021.

103. BOSTWICK 2023, pp. 468-469. In particolare, i concetti chiave sono i seguenti: *System-Centric Design, Model-Based Approach, Holistic Information Flow, State-Based Interactions, Federated Repositories, Actionable Information, Scalable Mechanisms*.

104. CHELI 2021, p. 954.

- A. BOLTON, L. BUTLER, I. DABSON, M. ENZER, M. EVANS, T. FENEMORE, F. HARRADENCE, E. KEANEY, A. KEMP, A. LUCK, N. PAWSEY, S. SAVILLE, J. SCHOOLING, M. SHARP, T. SMITH, J. TENNISON, J. WHYTE, A. WILSON, C. MAKRI (2018), *The Gemini Principles*, in “CDBB Publications”, 2018
- V. BONCINELLI (2021), *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in “Rivista italiana di informatica e diritto”, 2021, n. 1
- B. BOSTWICK (2023), *Lagging Legislation: The Use of Digital Twins Calls by Manufacturers Calls for New Legal Regulations*, in “Journal of High Technology Law”, vol. 23, 2023, n. 2
- H. BOYES, B. HALLAQ, J. CUNNINGHAM, T. WATSON (2018), *The industrial internet of things (IIoT): An analysis framework*, in “Computers in Industry”, vol. 101, 2018
- A. BUDIARDJO, D. MIGLIORI (2021), *Digital Twin System Interoperability Framework*, A Digital Twin Consortium White Paper, 2021
- M. BUNDIN, A. MARTYNOV, E. SHIREEVA (2022), *Legal Issues on the Use of “Digital Twin” Technologies for Smart Cities*, in A.V. Chugunov, M. Janssen, I. Khodachek, Y. Misnikov, D. Trutnev (eds.), “Electronic Governance and Open Society: Challenges in Eurasia, EGOSE 2021”, Springer, 2022
- C. BUZZACCHI (2016), *Tecnologia e protezione dei dati personali nella società dei big data. Problemi di profilazione e di garanzia della sicurezza pubblica*, in F. Pizzolato, P. Costa (a cura di), “Sicurezza e tecnologia”, Giuffrè, 2016
- S. CALZOLAIO (2023-A), *Isolamento e relazioni sociali. Il Connection-in-All-Policies approach. Nota a: U.S. Surgeon General, Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General’s Advisory on the Healing Effects of Social Connection and Community*, 2023, in “Rivista italiana di informatica e diritto”, 2023, n. 2
- S. CALZOLAIO (2023-B), *Social media e minori. Il Safety-first approach. Nota a: U.S. Surgeon General, Social Media and Youth Mental Health. The U.S. Surgeon General’s Advisory*, 2023, in “Rivista italiana di informatica e diritto”, 2023, n. 2
- S. CALZOLAIO (2017), *Protezione dei dati personali*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), “Digesto delle Discipline Pubblicistiche”, Utet Giuridica, 2017
- E. CHELI (2021), *Conclusioni*, in “Osservatorio sulle fonti”, 2021, n. 2
- A. COSSIRI (2023), *Le campagne di disinformazione nell’arsenale di guerra: strumenti giuridici per contrastare la minaccia alla prova del bilanciamento*, in “Rivista italiana di informatica e diritto”, 2023, n. 2
- C. COSTANZI (2020), *The Legal Implications of Building Information Modeling (BIM) in Public Procurement Law. An Italian Perspective*, in “Rivista Giuridica AmbienteDiritto.it”, vol. 3, 2020
- G. DELLA MORTE (2018), *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, in M. Arcari, E. Milano, A. Tanzi (a cura di), “La ricerca del diritto nella comunità internazionale”, Editoriale Scientifica, 2018
- B. DORSEMAINE, J-P. GAULIER, J-P. WARY, N. KHEIR, P. URIEN (2015), *Internet of Things: a defnition and taxonomy*, Conference Paper: The 9th international conference on next generation mobile applications, services and technologies, 2015
- J. DREXL (2016-A), *Data Ownership and Access to Data*, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate (documento redatto da J. Drexler, R.M. Hilty, L. Desautnettes, F. Greiner, D. Kim, H. Richter, G. Surblytè, K. Wiedemann), 2016
- J. DREXL (2016-B), *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, in “Max Planck Institute for Innovation & Competition”, Research Paper No. 16-13, 2016

- A. FULLER, Z. FAN, C. DAY, C. BARLOW (2020), *Digital Twin: Enabling Technologies, Challenges and Open Research*, in "IEEE Access", 2020
- A. GANDOMI, M. HAIDER (2015), *Beyond the hype: Big data concepts, methods, and analytics*, in "International Journal of Information Management", vol. 35, 2015
- B. GARSKE, W. HOLZ, F. EKARDT (2024), *Digital twins in sustainable transition: exploring the role of EU data governance*, in "Frontiers in Research Metrics and Analytics", vol. 9, 2024
- E.H. GLAESSGEN, D.S. STARGEL (2013), *The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles*, in "Proceedings of the 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference (Honolulu, HI, USA, 23–26 April 2012)", 2013
- M. GRIEVES (2014), *Digital Twin: Manufacturing Excellence through Virtual Factory Replication*, Whitepaper, 2014
- M. GRIEVES (2005), *Product lifecycle management: the new paradigm for enterprises*, in "International Journal of Product Development", vol. 2, 2005, n. 1-2
- M. GRIEVES, J. VICKERS (2017), *Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems*, in "Transdisciplinary perspectives on complex systems", Springer, 2017
- A. IANNUZZI (2024-A), *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024
- A. IANNUZZI (2024-B), *Metaverso, Digital Twins e diritti fondamentali*, in "Rivista italiana di informatica e diritto", 2024, n. 2
- A. IANNUZZI (2021), *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in "Studi parlamentari e di politica costituzionale", 2021, n. 209
- M.J. KAUR, V.P. MISHRA, P. MAHESHWARI (2020), *The Convergence of Digital Twin, IoT, and Machine Learning: Transforming Data into Action*, in M. Farsi, A. Daneshkhah, A. Hosseinian-Far, H. Jahan-khani (eds.), "Digital Twin Technologies and Smart Cities", Springer, 2020
- W. KERBER, H. SCHWEITZER (2017), *Interoperability in the Digital Economy*, in "Journal of Intellectual Property, Information Technology and Electronic Commerce Law", vol. 8, 2017, n. 1
- Z. LIU, N. MEYENDORF, N. MRAD (2018), *The role of data fusion in predictive maintenance using digital twin*, in "AIP Conference Proceedings", 2018
- E. LONGO (2024-A), *La disciplina del "rischio digitale"*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024
- E. LONGO (2024-B), *La disciplina della cybersecurity nell'Unione europea e in Italia*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, "La regolazione europea della società digitale", Giappichelli, 2024
- R. MORO VISCONTI (2016), *Internet delle cose, Networks e plusvalore della connettività*, in "Il diritto industriale", vol. 6, 2016
- V. PAGNANELLI (2023), *La smart city come ecosistema digitale. Profili di data governance*, in "dirittifondamentali.it", 2023, n. 2
- P. PALENSKY, M. CVETKOVIC, D. GUSAIN, A. JOSEPH (2022), *Digital twins and their use in future power systems*, in "Digital Twin", 2022
- O. POLLICINO, M. BASSINI (2017), *Commento all'art. 8*, in R. Mastroianni, O. Pollicino, S. Allegrezza, F. Pappalardo, O. Razzolini (a cura di), "Carta dei diritti fondamentali dell'Unione europea", 2017

- Q. QI, F. TAO (2018), *Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison*, in "IEEE Access", vol. 6, 2018
- M.M. RATHORE, S.A. SHAH, D. SHUKLA, E. BENTAFAT, S. BAKIRAS (2021), *The Role of AI, Machine Learning, and Big Data in Digital Twinning: A Systematic Literature Review, Challenges, and Opportunities*, in "IEEE Access", vol. 9, 2021
- S. SAPIENZA, M. PALMIRANI, S. GRECO (2024), *Data Sharing Governance in Digital Twins and Smart Cities: The European Data Strategy*, in A. Kö, G. Kotsis, A.M. Tjoa, I. Khalil (eds.), "Electronic Government and the Information Systems Perspective. EGOVIS 2024", Springer, 2024
- G.N. SCHROEDER, C. STEINMETZ, C.E. PEREIRA, D.B. ESPINDOLA (2016), *Digital twin data modeling with automation ML and a communication methodology for data exchange*, in IFAC-PapersOnLine 49, 2016
- C. SEMERARO, M. LEZOCHE, H. PANETTO, M. DASSISTI (2021), *Digital twin paradigm: A systematic literature review*, in "Computers in Industry", vol. 130, 2021
- Z. SHEN, F. ARRAÑO-VARGAS, G. KONSTANTINOU (2023), *Artificial intelligence and digital twins in power systems: Trends, synergies and opportunities*, in "Digital Twin", 2023
- A. SIMONCINI (2023), *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in "Rivista Associazione Italiana Costituzionalisti", 2023
- A. SIMONCINI (2021), *Sistema delle fonti e nuove tecnologie. Le ragioni di una ricerca di diritto costituzionale, tra forma di stato e forma di governo*, in "Osservatorio sulle fonti", vol. 2, 2021
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "Bio-Law Journal – Rivista di BioDiritto", vol. 1, 2019
- A. SIMONCINI, E. LONGO (2021), *Fundamental Rights and the Rule of Law in the Algorithmic Society*, in H-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds.), "Constitutional Challenges in the Algorithmic Society", Cambridge University Press, 2021
- A. SIMONCINI, S. SUWEIS (2019), *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in "Rivista di filosofia del diritto", 2019
- I. SPEZIALE, C. BASUNTI (2024), *Cooperative di dati e gemelli digitali urbani*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024
- T. STREINZ (2021), *The Evolution of European Data Law*, in P. Craig, G. De Búrca (eds.), "The Evolution of EU Law", Oxford University Press, 2021
- G. SUFFIA (2023), *How to regulate a Digital Twin City? Insights from a Proactive Law approach: How "human in the loop" and "precautionary principles" can serve policymakers in their attempt to incorporate respect of rights and solidarity in the smart city*, in "24th Annual International Conference on Digital Government Research – Together in the unstable world: Digital government and solidarity", ACM, 2023
- F. TAO, M. ZHANG, Y. LIU, A.Y.C. NEE (2018), *Digital twin driven prognostics and health management for complex equipment*, in "CIRP Annals", vol. 67, 2018, n. 1
- M. TELLER (2021), *Legal aspects related to digital twin*, in "Philosophical Transactions of the Royal Society A", vol. 379, 2021
- S. TORREGIANI (2024), *Intermediari di dati e cooperative di dati nell'ambito del Data Governance Act: verso un nuovo approccio nella gestione dei dati?*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024
- S. TORREGIANI (2023), *Il Data Act: una versione europea del Data Nationalism?*, in "Rivista italiana di informatica e diritto", 2023, n. 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
- E.J. TUEGEL, A.R. INGRAFFEA, T.J. EASON, S.M. SPOTTSWOOD (2011), *Reengineering Aircraft Structural Life Prediction Using a Digital Twin*, in “International Journal of Aerospace Engineering”, 2011
- J. VAN DIJCK (2014), *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in “Surveillance and Society”, vol. 12, 2014, n. 2
- A. WIEBE (2016), *Protection of industrial data – a new property right for the digital economy?*, in “Journal of Intellectual Property Law & Practice”, 2016
- M.M. WINKLER, J. MOSCA (2015), *Cloud computing e protezione dei dati personali*, in M. Fumagalli Mera-viglia (a cura di), “Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?”, Editoriale Scientifica, 2015
- H. ZECH (2016), *A legal framework for a data economy in the European Digital Single Market: rights to use data*, in “Journal of Intellectual Property Law & Practice”, 2016
- V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE (2016), *Ten Legal perspectives on the “Big data revolution”*, in F. Di Porto (a cura di), “Concorrenza e Mercato, Numero speciale. Big Data e concorrenza”, 2016
- Y. ZHENG, S. YANG, H. CHENG (2019), *An application framework of digital twin and its case study*, in “Journal of Ambient Intelligence and Humanized Computing”, vol. 10, 2019, n. 3
- M.M. ZOLTICK, J.B. MAISEL (2023), *Societal Impacts: Legal, Regulatory and Ethical Considerations for the Digital Twin*, in N. Crespi, A.T. Drobot, R. Minerva (eds.), “The Digital Twin”, Springer, 2023



VINCENZO CALDERONIO

Causa ed effetto dell'intelligenza artificiale: sulla natura giuridica dell'output dell'IA e il suo impatto sul regime di responsabilità

Il contributo esplora criticamente la nozione di autonomia dell'intelligenza artificiale (IA) e il suo impatto sul piano giuridico, ponendo in dialogo informatica, giurisprudenza e recente normazione europea. Attraverso un'analisi comparata delle definizioni di IA e algoritmo, l'articolo tenta di chiarire le implicazioni della capacità adattiva dei sistemi d'intelligenza artificiale, interrogandosi sulla possibilità di attribuire valore giuridico agli output da essi generati. Particolare attenzione è riservata al paradigma causale sotteso ai modelli di machine learning, alla luce della giurisprudenza italiana (sentenza Franzese) e delle previsioni dell'AI Act, con lo scopo di evidenziare limiti strutturali dell'IA rispetto ai concetti di responsabilità, imputabilità e personalità giuridica. L'indagine si conclude con l'analisi di tre contesti applicativi – proprietà intellettuale, sistema giudiziario e ambito medico – per proporre un modello di responsabilità ancorato all'azione umana e coerente con la logica dell'accertamento *ex post*.

Intelligenza Artificiale – Causalità – XAI – Responsabilità

Cause and effect of artificial intelligence: on the legal nature of AI output and its impact on the liability regime

The contribution critically explores the notion of artificial intelligence (AI) autonomy and its impact on the legal level, placing theoretical computer science, jurisprudence and recent European standardisation in dialogue. Through a comparative analysis of the definitions of AI and algorithm, the article clarifies the implications of the adaptive capacity of artificial intelligence systems, questioning the possibility of attributing legal value to the generated outputs. Particular attention is paid to the causal paradigm underlying machine learning models, in the light of Italian case law (Franzese ruling) and the provisions of the AI Act, to highlight the structural limits of AI concerning the concepts of responsibility, imputability and legal personality. The survey concludes by analysing three application contexts – intellectual property, the judicial system and the medical field – to propose a liability model anchored to human action and consistent with the logic of *ex post* verification.

Artificial Intelligence – Causality – XAI – Responsibility

SOMMARIO: 1. Introduzione. – 2. Base giuridica per la definizione di intelligenza artificiale. – 3. Distinzione tra intelligenza artificiale e algoritmo nella computer science. – 4. L'autonomia come segno distintivo dell'IA e la circoscrizione della sua area di operatività. – 4.1. Il limite dell'autonomia dell'intelligenza artificiale. – 4.2. La natura giuridica dell'output dell'intelligenza artificiale. – 5. Il ruolo dei sistemi d'intelligenza artificiale nell'ordinamento giuridico. – 5.1. Alcuni esempi. – 6. Conclusioni.

1. Introduzione

L'intelligenza artificiale non possiede ancora oggi dei contorni ben definiti. Contemporaneamente alla recente diffusione di algoritmi di IA accessibili a chiunque, si sta sviluppando un dibattito intorno alla forma che una sua possibile definizione giuridica potrebbe assumere. In questo quadro, nonostante la crescente emanazione di atti giuridici aventi ad oggetto l'IA, il problema della comprensione dei suoi meccanismi di funzionamento permane. Il tema è stato ampiamente studiato in letteratura¹ e rappresenta ancora oggi uno dei maggiori ostacoli per il raggiungimento di una definizione coerente di intelligenza artificiale.

Lo scopo di quest'articolo è quello di analizzare questo problema con una metodologia comparatistica atta ad investigare le diverse definizioni di IA e algoritmo date dal diritto e dall'informatica. Attraverso questa ricognizione l'articolo si propone di focalizzare la sua attenzione sul problema dell'autonomia dell'IA. Mentre il dibattito prevalente sulla natura dell'intelligenza artificiale, nato dalla domanda di Turing "can machine think?"², si è sempre concentrato sulle possibilità che l'IA ha di raggiungere il pensiero umano³, quest'articolo si propone di analizzare se la stessa abbia facoltà

di produrre output giuridicamente rilevanti e se effettivamente agli stessi possa essere conferito un valore giuridico scisso dal rapporto di dipendenza rispetto all'agire umano.

La seconda parte del contributo analizzerà la questione attraverso la chiave interpretativa offerta dalla Corte di Cassazione con la sentenza Franzese (Sez. Unite Penali, n. 30328 del 10 luglio 2002). Laddove infatti l'output dell'IA verrà identificato come prodotto di un calcolo statistico, la sua influenza causale sulle dinamiche che lo coinvolgono dovrà essere controbilanciata da un adeguato valore giuridico che possa garantire le posizioni dei decisori umani che se ne avvalgono. A tal fine verranno analizzati nella parte conclusiva alcuni casi pratici per cercare di comprendere come questi sistemi potranno essere inseriti nel nostro ordinamento giuridico all'interno della cornice regolamentare istituita dall'AI Act, cercando di rispettare un modello di responsabilità improntato alla chiarezza.

2. Base giuridica per la definizione di intelligenza artificiale

Il primo paradigma giuridico per regolamentare l'IA emergente a livello mondiale è quello dell'Unione europea che sotto il nome di AI Act⁴ riunisce

1. Si vedano BRENNAN 2023 e BATHAEE 2018.

2. TURING 1950.

3. I lavori di TURING 1950 e SEARLE 1980 possono essere considerati i capostipiti delle due diverse visioni di IA che oggi sono presenti in letteratura: l'una che vede l'IA come un'entità al pari degli organismi viventi e l'altra come strumento incapace di comprendere o volere.

4. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (Artificial Intelligence Act).

una serie di atti giuridici a vocazione universale⁵. I quali comprendono questioni giuridiche complesse come quelle della definizione di IA, della gestione di questi sistemi nel mercato unico europeo e della regolamentazione della responsabilità per gli output prodotti. L'impatto di questa prima legislazione sul tema dell'inquadramento giuridico dell'intelligenza artificiale è stato determinante a livello mondiale. Infatti, frutto di un lavoro di investigazione scientifica e giuridica iniziato nel 2018⁶, la terminologia e le forme del paradigma giuridico europeo hanno ispirato alcune proposte legislative comparse di recente sul tema⁷, tra le quali è bene ricordare l'Executive order del Presidente degli Stati Uniti Biden⁸, la Risoluzione ONU del marzo 2024⁹, il disegno di legge brasiliano n. 2338/2023¹⁰ e la legge italiana n.132/2025¹¹.

Il paradigma europeo, che ha istituito formalmente una definizione giuridicamente rilevante di intelligenza artificiale, non si è però ritrovato per primo ad affrontare l'argomento. Infatti in campo italiano un primo tentativo di definizione di intelligenza artificiale è stato prodotto dalla giurisprudenza amministrativa che, nella sentenza del Consiglio di Stato n. 7891/2021 ha tentato di dare una compiuta definizione di algoritmo e intelligenza artificiale, in funzione sostitutiva del legislatore, in un caso avente ad oggetto una decisione

algoritmica effettuata illegittimamente. In questo caso il Consiglio di Stato ha inizialmente richiamato la definizione del giudice di prime cure che aveva definito l'algoritmo come: "Semplicemente una sequenza finita di istruzioni, ben definite e non ambigue, così da poter essere eseguite meccanicamente e tali da produrre un determinato risultato". Procedendo poi con una differenziazione tra algoritmo e intelligenza artificiale secondo la quale: "Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di machine learning e crea un sistema che non si limita solo ad applicare le regole software e i parametri preimpostati (come fa invece l'algoritmo 'tradizionale') ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico"¹².

Inquadrando così come punto determinante per la distinzione tra algoritmo e intelligenza artificiale l'autonomia, contenuta nella terminologia "elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti", che la seconda dimostra discostandosi in parte dai parametri preimpostati dal codice di programmazione.

D'altra parte, in campo comunitario, l'approccio dell'Unione europea alla regolamentazione ha prodotto nella versione definitiva del testo dell'AI

5. La terminologia AI Act oggi comprende il Regolamento orizzontale di recente approvazione in seno al Parlamento europeo fondato su numerosi atti giuridici tra i quali l'ormai ritirata AI Liability Directive, doc. COM (2022) 496, e due atti preliminari che hanno influito maggiormente sullo sviluppo della normativa: Commissione europea, *Libro bianco sull'intelligenza artificiale*, doc. COM(2020) 65; Commissione europea, *Relazione sulle implicazioni in materia di sicurezza e responsabilità dell'intelligenza artificiale*, doc. COM(2020) 64, 2020.

6. Si veda sul punto il lavoro preliminare di ricerca e inquadramento teorico della fattispecie effettuato dal gruppo di esperti indipendenti nominato dalla Commissione europea, che ha fortemente inciso sulla legislazione finale e sulla definizione della terminologia del dibattito regolatorio a livello internazionale. HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE 2020, 2019-A, 2019-B.

7. Per una rassegna articolata degli sviluppi legislativi sul tema si vedano i lavori di TADDEI ELMI-MARCHIAFAVA segnalati nei riferimenti bibliografici.

8. United States, Executive Office of the President [Joseph Biden]. *Executive Order 14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. 30 October 2023. Federal Register, vol. 88, no. 210, pp. 75191-75226.

9. United Nations General Assembly, *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, seventy-eight session A/RES/78/L.49, adopted 11 March 2024.

10. Brasil, *projeto de lei* n. 2338-2023, di cui si può trovare una trattazione con allegata una traduzione non ufficiale in BELLI-CURZI-GASPAR 2023.

11. Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale".

12. Citazioni entrambe provenienti dalla sentenza del Consiglio di Stato n. 7891/2021. Si veda inoltre in argomento PIETRANGELO-NANNIPIERI 2023, che sul tema inquadra con precisione i problemi della questione definitoria.

Act una definizione d'intelligenza artificiale basata sul rischio, nella quale l'IA viene definita in base a differenti livelli di autonomia associati a diversi livelli di rischio. L'articolo 3(1) dell'AI Act dà questa definizione di sistema d'intelligenza artificiale: "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"¹³.

Un punto in comune che hanno le due definizioni del Consiglio di Stato e dell'Unione europea è il riferimento che fanno entrambe alle capacità di adattamento dei sistemi IA dopo lo sviluppo, caratteristica che li distingue dagli algoritmi che invece sono statici nel loro funzionamento¹⁴. Infatti, in letteratura sembra essere abbastanza affermata l'idea di definire l'IA in base all'autonomia che mostra¹⁵ e contemporaneamente questo si spiega in virtù della criticità di questa caratteristica. È l'autonomia a segnare la differenza tra un algoritmo e un sistema IA, il quale, a differenza dell'algoritmo, sarà capace di apprendere autonomamente *pattern* di risposta grazie al machine learning¹⁶. Questo, nel quadro della legislazione europea, viene tradotto nella formula "progettato per operare con diversi livelli di autonomia", che pare essere impiegata strategicamente dalla Commissione europea al fine di classificare i sistemi di IA in base al rischio

La scelta regolamentare in questo senso pare efficace perché risponde ad un'esigenza reale, quella di definire diversi livelli di tutela a seconda del rischio potenziale di questi sistemi. La possibilità di associare a diversi livelli di autonomia corrispondenti obblighi normativi che crescono con l'autonomia del sistema si spiega in virtù del fatto che più un sistema di IA è autonomo, più sarà imprevedibile e di conseguenza aumenterà anche il rischio per un output non voluto. Ciononostante, il riferimento a livelli variabili di autonomia, lasciando ampi margini giuridici per l'inquadramento della fattispecie, rischia anche di omettere l'indicazione di un eventuale limite ad essa: esiste questo limite? E se vi è un limite all'autonomia dell'IA, dove va posto? Questi interrogativi sono fondamentali sia per una stringente definizione di sistema d'intelligenza artificiale¹⁷ che per una chiara attribuzione della responsabilità degli output prodotti da esso. In questo senso può essere utile effettuare una prima comparazione tra IA e algoritmo per scoprire in quale punto del loro funzionamento appare questa caratteristica, l'autonomia, e, successivamente, verificarne l'estensione.

3. Distinzione tra intelligenza artificiale e algoritmo nella computer science

Algoritmo e intelligenza artificiale sono due concetti pratici della computer science. Entrambi possono essere fatti derivare dal concetto più ampio e primigenio di *computazione*, derivato da una

13. Art. 3(1) dell'AI Act, Regolamento (UE) 2024/1689 e ripresa dai principi dell'OECD in tema di AI, *OECD Principles on Artificial Intelligence*. OECD Publishing 2019.

14. Sulla centralità del ruolo dell'autonomia per la definizione di questi sistemi nel quadro regolamentare dell'AI Act si veda FERNÁNDEZ-LLORCA-GÓMEZ-SÁNCHEZ-MAZZINI 2024, che propone un'interessante rassegna terminologica delle definizioni impiegate dall'AI Act, e le recenti linee guida della Commissione europea sul tema, *Orientamenti della Commissione sulla definizione di un sistema di intelligenza artificiale ai sensi del Regolamento (UE) 2024/1689 (AI Act)*, doc. C(2025) 924, che stabiliscono espressamente come "il livello di autonomia costituisce una condizione necessaria per determinare se un sistema possa qualificarsi come sistema di intelligenza artificiale".

15. Si vedano questi testi provenienti dal dibattito americano sulle potenzialità dell'IA: LECUN 2022, BUBECK-CHANDRASEKARAN-RONEN et al. 2023 che hanno contribuito non poco anche grazie ai lavori svolti nel 2023 sugli LLM, in particolare OPENAI 2023, all'introduzione nel regolamento europeo della categoria dei *general-purpose AI systems* che ancora a oggi non sono stati chiaramente definiti dalla letteratura scientifica dell'area della computer science.

16. Su tutti si veda RUSSELL-NORVIG 2010.

17. Si veda ALMADA 2025 che lucidamente critica l'eccessiva ampiezza delle linee guida della Commissione in tema di definizione di sistema IA, le quali si prestano a interpretazioni estensive potenzialmente rischiose per la certezza del diritto.

categoria di numeri definiti computabili per la prima volta da Turing nel 1936¹⁸. È da questa categoria che è opportuno partire per ottenere una definizione di algoritmo, sorprendentemente assente sia nell'AI Act che nel Regolamento generale sulla protezione dei dati (GDPR)¹⁹, nonostante il ruolo centrale che quest'architettura informatica ricopre per la costruzione di sistemi IA, nonché per il ruolo giuridicamente rilevante che ha in numerose previsioni delle citate normative.

Una più moderna e formale descrizione di cosa sia un algoritmo derivante dalla computer science la si deve a diversi tentativi di risolvere l'*Entscheidungsproblem* che fu proposto da David Hilbert nel 1928²⁰. L'*Entscheidungsproblem*, o problema della decisione, originariamente aveva ad oggetto la domanda sull'esistenza di una procedura meccanica capace di risolvere ogni problema della matematica²¹. In particolare esso chiedeva se per una formula espressa nel linguaggio formale della logica del primo ordine esistesse una procedura in grado di dichiarare la solvibilità o meno della stessa²². Entrambe le soluzioni proposte da Alan Turing e Alonzo Church dimostrarono l'insolubilità del problema, determinando al contempo un mutamento della sua impostazione teorica. Turing,

nell'elaborare l'omonima Macchina, riformulò infatti il problema in termini di computabilità, sostenendo che un problema è computabile, ossia risolvibile mediante una procedura meccanica, se la macchina, che incarna il metodo meccanico richiesto dal problema della decisione, termina il proprio calcolo²³. La Macchina di Turing ha finito così col diventare la moderna formalizzazione di quello che oggi è un algoritmo.

Le due fondamentali proprietà dell'algoritmo nella teorizzazione di Turing sono la capacità di fornire una procedura meccanica che a partire da un input conduce a un output e la terminazione. Tuttavia, nel caso di un problema senza soluzione, la computazione della Macchina di Turing tende a essere infinita, ovvero a non terminare. In tali circostanze, non si potrebbe parlare propriamente di algoritmo, poiché verrebbe meno la seconda proprietà fondamentale: la capacità di giungere a un risultato finito. Qualunque procedimento meccanico è suscettibile di essere definito algoritmo. Ad esempio, la legge processuale e il diritto amministrativo sono a tutti gli effetti degli algoritmi e rientrano in quella parte del diritto che è da ritenersi computabile²⁴.

18. TURING 1936.

19. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

20. In breve il problema della decisione chiede “[if] there is an absolutely mechanical procedure, that is an algorithm, for deciding the satisfiability or unsatisfiability of any given sentence” (BÖRGER–GRÄDEL–GUREVICH 2001). Questo problema è stato scoperto essere irrisolvibile da Kurt Gödel in matematica con il primo teorema di incompletezza, e in informatica da Alan Turing e Alonzo Church indipendentemente. La scoperta dell'irrisolvibilità del problema ha dato origine alla distinzione tra funzioni computabili e non, secondo la quale per le funzioni computabili esiste un algoritmo che porta ad una soluzione univoca, fattispecie inesistente per le funzioni non computabili; sulla rilevanza del tema in campo giuridico si veda BRENNAN 2023, che propone un'interpretazione giuridicamente rilevante del problema per dimostrare l'impossibilità di conoscere *ex ante* se un'IA produrrà un output etico o meno, rientrando le questioni etiche nella sfera della non computabilità.

21. “The Entscheidungsproblem is solved when we know a procedure that allows for any given logical expression to decide by finitely many operations its validity or satisfiability [...] The Entscheidungsproblem must be considered the main problem of mathematical logic”: BÖRGER–GRÄDEL–GUREVICH 2001, p. 3.

22. *Ibidem*.

23. TURING 1936.

24. Si veda quanto affermato in BORRUSO 1995 “Tutte le volte nelle quali la legge è formulata in maniera così rigorosa da costituire una regola generale, astratta, completa, analitica, inequivoca [...] la legge ha i requisiti di quello che in informatica (e in matematica) si chiama ‘algoritmo’ e, quindi, può ben essere applicata anche da un computer [...] e in taluni casi – sia pur pochi – li ha, come, soprattutto, nel campo del diritto processuale e amministrativo”.

Rispetto alla nozione di algoritmo la definizione di intelligenza artificiale non se ne discosta nelle sue architetture fondamentali, senonché, a differenza dell'algoritmo che è interamente programmato *ex ante* per raggiungere un determinato scopo, l'IA è basata sul machine learning, una tecnica che permette di apprendere autonomamente *pattern* di risposta senza che essi siano stati programmati interamente prima²⁵. Diversamente rispetto a quanto avviene con un semplice algoritmo, nel caso dell'intelligenza artificiale non è il programmatore che crea integralmente l'IA. Il programmatore definisce l'architettura e le regole di apprendimento del sistema, selezionando specifici algoritmi o modelli di apprendimento automatico. Il comportamento del sistema non è tuttavia determinato direttamente dalle singole istruzioni, ma si struttura nel corso della fase di addestramento, in cui il modello si forma a partire dai dati e dai criteri di ottimizzazione stabiliti²⁶. Una volta che le risposte fornite dal programma sono considerate soddisfacenti dagli sviluppatori, allora si può affermare di avere un modello di risposta. In definitiva, in ogni caso il modello non è altro che un *pattern* di risposte che il programma ha imparato a restituire a fronte di determinati input.

4. L'autonomia come segno distintivo dell'IA e la circoscrizione della sua area di operatività

Il vero e proprio *quid pluris* dell'IA è la sua autonomia, ovvero il come un dato modello di IA sviluppa una particolare prassi di risposta²⁷. L'autonomia dell'IA sta nel fatto che essa apprende da

sé le vie mediante le quali corrispondere la risposta esatta, corrispondente all'output atteso, senza che nella maggior parte dei casi gli sviluppatori siano in grado di stabilire il percorso logico in base al quale il programma è arrivato alla soluzione²⁸. Sotto questo profilo la definizione di intelligenza artificiale proposta dal Consiglio di Stato potrebbe risultare troppo vaga. L'ambiguità sorge nella parte in cui si afferma che l'IA "elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico"²⁹. Sul punto non è chiaro se si debba intendere che il processo di apprendimento automatico sia contemporaneo al funzionamento dell'IA o se esso avvenga in un'altra fase.

In questo senso la manualistica³⁰ spiega come i "criteri d'inferenza" non vengono elaborati costantemente, ma solamente nella fase di addestramento dove il modello IA apprende il *pattern* di risposte che poi adotterà in maniera più o meno uniforme nella fase di interazione con gli utenti. In essa, infatti, il modello rimarrà statico, come l'algoritmo, e per l'aggiornamento del modello di risposta sarà necessaria un'ulteriore fase di addestramento. Un sistema d'intelligenza artificiale dopo l'addestramento viene rilasciato in una determinata versione, ad esempio, GPT è stato rilasciato prima in versione 3.5 e successivamente in versione 4. Ogni versione è vincolata ad un particolare modello di risposta che non si auto aggiorna e per ogni innovazione delle capacità di risposta di un modello IA è necessario effettuare nuovamente una fase di training manualmente e aggiornare il precedente modello fornendogli

25. Per un'interpretazione giuridicamente rilevante del concetto di autonomia di un sistema tecnologico, anche relativamente alla nozione di machine learning, si veda SARTOR-OMICINI 2016.

26. RUSSELL-NORVIG 2010.

27. Un esempio nostrano di ricerca sulla *Explainable Artificial Intelligence* (XAI), branca dell'informatica dedicata alla ricerca delle logiche per le quali un determinato sistema di IA corrisponde a determinati output piuttosto che altri, con ampia rilevanza in ambito internazionale è rappresentato da GUIDOTTI-MONREALE-RUGGIERI et al. 2018; mentre, un altro approccio interessante proveniente dalla ricerca internazionale è quello proposto in RIBEIRO-SINGH-GUESTRIN 2016.

28. Questo è il fenomeno che dà origine al *black box problem*, la cui rilevanza giuridica è stata messa in luce da BATHAEE 2018.

29. Sentenza del Consiglio di Stato n. 7891/2021.

30. RUSSELL-NORVIG 2010.

nuovi dati³¹. Ad oggi le tecniche di *continual learning*, che permetterebbero ai sistemi IA di apprendere in tempo reale, non sono integrabili nei modelli di machine learning per via della loro impraticabilità³². Tuttavia, anche se si ipotizzasse un futuro in cui l'IA fosse capace di adattarsi all'ambiente e all'informazione in tempo reale, ci si potrebbe domandare quanto questa forma d'interazione possa essere simile a quella propria delle forme d'intelligenza naturale³³.

In ogni caso queste brevi considerazioni sembrano porsi in antitesi con le definizioni di IA date dal Consiglio di Stato e dalla Commissione europea, nella parte in cui entrambe le definizioni affermano che l'intelligenza artificiale apprende e si auto aggiorna sulla base dei dati dell'ambiente circostante³⁴. Ciò è vero, ma con la precisazione che questo tipo di comportamento adattivo non è qualcosa che la macchina compie spontaneamente, ma piuttosto essa necessita dell'intervento umano per ogni nuovo aggiornamento. Con la

conseguenza che dopo l'aggiornamento il modello di risposta del sistema IA rimarrà cristallizzato fino al prossimo aggiornamento umano. Resta aperto il problema di come un modello di IA apprenda a corrispondere gli output esatti. È questo infatti il momento nel quale compare l'autonomia dell'intelligenza artificiale che la distingue da un mero algoritmo.

4.1. Il limite dell'autonomia dell'intelligenza artificiale

La questione è attualmente affrontata dal filone di ricerca sull'*explainable artificial intelligence* (XAI)³⁵, devota alla ricerca della risposta sul come i sistemi di intelligenza artificiale possano apprendere autonomamente, quali regole impiegano, se effettivamente vi è una loro autonomia e quanto essa sia estesa. È da questo campo di ricerca che sono nate le prime voci critiche sull'effettiva estensione dell'autonomia dell'intelligenza artificiale e dunque anche sulla natura degli output che produce.

31. Questa tra l'altro è una delle ragioni all'origine della pratica di raccolta e utilizzo dei dati degli utenti da parte di OpenAI che ha inizialmente causato il blocco da parte del Garante della Privacy, dati utili per aggiornare il modello di risposta, doc. web 10085455.
32. Per aver riscontro di quanto affermato si veda la sezione "On the path to more general artificial intelligence" al punto *continual learning* a p. 93 di Bubeck–Chandrasekaran–Ronen et al. 2023 dove viene ampiamente descritto come uno dei limiti di GPT-4 è che esso non può apprendere in tempo reale, affermazione che comporta la fissità di questi modelli, che restano ancorati a determinati modelli di risposta incapaci di auto aggiornarsi.
33. In argomento SHANAHAN–CROSBY–BEYRET–CHEKE 2020 dove vengono descritti diversi limiti dell'IA quando comparata all'intelligenza animale come ad esempio l'assenza di comprensione della causalità, la non trasferibilità delle informazioni apprese in altri ambiti e l'assenza di scopi e motivazioni intrinseci.
34. Aspetto rimarcato ulteriormente dalla Commissione europea negli *Orientamenti della Commissione sulla definizione di un sistema di intelligenza artificiale ai sensi del Regolamento (UE) 2024/1689 (AI Act)*, doc. C(2025) 924, nei quali si afferma come "l'adattabilità" si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare comportamento durante l'uso". È opportuno precisare che l'adattività dei sistemi di intelligenza artificiale, nella maggior parte dei casi, non implica un apprendimento continuo. Infatti, il modello apprende durante la fase di addestramento, mentre nella fase di utilizzo non sviluppa nuovi *pattern* di risposta, ma si limita a adattare il proprio comportamento in base agli input ricevuti, senza aggiornare autonomamente i propri parametri. Definizioni troppo ampie, come il riferimento alle capacità di autoapprendimento, potrebbero quindi generare ambiguità interpretative (ALMADA 2025), in particolare nel trattamento sanzionatorio, alimentando letture che accostano l'adattabilità dell'IA a forme di apprendimento naturale e, in ultima analisi, a ipotesi di rieducabilità attraverso la pena. Per questo motivo, è fondamentale circoscrivere con precisione il concetto di apprendimento automatico, escludendo dal suo perimetro forme di interattività proprie dell'intelligenza naturale e scenari speculativi o fantascientifici.
35. Sul punto si vedano i contributi di GUIDOTTI–MONREALE–RUGGIERI et al. 2018 e RIBEIRO–SINGH–GUESTRIN 2016, che rappresentano vere e proprie pietre miliari sul tema, tentando di dare risposta sul come si sviluppino i modelli di risposta dei sistemi IA.

In letteratura una scuola di pensiero molto diffusa³⁶ risponde a queste domande affermando che il metodo di ragionamento sul quale sono basate le IA sia la probabilità, in accordo con la sua provenienza dalla computazione. Alcuni esempi del funzionamento probabilistico dell'attuale intelligenza artificiale sarebbero l'*attention mechanism* basato sul transformer e il caso *husky vs wolf*. L'*attention mechanism* è una tecnica di addestramento particolarmente usata per i *large language models* (LLMs) mediante la quale l'algoritmo nella fase di addestramento associa a ciascuna informazione data in input un valore numerico percentuale differente, concentrandosi così sulle informazioni che si presentano più spesso e associando ad esse un peso maggiore³⁷; successivamente nella fase di generazione di testo l'algoritmo determinerà quale parola generare sulla base di calcoli probabilistici basati sulla frequenza delle parole usate in contesti simili. Quest'informazione sarà presa sulla base dei dati di addestramento dai quali ha appreso i *pattern* di risposta. Le parole che genererà l'algoritmo saranno dunque quelle alle quali è stato associato lo *score* più alto e baserà su di esse l'output. È facilmente intuibile come la logica sottostante a questo tipo di funzionamento sia la logica della probabilità statistica. Nell'esempio di una traduzione l'algoritmo non si concentrerà sul significato complessivo del testo ma procederà con la traduzione basandosi sulla frequenza delle parole e dando più importanza a quelle che si presentano più spesso.

In modo analogo, nell'esempio *husky vs wolf*, l'algoritmo incaricato di classificare immagini di cani come "husky" o "wolf" ha prodotto una classificazione errata, etichettando alcune foto di

husky come lupi. Quando i ricercatori hanno chiesto all'algoritmo sulla base di quale criterio avesse erroneamente classificato un husky come lupo, l'IA ha risposto indicando la presenza della neve: riconosceva una foto come "lupo" basandosi esclusivamente sullo sfondo innevato (*snow pattern*)³⁸. Quest'esempio di modello in *over-fitting*³⁹ rispetto ai dati che riceve sembra dimostrare che l'IA si basi su un'analisi quantitativa, nella quale a fronte del *pattern* ricorrente associa una voce di classificazione. In questo senso il machine learning, differentemente rispetto all'apprendimento naturale⁴⁰, individua una maggiore concentrazione di pixel bianchi, la neve, nelle foto rappresentanti i lupi ai quali associa la voce "wolf". Ciò sembrerebbe dimostrare come il machine learning riesca a emulare una parte del pensiero umano basata su un modello di apprendimento *try and error* dal quale però non sempre è possibile risalire a motivazioni fondate. Questa dimensione dell'autonomia dell'IA, che pure è capace di dimostrare livelli d'intelligenza elevati, pone però un problema per le categorie classiche del diritto, creando una notevole incertezza circa la natura giuridica degli output che produce.

4.2. La natura giuridica dell'output dell'intelligenza artificiale

In questo quadro, l'output dell'intelligenza artificiale sembra essere prodotto dalla riproduzione di una legge statistica che, come nel caso *husky vs wolf*, esegue meccanicamente un'analisi quantitativa dei dati senza una reale comprensione causale della situazione che le viene posta⁴¹. Per tale ragione, molti output dei sistemi di intelligenza artificiale

36. Si vedano i lavori di BENDER–GEBRU–MCMILLAN–MAJOR–SHMITCHELL 2021 e FOKAS 2023.

37. Vedi VASWANI–SHAZEER–PARMAR et al. 2017 e per una spiegazione semplificata *Attention mechanism: Overview* (Meccanismo di attenzione: Panoramica), un video di Google Cloud Tech. Va ricordato che è quest'architettura informatica a costituire il fondamento di tutti i modelli di IA generativa ad oggi disponibili.

38. Nel caso in esempio i ricercatori hanno volutamente fornito all'IA immagini di lupi con associato lo *snow pattern* perseguendo volutamente un modello sbagliato, si veda RIBEIRO–SINGH–GUESTRIN 2016.

39. L'overfitting è un problema frequente per i modelli statistici troppo complessi che sviluppano un sovradattamento ai dati di addestramento, il che li rende impraticabili in contesti in cui vi sono dati differenti a causa della loro mancanza di generalità, YING 2019.

40. SHANAHAN–CROSBY–BEYRET–CHEKE 2020.

41. Su tutti si veda l'esperimento della stanza cinese di John Searle, nel quale egli, emulando il meccanismo di black box dell'IA, immagina di trovarsi in una stanza chiusa con un dizionario di cinese-inglese, dalla porta gli vengono passati dei biglietti scritti in cinese che lui raccoglie e traduce con il dizionario per comprenderli e

risultano difficilmente spiegabili, in quanto non fondati su catene di ragionamento causale assimilabili a quelle proprie del pensiero umano, ma sulla correlazione statistica tra variabili. In questo senso, affermare che in una fotografia sia rappresentato un lupo piuttosto che un husky in ragione della maggiore presenza di neve, ossia di una più elevata concentrazione di pixel bianchi, equivale a fornire una motivazione meramente descrittiva e statisticamente orientata, insufficiente sul piano logico e priva di reale valore esplicativo.

Questo fenomeno, ovvero quello dell'incidenza della probabilità sull'assunzione di un fatto come motivazione per spiegare una data circostanza, è stato affrontato a suo tempo dalle Sezioni Unite della Corte di Cassazione nella famosa sentenza *Franzese*, chiamata a pronunciare un principio di diritto su una questione molto simile avente ad oggetto la base motivazionale per giudicare una causa come penalmente rilevante ai fini della condanna. Il tema, lungi dall'essere desueto, è fondamentalmente connesso alla fattispecie dell'intelligenza artificiale e alla natura giuridica dei suoi output, così come al valore giuridico che l'ordinamento è chiamato a dare di essi. Uno dei passaggi chiave della sentenza *Franzese* ha infatti ad oggetto "i criteri di determinazione e di apprezzamento del valore probabilistico della spiegazione causale", e dunque la legittimità dell'uso di tecniche valutative probabilistiche in tema di pronunce giudiziali.

Già infatti nel caso COMPAS⁴², algoritmo di predizione della recidiva, è venuto in essere il limite che la predizione probabilistica può avere nella

spiegazione causale degli eventi. Nel caso di specie, usando lo stesso criterio probabilistico di analisi quantitativa dei dati del caso *husky vs wolf*, l'algoritmo COMPAS dava in output maggiori livelli di rischio di recidiva per le persone di colore solo sulla base di un dato statistico, ovvero che la maggior parte delle persone di colore registrate nel database erano poi risultate recidive⁴³. In questa situazione ci si trova di fronte a un dato statisticamente corretto ma privo di efficacia giustificativa sotto il piano causale, questo perché l'essere una persona di colore non è causa sufficiente per la giustificazione di una previsione di recidiva. Sotto un profilo causale una spiegazione efficace potrebbe alternativamente essere la presenza di indici, come potenziali motivazioni del reo, che lo possano spingere a commettere un illecito nuovamente, ma a ben vedere quest'indice causale può essere confermato con certezza solo *ex post*, a fatto compiuto.

Su questo punto di intersezione tra XAI e giurisprudenza di legittimità si innesta la questione sulla natura giuridica dell'output dell'intelligenza artificiale. Mentre il settore della XAI ad oggi approfondisce il tema della distinzione tra causazione e spiegazione⁴⁴, pure fondamentale per lo sviluppo di sistemi IA più intelligenti, questa stessa questione è già stata parzialmente risolta dalle Sezioni Unite affermando come il calcolo statistico e la probabilità non siano sufficienti per dare una spiegazione sulla causazione degli eventi e che, nel giudizio, essi non possono soppiantare il necessario accertamento processuale del decorso causale nel caso concreto⁴⁵. La conseguenza per il giudice

formulare risposte che poi ritradurrà e ripasserà da sotto la porta, corrispondendo così output corretti e coerenti senza l'effettiva comprensione della lingua cinese. Questo esperimento mentale ha dimostrato come l'IA abbia a disposizione una forma di comprensione solamente sintattica alla quale manca la comprensione semantica della realtà, che è necessaria per poter attribuire a qualunque entità forme di soggettività, SEARLE 1980.

42. *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS), noto software americano usato per predire la possibilità di recidiva di un imputato, al centro del caso *Eric Loomis* (*State v Loomis*, 881 NW2d 749, 754 – Supreme Court of Wisconsin), nel quale è stato dimostrato come il software sistematicamente desse in output percentuali maggiori di potenziali recidivi per gli imputati di colore solo sulla base della rilevanza statistica del dato sulla loro carnagione. Vedi CARNAT 2024.

43. Lo studio condotto da ProPublica è stato presentato in Larson–Mattu–Kirchner–Angwin, *How We Analyzed the COMPAS Recidivism Algorithm*, 2016 e Angwin–Larson–Mattu–Kirchner, *Machine Bias*, 2016 in propublica.org.

44. Si veda CARLONI–BERTI–COLANTONIO 2023.

45. Cass., Sez. Unite Penali, n. 30328 del 10 luglio 2002, *Franzese*, da leggere secondo l'interpretazione data da VIGANÒ 2013: "la mancanza di una legge di copertura con coefficiente statistico pari o prossimo al 100%

è espressa dal principio di diritto che recita “non è consentito dedurre automaticamente dal coefficiente di probabilità espresso dalla legge statistica la conferma, o meno, dell'ipotesi accusatoria sull'esistenza del nesso causale”⁴⁶.

In questo senso, tale principio di diritto pare applicabile per estensione analogica anche alla fattispecie del valore giuridico dell'output dell'intelligenza artificiale. Essendo lo stesso solo frutto di un mero calcolo statistico, come nei casi portati ad esempio, esso non costituirà mai il prodotto di un'analisi causale basata su una valutazione *ex post* dei dati rilevanti, ma costituirà tutt'al più una forma di applicazione *ex ante* della legge statistica generale al caso concreto e pertanto suscettibile di errori e inesattezze logiche⁴⁷. Pertanto, alla luce della chiave interpretativa offerta dalla sentenza Franzese, l'output dell'intelligenza artificiale potrebbe al più essere considerato uno strumento di supporto, utile a rappresentare leggi di tipo statistico o scientifico-universale. In tale prospettiva, esso può fungere da elemento ausiliario nel processo decisionale, ma non potrà mai assurgere a criterio autonomo e risolutivo, giacché la decisione finale dovrà sempre fondarsi sul libero apprezzamento del giudice in relazione alle specifiche circostanze del caso concreto.

Tutto ciò, traslato in materia di valore giuridico dell'output dell'intelligenza artificiale, sembra suggerire che non solo l'output dell'IA non potrà avere sufficiente valore spieghazionale per essere posto a fondamento del giudizio, come già anticipato dalla sentenza Franzese a suo tempo e confermato dal caso Loomis, ma allo stesso tempo, ad esso non dovrà neanche essere attribuita una sufficiente facoltà giuridica per poter costituire autonomi rapporti di diritto se sciolto dal rapporto di dipendenza che esso ha rispetto all'agire umano, perché

inidoneo a costituire un rapporto di imputazione tra esso e l'ente che lo produce. In questo quadro risulta essere pienamente condivisibile la pronuncia del Consiglio di Stato in tema di inadeguatezza della decisione algoritmica a costituire autonomi rapporti giuridici quando sciolta da un vincolo di attribuzione rispetto ad una decisione umana.

5. Il ruolo dei sistemi d'intelligenza artificiale nell'ordinamento giuridico

Quest'ultimo punto della riflessione apre un inedito scenario sul ruolo che i sistemi d'intelligenza artificiale andranno a ricoprire nei nostri ordinamenti nel contesto recentemente inaugurato dall'Artificial Intelligence Act. Essi, alcuni già ora, verranno senz'altro integrati in molte delle professioni attualmente svolte nella società. Già sono noti i casi sia cinesi⁴⁸ che americani⁴⁹ di integrazione di IA nel settore giudiziario, ai quali possono essere accompagnati i casi dell'introduzione di questi sistemi in campo medico, artistico e amministrativo. La naturale conseguenza di quest'introduzione dell'IA nei nostri ordinamenti sarà la rilevanza giuridica dei suoi output, che andranno a influire sui rapporti tra consociati.

Per questa motivazione e in continuità con le argomentazioni dei paragrafi precedenti, la soluzione proposta in dottrina sulla possibilità di attribuire forme di personalità giuridica a questi sistemi⁵⁰ non pare essere percorribile. Infatti, a forme di personalità giuridica si accompagnano anche conseguenti facoltà come la possibilità di costituire, modificare o far terminare rapporti giuridici, e con esse anche la possibilità di esserne titolari e di essere potenziali soggetti imputabili per azioni legali connesse a questi mutamenti. Non solo gli attuali sistemi di IA non sono suscettibili di essere considerati soggetti

non può impedire l'ascrizione causale di un evento a una condotta, quando l'evento – a una considerazione *ex post* – non è ragionevolmente spiegabile se non come conseguenza di quella condotta”.

46. *Ibidem*.

47. Fenomeno questo alla base delle “allucinazioni” dell'intelligenza artificiale, ovvero di risposte prive di senso logico. Per un'ulteriore riflessione si veda il già citato caso degli *stochastic parrots* BENDER–GEBRU–MCMILLAN–MAJOR–SHMITCHELL 2021.

48. Si veda LIU-LIU-LIN 2024.

49. Si veda il già citato caso COMPAS, *State vs Loomis*, 881 NW2d 749, 754 (Win 2016) (Supreme Court of Wisconsin).

50. Si vedano HALLEVY 2010; SOLUM 2020.

agenti⁵¹, sia per la loro mancanza di raziocinio⁵² che per la loro natura sistemica, ma come si è visto i loro output sono ad oggi privi di spiegabilità e dunque di base motivazionale che possa fungere contestualmente da base giuridica per rendere tali sistemi imputabili. La conseguenza di questo ragionamento è che un sistema d'intelligenza artificiale sganciato dal rapporto di intrinseca dipendenza che esso ha con l'umano è privo di qualunque valore giuridico, il quale dunque deriva solamente dal quantum che l'umano decide di trasferire in questo sistema.

In questo quadro, l'attribuzione di forme di personalità giuridica a sistemi di intelligenza artificiale potrebbe legittimare forme di responsabilità oggettiva, fondate sull'accertamento causale degli eventi sulla base di considerazioni statistiche *ex ante* piuttosto che considerazioni causali *ex post*, così di fatto abbassando il livello di tutela costituzionale garantito alla tutela dei diritti della persona umana⁵³ e andando contro quanto statuito sul tema nel nostro ordinamento dalle sentenze gemelle della Corte Costituzionale (n. 348 e 349/2007) e dalla Corte di Cassazione con la sentenza Franzese⁵⁴. Pertanto, la necessità che si pone oggi sotto il profilo giuridico è quella di legare l'output

dell'intelligenza artificiale all'azione umana che l'ha causato, ancorando così i profili di responsabilità per gli output prodotti da questi sistemi al principio di personalità della responsabilità giuridica. Questa soluzione, sebbene attualmente adottabile, richiede un ulteriore approfondimento attraverso l'analisi di alcune questioni giuridiche già emerse nella prassi.

5.1. Alcuni esempi

Per dare maggiore concretezza a questa argomentazione, risulta utile esaminare alcuni esempi tratti dalla letteratura che illustrano l'impiego di sistemi IA già esistenti e attualmente utilizzati in diverse professioni. L'analisi di questi esempi potrà facilitare la comprensione del ruolo che questi sistemi potrebbero assumere nel quadro regolamentare delineato dall'AI Act.

I casi selezionati sono tre: proprietà intellettuale, uso d'IA nel sistema giuridico (giudiziario e pubblica amministrazione) e in campo medico. Gli ultimi due sono stati selezionati per affrontare contestualmente il tema della responsabilità, fattispecie di rilievo il cui futuro ancora oggi è incerto in seguito al ritiro dell'AI Liability Directive da parte della Commissione europea⁵⁵, che segna

51. Sul punto si vedano i contributi di FLORIDI 2023 e FLORIDI 2025, laddove la stessa definizione proposta di IA come *Agere sine Intelligere* risulta problematica sotto molteplici profili giuridici, tra i quali la responsabilità, la soggettività e la causalità. In tal senso va considerata la difficoltà nell'imputare gli output dell'IA ad una sua stessa facoltà agente, dovuta all'assenza di una loro spiegabilità intrinseca. Per alcune voci critiche si vedano ROLI-JAEGER-KAUFFMAN 2022; NYHOLM 2018.

52. Si veda ancora una volta sul punto il noto argomento della stanza cinese proposto in SEARLE 1980 per dimostrare come il nodo principale per la riproduzione di una forma d'intelligenza sia la comprensione di quelle funzioni soggettive, come la comprensione semantica del linguaggio, che danno origine all'identità. Al quale può essere accompagnata la già richiamata rappresentazione di IA come *stochastic parrot* presente in BENDER-GEBRU-McMILLAN-MAJOR-SHMITCHELL 2021.

53. Si veda sul punto SIMONCINI 2019, che lucidamente fa notare come "Vi è un effetto sulla sfera della libertà giuridica ben più rilevante e profondo delle possibili applicazioni tecnologiche; esso, in realtà, va ad intaccare uno dei fattori essenziali del fenomeno giuridico in quanto tale, ovvero l'idea stessa dell'esistenza di un nesso di causalità tra gli eventi e, conseguentemente, la distinzione 'mezzo-fine' ovvero 'agente-strumento' nella definizione dei comportamenti e delle relazioni" con una possibile conseguente riduzione delle tutela costituzionalmente garantita derivante dalla scelta di far prendere agli algoritmi di IA decisioni giuridicamente rilevanti.

54. Sentenze che sebbene distinte sul piano dell'oggetto della pronuncia, le prime in tema di principio di colpevolezza e la seconda in tema di accertamento del nesso causale, possono essere interpretate alla luce di un unico criterio, ovvero quello della chiara attribuzione di responsabilità individuale per gli illeciti penali, rigettando formule vaghe idonee ad annacquare la responsabilità penale dell'individuo.

55. Commissione europea, *Proposta di direttiva del Parlamento europeo e del Consiglio sull'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale* (AI Liability Directive),

un rilevante vuoto legislativo europeo in tema di responsabilità per gli output prodotti dall'IA. Ad ogni modo si partirà trattando il tema della proprietà intellettuale, forse il migliore per affrontare per prima la questione della natura giuridica degli output dell'intelligenza artificiale.

5.1.1. *Proprietà intellettuale*

Con l'introduzione dell'intelligenza artificiale generativa, capace di creare contenuti innovativi partendo dai dati in input combinati con quelli del proprio dataset, è venuta in essere anche la relativa questione sulla protezione del diritto d'autore e sulla possibilità di riconoscerlo ai sistemi di IA. Sotto quest'ultimo profilo ha fatto molto discutere a livello internazionale il caso DABUS, discusso dal Tribunale federale australiano⁵⁶, il quale, in una decisione sui generis, ha deciso di riconoscere al sistema IA denominato Dabus (*Device for the Autonomous Bootstrapping of Unified Sentience*) il diritto di possedere dei brevetti su due invenzioni da esso generate, riconoscendogli così di fatto anche la qualifica di inventore. Tale decisione è stata poi ribaltata dalla Full Federal Court che ha stabilito come il diritto d'autore e la brevettabilità di un'invenzione siano riconoscibili solo alle persone fisiche, escludendo così di fatto la possibilità di accordare a sistemi IA qualunque diritto di paternità per l'opera computazionale⁵⁷. La questione ha fatto molto discutere⁵⁸, anche in relazione al ruolo che oggi hanno i sistemi di intelligenza artificiale generativa nella creazione di contenuti. Infatti è ancora poco chiaro quale sia lo statuto giuridico dell'opera realizzata con lo strumento informatico, proprio per via del *quid pluris* che l'IA vi aggiunge rispetto al contributo umano.

In questo quadro sicuramente sembra essere corretta la critica di forme di attribuzione di diritto d'autore alle macchine posto che, come già fatto notare⁵⁹, il lavoro svolto dal sistema IA sulla generazione di un'opera computazionale è sempre eterodiretto dall'essere umano che programma il sistema e definisce in input i suoi obiettivi. Pertanto, all'output dell'IA non può essere riconosciuto il carattere della *creatività*, necessario al fine del riconoscimento del diritto d'autore, perché l'opera prodotta dall'IA non sarà altro che una forma di riproduzione meccanica di *pattern* ricorrenti che l'IA ha imparato a riconoscere nei dati sui quali essa è stata addestrata⁶⁰. In questo senso, il valore giuridico del suo output può invece venire in essere in relazione al riconoscimento del diritto d'autore alla persona fisica che l'ha prodotto avvalendosi dell'IA come strumento. Confermando il giudizio espresso precedentemente sul valore giuridico da attribuire all'output dell'intelligenza artificiale: ovvero come intrinsecamente legato ad un rapporto di dipendenza con l'agire umano.

5.1.2. *L'uso dell'IA nel sistema giudiziario*

Nel caso di utilizzo dell'intelligenza artificiale nell'ambito dell'ordinamento giuridico il rapporto tra l'output dell'IA e l'umano si capovolge. Mentre nel caso del diritto d'autore l'IA è uno strumento nelle mani umane, mediante il quale l'umano produce un output, nel caso del sistema giudiziario l'output dell'IA esercita una notevole influenza sul giudice umano o sul destinatario del provvedimento amministrativo automatizzato nel caso di uso di IA nella pubblica amministrazione.

Come già visto in relazione al caso COMPAS, la questione attiene al tipo di valore giuridico che

doc. COM(2022) 496, che successivamente alla pubblicazione del report di HACKER 2024, era entrata in una fase di stallo a causa dell'incertezza se propendere per un sistema di responsabilità basato sulla colpa o sulla responsabilità oggettiva, infine definitivamente ritirata dalla Commissione europea. Fattispecie che invece è regolamentata nell'attuale versione della proposta legislativa brasiliana (PL 2338-2023) agli articoli 35-39.

56. Federal Court of Australia, *Thaler v Commissioner of Patents* [2021] FCA 879.

57. MATULIONYTE 2022.

58. *Ibidem*, per una puntuale critica della decisione della corte federale australiana.

59. *Ibidem*.

60. Per un orientamento opposto si veda DESHPANDE-KAMATH 2020 che, analizzando il caso DABUS nel contesto della legislazione indiana, afferma come la sua opera possa essere brevettabile, essendo assente nel Patents Act indiano del 1970 ogni riferimento alla persona naturale, con invece ampi margini di interpretabilità del termine "person", arrivando ad includere anche il Governo ed i suoi organi funzionali.

bisogna riconoscere all'output dell'IA nell'eventualità in cui esso concorra a determinare una decisione umana. Punto di partenza per questa riflessione è che di fatto, la sola presenza di un output dell'IA come elemento di valutazione per il giudice rende lo stesso output idoneo ad avere un valore giuridico autoritativo sull'interpretazione che il giudice darà del caso⁶¹. Esso contribuirà dunque a definire la prospettiva attraverso la quale il giudice interpreterà i fatti, concorrendo insieme agli altri elementi di prova a definire il caso stesso. Per questa motivazione, come fatto notare da Simoncini, non è sufficiente che la legge richieda, come nel caso di COMPAS, che la valutazione giudiziale si basi anche su ulteriori elementi valutativi e non integralmente sull'output dell'intelligenza artificiale. Questo perché "chi ha preso la decisione, infatti, avrà sempre la possibilità di sostenere che nella decisione si è solo avvalso dell'algoritmo, ma non è stato 'sostituito' da esso"⁶². Ci si trova qui di fronte ad un contesto nel quale, una volta introdotto l'output dell'IA all'interno dell'ordinamento, nel caso di specie all'interno della valutazione giudiziale, esso avrà a prescindere un valore giuridico di fatto, indipendentemente dall'uso che se ne farà. In questo quadro è fondamentale l'applicazione delle regole di design *ex ante* che l'AI Act impone per la progettazione di sistemi d'intelligenza artificiale ad

alto rischio per il loro possibile impatto sociale, al fine di prevenire possibili errori di questi sistemi⁶³. Ad esse in ogni caso appare opportuno affiancare oneri di motivazione rafforzati per il giudice che si avvalga di output IA nella valutazione della prova o nel giudizio⁶⁴. Quest'ultima esigenza appare necessaria per circoscrivere razionalmente l'ambito d'applicazione dell'IA di fronte alla contestuale possibilità che i suoi output vadano ad influenzare in maniera sproporzionata la valutazione giudiziale.

Accanto a questa questione, in rapporto di dipendenza si pone la questione già affrontata dalla giurisprudenza nostrana della legittimità della decisione automatizzata, in buona parte risolta dalla sentenza del Consiglio di Stato n. 2270/2019, con la quale è stata affermata l'indoneità di una decisione puramente automatizzata a definire rapporti giuridici tra i consociati, fattispecie già normata dall'art. 22. co.1 GDPR. Senza dilungarsi troppo sul punto⁶⁵, parrebbe opportuna l'introduzione formale di un obbligo di decisione umana per tutte quelle questioni sostanziali, o *semantiche*, idonee a influire sui diritti fondamentali dell'individuo, lasciando così aperta la possibilità di utilizzare algoritmi di IA per la risoluzione di questioni procedurali, o *sintattiche*⁶⁶, puramente computazionali, le quali sono anch'esse parte del diritto,

61. Argomento già discusso in Simoncini 2019 e Carnat 2024. In quest'ultimo contributo va segnalata la riflessione sull'*automation bias*, oggetto dell'art. 14.4(b) dell'AI Act, ovvero la possibile tendenza ad affidarsi automaticamente o a fare eccessivo affidamento sui risultati prodotti da un sistema di IA, fenomeno che contribuisce a ridurre il margine di indipendenza della decisione umana quando coadiuvata da un sistema IA.

62. SIMONCINI 2019 p. 81.

63. Si veda il Capitolo 3, sezioni 2 e 3 dell'AI Act (Regolamento (UE) 2024/1689) che stabilisce requisiti e obbligazioni per i provider di sistemi d'intelligenza artificiale ad alto rischio. Accanto ad esso si pone il considerando 61 che stabilisce esplicitamente come "L'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana", ripreso anche dall'art. 15 della legge 132/2025 che recita "nei casi di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria è sempre riservata al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti".

64. Ampliando un poco l'orizzonte, si veda sul tema dell'incidenza degli strumenti informatici sulla discrezionalità giudiziale BORRUSO 2002.

65. Già oggetto di cospicua dottrina, si vedano ancora una volta SIMONCINI 2019 e la giurisprudenza nazionale del TAR Lazio sezione III bis nn. 9224-9230 del 2018 e 12026 del 2016.

66. Distinzione che riprende quanto statuito da SEARLE 1980 che usa i due termini per definire due differenti tipologie di operazioni: le operazioni sintattiche, come il calcolo, le quali non richiedono necessariamente una effettiva comprensione dell'operazione purché essa venga portata a compimento con successo e le operazioni

soprattutto procedurale ed amministrativo, e per le quali non è necessaria la partecipazione decisionale umana⁶⁷.

La *ratio* di questa norma andrebbe rinvenuta nell'impossibilità di risalire a logiche coerenti nei sistemi d'intelligenza artificiale, i quali, fondandosi solamente su procedimenti computazionali sintattici, difficilmente potranno pervenire a logiche decisionali effettivamente spiegabili se impiegati per effettuare decisioni giuridicamente rilevanti. Pertanto, andando oltre il già noto divieto di decisione automatizzata per la determinazione di questioni attinenti ai diritti fondamentali⁶⁸, la non spiegabilità delle decisioni automatizzate potrebbe rendere insufficienti le forme di tutela come l'intervento umano⁶⁹ o il diritto alla spiegazione delle decisioni algoritmiche⁷⁰, ricadendo così in fattispecie di incostituzionalità *ab origine* dell'algoritmo di IA impiegato per processi decisionali per la sua mancanza di trasparenza, già richiamate da Simoncini⁷¹. Per questa ragione l'intervento legislativo sul punto è auspicabile, al fine di definire un'area di operatività per i sistemi di IA limitata alle sole funzioni sintattiche.

5.1.3. L'uso dell'IA in campo medico

Infine viene in rilievo l'uso di sistemi IA in campo medico, dove numerosi profili dubbi di responsabilità, già in parte sollevati e analizzati dalla giurisprudenza Francese, sorgono in relazione all'impatto che l'uso di questi sistemi può avere per la responsabilità professionale del medico. Anche

qui, come nel caso dell'uso dell'IA nel giudiziario, ci si trova di fronte ad una fattispecie nella quale, una volta introdotto l'output dell'IA come elemento di valutazione del caso, esso inevitabilmente andrà a concorrere con gli altri strumenti d'analisi a disposizione del medico a formare la diagnosi finale. Però, diversamente rispetto al caso dell'uso dell'IA nel giudiziario, verrà qui in rilievo non soltanto l'output dell'IA come elemento valutativo per la diagnosi, ma anche l'uso dell'IA stessa come strumento diagnostico per l'analisi del caso. Risultando così in una sfera di responsabilità ampliata per il medico moderno che dovrà rispondere della valutazione fatta dell'output dell'IA e dell'uso fatto del sistema per la produzione di quel determinato output.

In questo senso, va preliminarmente menzionata la precedenza dell'onere di ripartizione delle responsabilità lungo la catena causale che porta alla generazione dell'output dell'IA, al fine di alleggerire il carico del medico operante. L'AI Act prevede a questo con obbligazioni da porre a carico dello sviluppatore del sistema d'IA (*provider*) e del gestore del sistema (*deployer*)⁷², al fine di garantire che il sistema IA, una volta a disposizione del medico, produca output affidabili e con pochi margini di errore e che nel caso in cui invece accada l'opposto, a risponderne non sia il medico ma lo sviluppatore o il gestore del sistema. In questo quadro già si possono identificare tre differenti livelli di causazione, in parte applicabili anche al caso

semantiche, le quali di contro richiedono necessariamente una parte motivazionale di comprensione affinché il risultato sia valido, proprio come lo richiedono le decisioni giudiziali.

67. Si veda sul punto quanto già detto in nota 23, dove viene richiamato il contributo di BORRUSO 1995, il quale con lungimiranza già intravedeva il possibile campo d'applicazione degli algoritmi nel diritto.

68. Si segnalano inoltre le sentenze della Corte Costituzionale n. 1/1971, n. 139/1982 e n. 367/2004, in controtendenza rispetto all'ordinamento cinese nel quale invece si impiegano sperimentalmente algoritmi di IA per verificare la possibilità di razionalizzare e rendere più efficiente il procedimento decisionale giudiziario, si veda LIU-LIU-LIN 2024.

69. Si veda sul punto ALMADA 2019.

70. Codificato dall'art. 86 dell'AI Act recante norme sul "diritto alla spiegazione dei singoli processi decisionali".

71. SIMONCINI 2019.

72. Entrambe queste figure sono definite dall'art. 3(3-4) dell'AI Act e si riferiscono a due differenti momenti della catena di sviluppo dell'IA. Infatti il *provider* sarà il responsabile dello sviluppo del modello d'IA, ovvero del modello di risposta, mentre il *deployer* sarà colui che svilupperà e gestirà l'applicativo dell'IA, il quale conterrà al suo interno il modello adattato alle esigenze particolari per il quale viene successivamente ottimizzato. Le due figure potranno ovviamente coincidere. Per una differenza tra *AI model* e *AI system* nel quadro dell'AI Act si veda FERNÁNDEZ-LLORCA-GÓMEZ-SÁNCHEZ-MAZZINI 2024.

dell'uso dell'IA nel giudiziario, idonei a costituire una prima teorica catena di responsabilità:

- 1) Responsabilità dello sviluppatore del modello IA (*provider*) per il training dei dati e l'aggiornamento del modello.
- 2) Responsabilità del gestore del sistema IA (*deployer*) per la gestione dell'applicativo.
- 3) Responsabilità del medico decisore per la decisione finale.

Una giustificazione per questa preliminare classificazione dei momenti causali rilevanti nella catena di responsabilità per la decisione medica presa con l'ausilio dell'IA la si rinviene in quanto affermato sul punto da Naik *et al.* "it is the underlying data than the algorithm itself that is to be held responsible. Models can be trained on data which contains human decisions or on data that reflects the second-order effects of social or historical inequities"⁷³. Mentre l'AI Act copre le fattispecie di responsabilità per i primi due livelli della catena causale, l'ultimo, quello della responsabilità del decisore umano, rimane fuori dal paradigma europeo e viene delegato alla legislazione nazionale⁷⁴.

Su quest'ultimo caso, la giurisprudenza Francese fornisce un'importante chiave interpretativa. Lo scenario tipico è quello di una decisione medica influenzata dall'output dell'IA o addirittura messa in discussione da esso: ad esempio, nel caso in cui una diagnosi errata porti a conseguenze

infauste per il paziente e, in retrospettiva, l'IA abbia suggerito un decorso alternativo più favorevole. In questo quadro, messe da parte le questioni sulla correttezza dell'output concernenti i primi due livelli di responsabilità, e quindi assumendo l'esistenza di un output corretto, la questione che viene in rilievo è se l'output dell'IA rappresentante un decorso alternativo favorevole possa legittimare una pronuncia di condanna del medico. Ebbene, la risposta che l'interpretazione della sentenza Francese ci offre pare essere di segno negativo. Questo perché l'output dell'IA, essendo il prodotto di un calcolo probabilistico, rappresenterà tutt'al più "il coefficiente di probabilità espresso dalla legge statistica" e giammai un reale decorso alternativo degli eventi. Questo aspetto duplice della causalità è riconducibile alla distinzione tra causalità scientifica e causalità giuridica per la quale, se la prima considera la validità di una legge in astratto, la seconda valuta la relazione causale nel caso concreto⁷⁵. Per comprendere la rilevanza di questa distinzione, si può richiamare l'esempio formulato da Viganò⁷⁶: se Tizio avvelena Caio con un veleno che causa la morte nel 100% dei casi, ma prima che il veleno faccia effetto Sempronio gli spara uccidendolo, sarà Sempronio ad aver cagionato la morte, non Tizio, nonostante il veleno fosse letale. Questo perché, ai fini giuridici, la *condicio sine qua non* è rappresentata dall'azione che ha effettivamente determinato l'evento nel

73. NAIK-HAMEED-SHETTY *et al.* 2022.

74. Per un quadro completo del funzionamento dell'impianto obbligatorio dell'AI Act in campo medico si veda VAN KOLFSCHOOTEN-VAN OIRSCHOT 2024, che inquadra con chiarezza il rapporto tra i tre livelli di responsabilità comprendenti *provider*, *deployer* e decisore finale. Inoltre ad oggi è ancora dubbio se le norme previste dall'AI Liability Directive, comprendenti l'obbligo di divulgazione delle prove (art. 3) e la presunzione di causalità (art. 4), entreranno effettivamente a far parte degli ordinamenti nazionali al fine di coprire anche il terzo livello di responsabilità.

75. Sul tema si veda BLAIOTTA 2010 che affronta in maniera sistematica il tema della causalità giuridica, comparandola alla causalità scientifica e segnalando che, mentre nella causalità scientifica la nozione di legge scientifica faccia riferimento alla regolarità con la quale un fenomeno si presenta, nel diritto la causalità che rileva ai fini del giudizio è quella che nel caso concreto ha dato origine alla fattispecie oggetto di censura.

76. VIGANÒ 2013: "Riprendendo uno dei tanti esempi di scuola discussi in letteratura, pensiamo a una ipotetica legge scientifica che asserisca che il morso del serpente mocassino è sempre letale per la vittima, la quale invariabilmente decede qualche ora dopo il morso, senza alcuna possibilità di essere salvata mediante la somministrazione di un siero o di altro presidio terapeutico. Se – prima che il veleno del serpente, introdotto furtivamente da A nel letto di B, abbia sortito il proprio effetto letale – B viene attinto da un colpo di pistola sparatogli da C, è evidente che la morte di B dovrà essere attribuita, in base a una considerazione *ex post*, a un decorso causale diverso rispetto al morso del serpente (e dunque alla condotta di A), malgrado la natura universale della legge scientifica che assicura, in una prospettiva generalizzante ed *ex ante*, che tutti coloro che vengono morsi dal serpente sono destinati a sicura morte".

caso concreto, e non da quella che in astratto ha il maggior coefficiente di probabilità nella causazione dell'evento.

Poiché l'output dell'IA rappresenta un'elaborazione statistica *ex ante*, puramente teorica e ipotetica, senza prendere in considerazione il reale decorso causale degli eventi accertato *ex post*, non può essere utilizzato come base per imputare la responsabilità al medico. Legittimare contestazioni della decisione medica sulla base di valutazioni alternative offerte da sistemi IA comporterebbe un'ingiusta espansione della sfera di responsabilità del medico, attribuendogli un obbligo di conformità a una previsione statistica che, per sua natura, non è equivalente a un'analisi fattuale e causale degli eventi effettivamente accaduti. Certamente la sola presenza di una previsione diagnostica da parte dell'IA contribuirà non poco allo sviluppo causale degli eventi e influirà, anche se tacitamente, sulla decisione medica. Per questo motivo sarebbe opportuna la previsione di obblighi di motivazione a presidio della libertà del medico che, se rispettati, possano scagionarlo nel caso di esito infuorto quando non ha seguito la raccomandazione potenzialmente positiva dell'IA. In ogni caso il giudizio di responsabilità va condotto sulla ragionevolezza della motivazione fornita dal medico e sull'influenza della sua decisione nel caso concreto, prendendo in considerazione la raccomandazione dell'IA solo in relazione ad essa e non in relazione al potenziale decorso causale alternativo, puramente teorico e incerto.

Contemporaneamente sul punto è bene anche ribadire quanto già affermato in tema di responsabilità del giudice che si avvalga di output di IA per la valutazione giudiziale, ovvero che la raccomandazione dell'IA non può essere considerata come vincolante né come unica *ratio* per il giudizio di responsabilità⁷⁷. Questo al fine di garantire entrambi i casi, quello positivo di tutela del medico diligente che abbia commesso un errore in buona fede, così come quello negativo del medico negligente che abbia basato la sua diagnosi unicamente sull'output dell'IA.

6. Conclusioni

L'analisi condotta evidenzia come la questione dell'autonomia dell'intelligenza artificiale non possa essere affrontata esclusivamente in termini tecnici o definitivi, ma impone una riflessione giuridica più ampia, centrata sulla natura e sul valore degli output generati da tali sistemi. Essi contribuiranno non poco alla determinazione in concreto di nuovi e autonomi rapporti di diritto, a prescindere da un loro riconoscimento formale. Come già visto nei casi dell'applicazione di IA in ambito medico e giuridico, ci si trova di fronte a contesti nei quali, una volta introdotto l'output dell'IA, esso inevitabilmente andrà a contribuire allo sviluppo causale degli eventi, influenzando sul processo decisionale umano e sulla costituzione o modificazione dei rapporti socio-giuridici tra i soggetti coinvolti.

Questa è una realtà inevitabile che il progresso tecnologico oggi in atto comporta, dove l'introduzione di algoritmi autonomi senz'altro contribuirà a rendere ancora più complessi e intricati i rapporti sociali nei nostri ordinamenti. Ciononostante, esiste una strada per il mantenimento di forme di indipendenza decisionale senza che essa comporti un maggiore carico per l'essere umano. Tale transizione sembra inevitabilmente implicare una rinuncia, da parte dell'essere umano, al controllo diretto su una serie di operazioni che in passato richiedevano il suo intervento e che oggi sono affidate ad algoritmi dotati di autonomia operativa. A questa perdita di controllo non si può rispondere con maggiori responsabilità per l'essere umano, ma piuttosto, ciò che appare oggi opportuno è la sostituzione di antiche forme di controllo con nuovi criteri d'imputazione della responsabilità basati sulla fiducia.

Il riconoscimento della natura probabilistica degli output dell'IA, prodotti da mere inferenze probabilistiche, prive di un contenuto esplicativo pienamente causale, conduce a escludere la possibilità di attribuire loro rilevanza giuridica autonoma se sciolta dal rapporto di dipendenza con l'agire umano. Per questa motivazione la responsabilità umana permane, anche se in una forma

77. È utile sul punto citare RUBEL-PHAM-CASTRO 2019, che con il termine *agency laundering* hanno ben inquadrato questa tendenza a voler "riciclare" le proprie azioni mediante l'uso di algoritmi di intelligenza artificiale, pratica che il diritto non può legittimare e che le teorie della responsabilità oggettiva e della personalità elettronica finirebbero col consentire.

diversa rispetto al controllo diretto sulla produzione dell'output. L'essere umano rimane responsabile per l'affidabilità dell'output prodotto dal sistema di IA. Questa forma di responsabilità sorge al fine di poter garantire tutti coloro che poi, nelle fasi conclusive della catena di responsabilità, potranno interagire con gli output prodotti dal sistema.

Questo nuovo paradigma di responsabilità, non basato su prevedibilità e controllo, ma piuttosto su un onere di affidabilità che, rivolgendosi alla società nel suo insieme, è idoneo a rendere imputabile l'individuo che ha contribuito alla creazione dell'output dell'IA, può aprire uno scenario inedito dove la sfera di responsabilità individuale risulta ampliata e al contempo alleggerita. L'ampliamento deriva dallo svincolarsi di queste forme di responsabilità dai criteri d'imputazione tradizionali di prevedibilità e controllo, per il quale un individuo può essere chiamato a rispondere di qualcosa anche dopo molto tempo e indipendentemente da un rapporto di causazione di tipo diretto. Contemporaneamente si verifica un alleggerimento

del peso della responsabilità, laddove all'individuo essa non potrà essere addossata per l'output dell'IA con la formula della colpa per la performance negligente, oggettivamente compiuta da un altro attore, il sistema IA, ma piuttosto all'individuo che si avvale dell'output dell'IA potranno essere richiesti oneri giustificativi e di trasparenza idonei a spiegare il suo rapporto con esso e la sussistenza della sua buona fede.

Questa descrizione sintetica di un nuovo paradigma di responsabilità, capace di superare i confini della tradizionale imputazione colposa, rappresenta oggi solamente un accenno di soluzione. Ulteriori ricerche su questo fronte si rendono necessarie. Tuttavia, quanto emerso delinea una direzione inedita per l'evoluzione del diritto, sollecitata dall'avvento dell'intelligenza artificiale, dove, a fronte di un ampliamento della sfera di responsabilità, può accompagnarsi la realizzazione dell'antico sogno di un suo alleggerimento, grazie alla delega a sistemi d'intelligenza artificiale di numerose attività una volta compiute dall'essere umano.

Riferimenti bibliografici

- M. ALMADA (2025), *What Is an Artificial Intelligence System, Really? Notes on the European Commission's Guidelines on Article 3 (1) of the AI Act*, in "Journal of AI Law and Regulation", vol. 2, n. 1, 2025
- M. ALMADA (2019), *Human intervention in automated decision-making: Toward the construction of contestable systems*, in "Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law", 2019
- Y. BATHAEE (2018), *The artificial intelligence black box and the failure of intent and causation*, in "Harvard Journal of Law & Technology", vol. 31, 2018
- L. BELLI, Y. CURZI, W.B. GASPARI (2023), *AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience*, in "Computer Law and Security Review", vol. 48, 2023
- E.M. BENDER, T. GEBRU, A. McMILLAN-MAJOR, S. SHMITCHELL (2021), *On the dangers of stochastic parrots: Can language models be too big?*, in "Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency", 2021
- R. BLAIOTTA (2010), *Causalità giuridica*, Giappichelli, 2010
- E. BÖRGER, E. GRÄDEL, Y. GUREVICH (2001), *The classical decision problem*, Springer, 2001
- R. BORRUSO (2002), *Discrezionalità e autonomia del giudice: il contributo dell'informatica giuridica*, in "Il Diritto dell'informazione e dell'informatica", 2002, n. 2
- R. BORRUSO (1995), *Il computer, il diritto romano e il giudice*, in "Informatica e diritto", 1995, n. 2
- L. BRENNAN (2023), *AI ethical compliance is undecidable*, in "Hastings Science & Technology Law Journal", vol. 14, 2023, n. 2

- S. BUBECK, V. CHANDRASEKARAN, R. ELDAN et al. (2023), *Sparks of Artificial General Intelligence: Early experiments with GPT-4*, arXiv preprint, arXiv:2303.12712
- G. CARLONI, A. BERTI, S. COLANTONIO (2023), *The role of causality in explainable artificial intelligence*, arXiv preprint, arXiv:2309.09901
- I. CARNAT (2024), *Addressing the risks of generative AI for the judiciary: The accountability framework(s) under the EU AI Act*, in "Computer Law & Security Review", vol. 55, 2024, 106067
- R. DESHPANDE, K. KAMATH (2020), *Patentability of inventions created by AI – the DABUS claims from an Indian perspective*, in "Journal of Intellectual Property Law & Practice", vol. 15, 2020, n. 11
- D. FERNÁNDEZ-LLORCA, E. GÓMEZ, I. SÁNCHEZ, G. MAZZINI (2024), *An interdisciplinary account of the terminological choices by EU policymakers ahead of the final agreement on the AI Act*, in "Artificial Intelligence and Law", 2024
- L. FLORIDI (2025), *AI as Agency without Intelligence: On Artificial Intelligence as a New Form of Artificial Agency and the Multiple Realisability of Agency Thesis*, in "Philosophy and Technology" vol. 38, 2025
- L. FLORIDI (2023), *AI as agency without intelligence: on ChatGPT, large language models, and other generative models*, in "Philosophy & Technology", vol. 36, 2023
- A.S. FOKAS (2023), *Can artificial intelligence reach human thought?*, in "PNAS Nexus", vol. 2, 2023, n. 12
- R. GUIDOTTI, A. MONREALE, S. RUGGIERI et al. (2018), *A survey of methods for explaining black box models*, in "ACM Computing Surveys (CSUR)", vol. 51, 2018, n. 5
- P. HACKER (2024), *Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence: Complementary impact assessment*, Study EPRS – European Parliamentary Research Service, 2024
- G. HALLEVY (2010), *The criminal liability of artificial intelligence entities – from science fiction to legal social control*, in "Akron Intellectual Property Journal", vol. 4, 2010
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2020), *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, European Commission, 2020
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019-A), *Ethics Guidelines for Trustworthy AI*, European Commission, 2019
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019-B), *A Definition of AI: Main Capabilities and Disciplines*, European Commission, 2019
- Y. LECUN (2022), *A Path Towards Autonomous Machine Intelligence*, Version 0.9.2, in openreview.net, 2022
- Z. LIU, S. LIU, Y. LIN (2024), *Building Smart Courts Through Large Legal Language Models? Experience from China*, in "AI from the Global Majority", 2024
- R. MATULIONYTE (2022), *AI as an Inventor: Has the Federal Court of Australia Erred in DABUS?*, in "Journal of Intellectual Property, Information Technology and Electronic Commerce Law", vol. 13, 2022
- N. NAIK, B.M.Z. HAMEED, D.K. SHETTY et al. (2022), *Legal and ethical consideration in artificial intelligence in healthcare: who takes responsibility?*, in "Frontiers in Surgery", vol. 9, 2022, 862322
- S. NYHOLM (2018), *Attributing agency to automated systems: Reflections on human-robot collaborations and responsibility-loci*, in "Science and Engineering Ethics", vol. 24, 2018, n. 4
- OPENAI (2023), *GPT-4 Technical Report*, arXiv preprint, arXiv:2303.08774
- M. PIETRANGELO, L. NANNIPIERI (2023), *Intelligenza artificiale e pubbliche amministrazioni, tra incertezze definitorie, usi disomogenei e giudici supplenti*, in "Ital-IA 2023: 3rd National Conference on Artificial Intelligence", Pisa, 29-31 maggio 2023

- M.T. RIBEIRO, S. SINGH, C. GUESTRIN (2016), *Why should I trust you?: Explaining the predictions of any classifier*, in "Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining", ACM, 2016
- A. ROLI, J. JAEGER, S.A. KAUFFMAN (2022), *How organisms come to know the world: Fundamental limits on artificial general intelligence*, in "Frontiers in Ecology and Evolution", vol. 9, 2022, 806283
- A. RUBEL, A. PHAM, C. CASTRO (2019), *Agency Laundering and Algorithmic Decision Systems*, in "Information in Contemporary Society: Proceedings of the 14th International Conference, iConference 2019", Springer, 2019
- S.J. RUSSELL, P. NORVIG (2010), *Artificial Intelligence: A Modern Approach*, Pearson Education, 2010
- G. SARTOR, A. OMICINI (2016), *The autonomy of technological systems and responsibilities for their use*, in "Autonomous Weapon Systems. Law, Ethics, Policy", Cambridge University Press, 2016
- J.R. SEARLE (1980), *Minds, brains, and programs*, in "Behavioral and Brain Sciences", vol. 3, 1980
- M. SHANAHAN, M. CROSBY, B. BEYRET, L. CHEKE (2020), *Artificial intelligence and the common sense of animals*, in "Trends in Cognitive Sciences", vol. 24, 2020, n. 11
- A. SIMONCINI (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal", 2019
- L.B. SOLUM (2020), *Legal personhood for artificial intelligences*, in W. Wallach, P. Asaro (eds.), "Machine Ethics and Robot Ethics", Routledge, 2020
- G. TADDEI ELMI, S. MARCHIAFAVA (2024), *Sviluppi recenti in tema di Intelligenza Artificiale e diritto (gennaio-aprile 2024)*, in "Rivista italiana di informatica e diritto", 2024, n. 1
- G. TADDEI ELMI, S. MARCHIAFAVA (2023-A), *Sviluppi recenti in tema di Intelligenza Artificiale e diritto (novembre-dicembre 2023)*, in "Rivista italiana di informatica e diritto", 2023, n. 2
- G. TADDEI ELMI, S. MARCHIAFAVA (2023-B), *Sviluppi recenti in tema di Intelligenza Artificiale e diritto (giugno-agosto 2023)*, in "Rivista italiana di informatica e diritto", 2023, n. 2
- G. TADDEI ELMI, S. MARCHIAFAVA (2023-C), *Sviluppi recenti in tema di Intelligenza Artificiale e diritto (gennaio-aprile 2023)*, in "Rivista italiana di informatica e diritto", 2023, n. 1
- G. TADDEI ELMI, S. MARCHIAFAVA (2022), *Sviluppi recenti in tema di Intelligenza Artificiale e diritto: Una rassegna di legislazione, giurisprudenza e dottrina*, in "Rivista italiana di informatica e diritto", 2022, n. 2
- A.M. TURING (1950), *Computing machinery and intelligence*, in "Mind", vol. 59, 1950, n. 236
- A.M. TURING (1936), *On computable numbers, with an application to the entscheidungsproblem*, in "Journal of Math", vol. 58, 1936
- H. VAN KOLFSCHOOTEN, J. VAN OIRSCHOT (2024), *The EU Artificial Intelligence Act (2024): implications for healthcare*, in "Health Policy", vol. 149, 2024, 105152
- A. VASWANI, N. SHAZEER, N. PARMAR et al. (2017), *Attention is all you need*, in "Advances in Neural Information Processing Systems", vol. 30, 2017
- F. VIGANÒ (2013), *Il rapporto di causalità nella giurisprudenza penale a dieci anni dalla sentenza Franzese*, in "Diritto penale contemporaneo", vol. 2, 2013
- X. YING (2019), *An overview of overfitting and its solutions*, in "Journal of Physics: Conference Series", vol. 1168, 2019, 022022



MAURIZIO DI MASI

Privacy e protezione dei dati mentali

L'articolo esamina il problema della tutela giuridica dei dati mentali negli ecosistemi neuro-digitali contemporanei, soffermandosi sulle inferenze algoritmiche relative a emozioni, stati cognitivi e vulnerabilità psicologiche. Si sostiene che le categorie attuali della protezione dei dati personali, incluse quelle dei dati particolari ai sensi del GDPR, risultino strutturalmente inadeguate a intercettare i rischi derivanti dalla profilazione psico-affettiva inferenziale, nella quale la particolarità dell'informazione emerge dall'output algoritmico più che dal dato di input. Pur riconoscendo il contributo dell'approccio risk-based del Regolamento (UE) 2024/1689 sull'intelligenza artificiale, l'analisi ne evidenzia i limiti rispetto agli effetti cumulativi e sistemici della lettura tecnologicamente mediata della sfera interiore. In una prospettiva critica e comparata, il contributo discute la proposta di una categoria autonoma di "dati mentali", mettendone in luce le ambivalenze regolatorie e il rischio di una normalizzazione giuridica dell'intrusione cognitiva. Si argomenta, in conclusione, che la posta normativa decisiva risieda nelle regole di fondo del diritto privato – in particolare contratti, proprietà e responsabilità – che strutturano l'accesso alla sfera interiore della persona e contribuiscono alla redistribuzione del potere informazionale negli ambienti digitali.

Dati mentali – Poteri privati – Dignità – Intelligenza artificiale – AI Act

Privacy and mental data protection

This article examines the legal status of mental data within contemporary neuro-digital ecosystems, focusing on algorithmic inferences about emotions, cognition and psychological vulnerability. It argues that existing EU data protection categories, including special categories of data under the GDPR, are structurally ill-equipped to capture the risks posed by inferred mental states. While acknowledging the contribution of the AI Act's risk-based approach, the analysis highlights its limited capacity to address the cumulative and systemic effects of psychological profiling. Through a critical and comparative perspective, the article assesses the proposal for an autonomous category of mental data and exposes its ambivalent regulatory effects. It ultimately contends that the core normative stakes lie in the background rules of private law – contracts, property, and liability – which silently structure access to the inner sphere of the person and normalize new forms of cognitive power.

Mental data – Private Powers – Dignity – Artificial Intelligence – AI Act

L'Autore è professore a contratto di Diritto del turismo presso il Dipartimento di Giurisprudenza dell'Università Roma Tre e professore a contratto di Istituzioni di diritto sportivo presso il Corso di Laurea in Scienze Motorie e Sportive, Università di Perugia

Il presente contributo sviluppa la relazione presentata al VI Mega Congresso Mundial "Robots Multifuncionales, Ciberseguridad Avanzada, Asistentes Virtuales y Derechos Fundamentales", 26 novembre 2025, organizzato da IgiTo (Istituto giuridico internazionale di Torino) – Escuela Interdisciplinar de Derechos Fundamentales Praeminentia Iustitia (Perù) – Universidade de Caxias do Sul (Brasil) – Universidade de Itaúna (Brasil)

SOMMARIO: 1. Oltre i dati “particolari”, verso le “informazioni neurali”. – 1.1. Diritto ed economia di fronte all’intenzione. – 2. I limiti delle attuali categorie particolari di dati personali. – 3. Le garanzie del GDPR tra “tecnica di libertà” e insufficienza strutturale. – 4. Il contributo del Regolamento (UE) 2024/1689. – 5. Per una categoria autonoma di “dati mentali”. – 5.1. Suggerimenti comparatistiche: California Consumer Privacy Act. – 5.2. Quale normalizzazione per i dati mentali? – 6. Brevi conclusioni: dati mentali e diritto privato.

*“Fool do not boast,
Thou canst not touch the freedom of my minde
With all thy charms, although this corporal rinde
Thou haste immanacld, while Heav’n sees good”.*

John Milton, *Comus*

1. Oltre i dati “particolari”, verso le “informazioni neurali”

Nel contesto degli ecosistemi digitali e neurotecnologici contemporanei, i dati psico-affettivi – ossia le informazioni che descrivono o consentono di inferire stati emotivi, motivazionali e cognitivi, nonché tratti della personalità – costituiscono una dimensione informativa qualitativamente distinta rispetto ai dati personali “tradizionali”. Tali dati, infatti, non si limitano a rappresentare condizioni oggettive di salute, né si collocano agevolmente nelle categorie classiche dei dati sanitari o biometrici. Essi descrivono, piuttosto, la trama dinamica della vita interiore, incidendo direttamente sulla capacità dell’individuo di autodeterminarsi e sulla sua autopercezione. Proprio per questa ragione, la tutela della dignità umana non può essere affidata

a garanzie settoriali o frammentarie. Suddetta tutela richiede – secondo l’analisi tracciata da Stefano Rodotà¹ – una *strategia giuridica integrata*, capace di mobilitare strumenti sia di diritto pubblico sia di diritto privato, al fine di assicurare che la sfera interiore della persona sia protetta non solo contro gli abusi del potere istituzionale, ma anche contro pratiche informative asimmetriche e forme di influenza tecnologicamente mediate esercitate da attori privati, dalle c.d. autorità private².

Le neurotecnologie attuali e le c.d. *Big Tech*³ rendono tangibile tale necessità. Da un lato, dispositivi invasivi come la stimolazione cerebrale profonda o le interfacce cervello-macchina impiantabili consentono la registrazione e la modulazione dell’attività neurale con un elevato grado di granularità⁴. Dall’altro, tecniche più o meno invasive (elettroencefalografia – EEG – di uso consumer,

1. A partire da RODOTÀ 1973.

2. BIANCA 1977.

3. Cfr. RESTA 2023, p. 1008 ss.; VETTORI 2022, p. 829 ss.; FERRARESE 2022; PARDOLESI 2021, p. 941 ss. Per una prospettiva giuspubblicistica si veda POLLICINO 2023, p. 410 ss.; BETZU 2021, p. 739 ss.; TORCHIA 2024, p. 15 ss.; RUOTOLO 2024, p. 46 ss.

4. La granularità indica il livello di dettaglio con cui un’informazione, un dato, un fenomeno o una regolazione viene scomposto e rappresentato. In termini generali, più un dato è granulare, più è analitico e fine; meno è granulare, più è aggregato e sintetico.

neurofeedback, sistemi di stimolazione cerebrale transcranica, interfacce cervello-computer e persino interfacce cervello-cervello) permettono un accesso esterno ai correlati neurali di emozioni, attenzione, fatica, ansia, motivazione e persino a forme rudimentali di “decodifica” di modelli cognitivi. Tutti dati fortemente appetibili per il mercato.

A ciò si aggiunge la capacità ormai matura dei sistemi di intelligenza artificiale di estrarre indicatori psico-affettivi non solo dai dati neurali in senso stretto, ma anche da segnali “deboli”: micro-variazioni nei modelli vocali, tempi di reazione, stili linguistici, modalità di interazione negli ambienti digitali e abitudini comportamentali on-line.

Peraltro, anche in recenti studi del *Science and Technology Options Assessment* (STOA), promossi dal Parlamento europeo, emerge come tali strumenti siano sempre più utilizzati al di fuori dei contesti clinici – nei luoghi di lavoro, negli ambienti educativi e negli ecosistemi dell'intrattenimento – con finalità di monitoraggio delle prestazioni, valutazione della concentrazione, prevenzione del *burnout* o personalizzazione dei contenuti⁵.

In questo quadro, allora, i dati mentali, psico-affettivi, assumono una rilevanza giuridica di pregnanza costituzionale, toccando il nucleo della dignità umana ed esponendo gli individui a nuove forme di lettura e di governo della soggettività che non riguardano soltanto ciò che essi fanno, ma anche come si sentono e come pensano⁶. Ciò che è in gioco non si limita più alla privacy come fin qui l'abbiamo conosciuta e teorizzata⁷, ma si estende all'accesso al foro interno della persona, con i conseguenti rischi di profilazione psicologica invasiva e difficilmente confutabile.

1.1. Diritto ed economia di fronte all'intenzione

Appare, pertanto, riduttivo considerare l'intelligenza artificiale – e, con essa, le pratiche di estrazione e inferenza degli stati mentali – come un fenomeno

puramente tecnico, al quale il diritto reagirebbe *ex post* in funzione correttiva. Come osservato da Giovanni Marini, difatti, il diritto ha svolto un ruolo attivo e anticipatorio nel rendere possibile l'attuale configurazione del potere algoritmico, attraverso un intreccio di clausole contrattuali, regimi di segretezza, tecniche proprietarie e dispositivi regolatori che hanno progressivamente *naturalizzato* l'appropriazione dei dati come risorsa economica⁸. In questo senso, l'accesso tecnologicamente mediato alla sfera interiore della persona non rappresenta una deviazione patologica del sistema giuridico, ma una sua conseguenza strutturale.

Un'ulteriore conferma di questa trasformazione in atto proviene da un recentissimo lavoro pubblicato dal *Leverhulme Centre for the Future of Intelligence* dell'Università di Cambridge, che descrive il passaggio dalla tradizionale “economia dell'attenzione” a quella che gli autori definiscono “economia dell'intenzione”⁹. La diffusione pervasiva degli assistenti virtuali consente alle piattaforme di anticipare – e dunque di sfruttare commercialmente – le intenzioni di acquisto degli utenti ancor prima che tali intenzioni entrino nella consapevolezza riflessiva degli stessi. Questa dinamica illustra con particolare chiarezza come il fulcro dell'estrazione informativa si stia spostando dal comportamento osservabile alla ricostruzione algoritmica di stati mentali pre-decisionali, rendendo la sfera interiore progressivamente più leggibile e, in una certa misura, governabile da attori economici tecnologicamente potenziati.

Risulta particolarmente interessante per il giurista, anche nel caso dei dati mentali, applicare il metodo critico di Duncan Kennedy, il quale – come noto – mira a individuare le forme di redistribuzione del potere prodotte dal diritto e il ruolo che le “regole di sfondo” svolgono nel modellare tali effetti redistributivi¹⁰. Da questo punto di vista, invero, l'immersione e il trattamento dei dati psico-affettivi non possono essere compresi esclusivamente

5. MAIA DE OLIVEIRA WOOD-BERGER-JARKE et al. 2024.

6. Cfr. MARINI 2024, p. 3 ss.

7. Cfr. RODOTÀ 1973; RODOTÀ 1991, p. 521 ss.; ALPA 1979, p. 65 ss.; ALPA 1985, p. 55 ss., in particolare p. 66 ss.; MARINI 2013, p. 250 ss.

8. MARINI 2024.

9. CHAUDHARY-PENN 2024.

10. Cfr. almeno KENNEDY 1991.

mediante categorie dogmatiche. Essi devono essere collocati all'interno della più ampia architettura del potere informativo che struttura chi beneficia dell'inferenza sugli stati mentali e chi, invece, ne subisce gli effetti collaterali.

Nell'attuale ambiente neuro-digitale, allora, tali dati diventano strumenti di vantaggio asimmetrico: coloro che dispongono dell'infrastruttura tecnologica e della capacità economica necessarie per estrarre, inferire e operazionalizzare pattern affettivi e cognitivi (i.e., le *Big Tech*) acquisiscono una leva decisiva sugli individui i cui stati interiori diventano leggibili¹¹.

I "vincitori" in questa configurazione includono i fornitori di tecnologie, gli operatori di piattaforme, i datori di lavoro e le assicurazioni, ossia soggetti in grado di convertire segnali minimi in indicatori di produttività, conformità o rischio psicologico. I "perdenti" sono le persone che, spesso senza reali possibilità di contestazione o di opt-out, diventano oggetto di una continua sorveglianza emotiva e cognitiva in contesti che non sono né clinici né terapeuticamente giustificati.

Tale asimmetria è sostenuta da una fitta rete di *background rules*: il controllo proprietario sulle infrastrutture digitali, l'opacità algoritmica protetta dal segreto industriale, la diffusa dipendenza socio-economica dai servizi digitali e la normalizzazione culturale della profilazione affettiva in nome dell'ottimizzazione, della sicurezza o del benessere. All'interno di questa architettura, i dati mentali non emergono semplicemente come una nuova categoria informativa, ma si rivelano come il prodotto di assetti strutturali di potere preesistenti, attraverso i quali la mente umana diventa un terreno di estrazione, valutazione e governo.

2. I limiti delle attuali categorie particolari di dati personali

Come noto nel GDPR, l'ordinamento giuridico europeo riconosce una categoria di dati dotati di

una tutela particolarmente rafforzata – i c.d. "dati sensibili", oggi definiti come "categorie particolari di dati personali" (art. 9 GDPR) – che comprende, tra l'altro, i dati relativi alla salute, i dati genetici e biometrici, le opinioni politiche, le convinzioni religiose e l'orientamento sessuale. I dati psico-affettivi possono rientrare in tale categoria nella misura in cui rivelino condizioni patologiche o siano suscettibili nella nozione ampia di "dati relativi alla salute"¹². Tuttavia, la maggior parte delle informazioni che descrivono l'umore, i livelli di attenzione, le disposizioni comportamentali o le vulnerabilità emotive non è né espressamente classificata né costantemente trattata come dato sanitario¹³.

Il problema non è tanto definitorio, quanto strutturale. Le categorie particolari di dati personali sono state costruite per situazioni in cui l'oggetto del trattamento è un'informazione acquisita e trattata come tale. I dati psico-affettivi, al contrario, sono spesso il risultato di inferenze algoritmiche. La loro "sensibilità" non risiede *ex ante* nella natura dei dati di input (una EEG, un *clickstream*, una registrazione vocale), bensì nella qualità dell'output, quali una classificazione della personalità, una stima del rischio depressivo, una previsione della propensione all'errore o alla devianza.

Sia la letteratura sui *neurorights*¹⁴ sia le ricerche STOA evidenziano come questo spostamento dall'oggetto "dato" al processo inferenziale sia catturato in modo insufficiente dal diritto positivo¹⁵. Il legislatore europeo ha concepito una protezione rafforzata per situazioni in cui la qualità particolare dell'informazione è immediatamente riconoscibile (ad esempio, i dati genetici o le cartelle cliniche). Ma quando un algoritmo, combinando segnali frammentari, genera un profilo psicologico che attribuisce all'individuo – ad esempio – ansia latente, vulnerabilità alla dipendenza o una soglia di attenzione ridotta, la tutela prevista per le categorie particolari di dati personali può intervenire troppo tardi e in modo inadeguato.

11. Parla di egemonia computazionale dei poteri privati FALCONE 2023.

12. Si rinvia a DI MASI 2021, p. 1233 ss. Ma diffusamente cfr. la completa monografia di CORSO 2025-A; nonché i contributi raccolti in CATANZARITI 2025, p. 4 ss.

13. IENCA-MALGIERI 2022.

14. Cfr. nella letteratura italiana almeno IENCA 2019, p. 52 ss.; AA.VV. 2021; POLLICINO 2021, p. 165 ss.; MOLLO 2021, p. 200 ss.; CIRILLO 2023, p. 666 ss.

15. MAIA DE OLIVEIRA WOOD-BERGER-JARKE et al. 2024.

Si crea così una zona grigia, in cui i dati di input non sono formalmente “particolari”, ma lo diventano in virtù del processo interpretativo cui sono sottoposti. È proprio all'interno di questo spazio interstiziale che emerge il rischio della profilazione psicologica invasiva, dato che gli individui vengono classificati e gestiti sulla base di valutazioni psico-affettive che non rientrano in modo univoco nelle categorie particolari di dati personali e che, pertanto, sfuggono – almeno in parte – alle garanzie più stringenti.

Al di là di queste tensioni fra formante dottrinale e formante legislativo¹⁶, sia la Convenzione europea dei diritti dell'uomo sia la Carta dei diritti fondamentali dell'Unione europea offrono ancoraggi costituzionali impliciti ma solidi per comprendere perché i dati psico-affettivi inferiti sollevino preoccupazioni che vanno ben oltre le categorie tradizionali della protezione dei dati. La Corte EDU ha interpretato l'art. 8 CEDU come comprensivo della tutela della dignità umana, dell'integrità psicologica e della capacità dell'individuo di svilupparsi autonomamente, estendendo così la nozione di vita privata fino a ricomprendere il *forum internum*, ossia la sfera interiore dell'identità, delle emozioni e delle convinzioni¹⁷. Analogamente, gli artt. 1, 3, 7 e 8 della Carta dei diritti fondamentali dell'Ue articolano una concezione della dignità che implica autodeterminazione cognitiva e decisionale, proteggendo gli individui da forme di interferenza tecnologica idonee a manipolare o a rendere leggibili i loro stati interni¹⁸.

Come ha autorevolmente sostenuto Stefano Rodotà, gli ambienti tecnologici contemporanei rimodellano progressivamente le condizioni di costruzione dell'identità, imponendo agli ordinamenti giuridici di riaffermare il primato della persona e di preservare l'integrità della dignità umana contro forme di espropriazione della soggettività rese possibili da infrastrutture digitali e macchine¹⁹. La “zona grigia” prodotta dall'inferenza algoritmica non rappresenta, allora, un semplice difetto di classificazione, bensì uno spazio di esercizio del potere informazionale, un potenziale *vulnus* all'impegno costituzionale europeo a tutela della dignità umana e dell'autodeterminazione della persona²⁰. È in questo spazio che la mente diventa conoscibile senza essere formalmente protetta, e governabile senza essere dichiarata disponibile. Il diritto, nel non vedere l'inferenza come problema autonomo, finisce così per accompagnare – più che contrastare – la trasformazione della sfera interiore in oggetto di decisione esterna.

3. Le garanzie del GDPR tra “tecnica di libertà” e insufficienza strutturale

Il GDPR rimane, per utilizzare la formulazione di Rodotà, una “tecnica di libertà”²¹, vale a dire un insieme di strumenti giuridici – si pensi ad esempio alla trasparenza, alla minimizzazione o ai diritti dell'interessato – concepiti per restituire potere agli individui rispetto alle attività di trattamento che li riguardano. Tuttavia, l'applicazione di tali garanzie ai dati psico-affettivi rivela limiti strutturali che non possono essere ignorati.

16. Sui formanti del diritto cfr. SACCO 1991.

17. Diffusamente cfr. MARINI 2013.

18. Per l'ampia interpretazione dei dati personali data dalla Corte di Giustizia UE vedi Cort. Giust., 20 dicembre 2017, C-434/16, *Peter Nowak v. Data Protection Commissioner*, par. 34.

19. RODOTÀ 2020.

20. Puntuali le osservazioni di STANZIONE 2021 pp. 15-16, il quale sottolinea come “[n]essun esercizio di diritto o libertà potrebbe, infatti, mai dirsi tale se realizzato per effetto del condizionamento, anche soltanto indiretto o parziale, da parte delle neurotecnologie sul processo cognitivo. Né, del resto, realmente libera potrebbe mai ritenersi alcuna scelta o condotta realizzata nel timore della trasparenza, della leggibilità, financo della predittività dei propri pensieri, delle proprie intenzioni, delle proprie intime convinzioni, appunto. Se, dunque, l'*habeas corpus*, nel proteggere fin nella sua corporeità la persona da atti coercitivi, ha rappresentato il fondamento dello Stato di diritto e l'*habeas data* – come diritto di autodeterminazione informativa – ha costituito il baricentro della tutela della persona nella società dell'informazione, l'*habeas mentem* dovrebbe allora rappresentare il fulcro di veri e propri neurodiritti”.

21. RODOTÀ 1973.

La trasparenza, ad esempio, presuppone che l'interessato sia informato circa le finalità e le modalità del trattamento. Nel caso dei dati mentali, ciò richiederebbe non solo l'informazione sull'esistenza del trattamento, ma anche una descrizione intelligibile della logica inferenziale che conduce dalla materia grezza (segnali neurali, dati comportamentali) all'output psicologico (ad esempio, "livello di stress", "profilo emotivo"). Nella pratica, tale condizione è raramente soddisfatta. Gli algoritmi impiegati sono complessi, protetti dal segreto industriale e spesso non pienamente decifrabili nemmeno dai loro sviluppatori. La trasparenza rischia così di degenerare in un simulacro informativo: l'interessato sa che "esiste un algoritmo", ma non comprende realmente che cosa esso inferisca né quale sia il margine di errore coinvolto.

Questa difficoltà non è contingente, ma riflette un limite più profondo dell'impianto concettuale della *data protection*. Come ha messo in luce Giovanni Marini, difatti, la narrazione del consenso e del controllo individuale delle informazioni tende a occultare il fatto che le architetture digitali contemporanee sono progettate per orientare le scelte prima ancora che esse si formino, producendo forme pervasive di *hypernudge* che operano a un livello antecedente rispetto alla decisione consapevole²². Applicata ai dati mentali, tale impostazione rischia di risultare particolarmente inadeguata, poiché la lesione dell'autodeterminazione non si manifesta tanto nel momento del trattamento dei dati a cui si presta il consenso, quanto nella strutturazione invisibile dell'ambiente cognitivo ed emotivo entro cui il soggetto è chiamato ad agire. In questo quadro, il consenso appare non solo insufficiente, ma concettualmente tardivo.

Si pensi, ancora, al principio di minimizzazione dei dati, che impone di raccogliere solo le informazioni necessarie rispetto alle finalità dichiarate²³. Tuttavia, quando tali finalità sono estremamente ampie – "migliorare l'esperienza dell'utente", "ottimizzare le prestazioni", "prevenire rischi per la

salute mentale" – il perimetro della necessità tende a espandersi indefinitamente, soprattutto laddove l'accesso a segnali psico-affettivi accresca le capacità predittive e classificatorie. Anche in questo caso, l'architettura originaria del GDPR, pensata per operazioni di trattamento relativamente stabili e finalità determinate, fatica a contenere pratiche estrattive fondate su correlazioni statistiche e apprendimento automatico²⁴.

Quanto ai diritti dell'interessato (accesso, rettifica, cancellazione, opposizione, limitazione, ecc.), essi presuppongono la possibilità di individuare, isolare e correggere l'informazione oggetto di trattamento. Nel caso dei dati mentali inferiti, tuttavia, ciò che dovrebbe essere "rettificato" è spesso un giudizio probabilistico ("alto rischio di *burnout*", "probabile tendenza impulsiva", ecc.), fondato su modelli opachi e dinamicamente aggiornati. Né il GDPR né il Regolamento sull'intelligenza artificiale (Regolamento (UE) 2024/1689²⁵) prevedono attualmente un diritto effettivo a contestare l'accuratezza dell'inferenza psicologica, a chiederne la revisione o a esigerne la non utilizzazione a fini decisionali.

Lo studio STOA, pur riconoscendo la solidità del quadro europeo di tutela dei diritti fondamentali, conclude che il ricorso alle garanzie esistenti rischia di lasciare scoperti proprio i profili di rischio più avanzati associati alle neurotecnologie e alle tecniche di inferenza degli stati mentali.

Ciò che emerge, in definitiva, è il limite strutturale di un modello di protezione fondato sull'idea di un soggetto capace di controllare informazioni che lo riguardano. Nel caso dei dati mentali, l'incisione sull'autodeterminazione precede il trattamento giuridicamente rilevante, collocandosi a monte della scelta e del consenso. Il GDPR continua così a operare come tecnica di libertà in un contesto in cui la libertà cognitiva è già stata silenziosamente ristrutturata.

Da qui, quindi, la necessità di riconcettualizzare la protezione dei dati mentali non semplicemente

22. MARINI 2024.

23. D'ORAZIO 2016.

24. IENCA-MALGIERI 2022; AMRAM 2020, p. 73 ss.

25. 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. Cfr. almeno RESTA 2022, p. 323 ss.; CAGGIANO-CONTALDI-MANZINI 2021; FINOCCHIARO 2024.

come un problema di conformità al GDPR, ma come una questione che attiene all'architettura del potere informazionale.

Tale quadro è destinato a essere ulteriormente inciso dalle proposte di revisione del GDPR discusse nell'ambito del c.d. *Digital Omnibus*, promosse dalla Commissione europea²⁶. Sebbene orientate principalmente a obiettivi di semplificazione e riduzione degli oneri amministrativi, tali modifiche sollevano interrogativi circa il possibile indebolimento di alcune garanzie, soprattutto nei contesti ad alta intensità tecnologica. In relazione ai dati mentali, il rischio è che interventi volti a

razionalizzare il quadro normativo non colgano la specificità dei processi inferenziali, lasciando irrisolta la tensione fra efficienza regolatoria e tutela della sfera interiore, con conseguente normalizzazione di pratiche di estrazione della sfera interiore difficilmente compatibili con una concezione forte della dignità e dell'autodeterminazione.

4. Il contributo del Regolamento (UE) 2024/1689

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale interviene su un piano diverso rispetto al GDPR: esso non disciplina il trattamento dei dati

26. Sul c.d. *Digital Omnibus* – attualmente oggetto di dibattito a livello europeo (proposte di regolamento, COM(2025) 837 e COM(2025) 836) – particolare rilievo assume la proposta di revisione della nozione di dato personale nel GDPR. Quello che emerge da una prima lettura della normativa, però, è il rischio che tale riforma tenda a spostare il *focus* dalla tradizionale concezione “oggettiva” dell'identificabilità, fondata sulla possibilità di identificazione anche indiretta mediante mezzi ragionevolmente utilizzabili, verso una nozione “relativa”, ancorata alla concreta capacità del singolo titolare del trattamento di identificare l'interessato con i mezzi a sua disposizione. Vedi lo staff working document della Commissione europea SWD(2025) 836 del 19 novembre 2025. In particolare, la proposta chiarisce che le informazioni non costituiscono dati personali per un determinato titolare del trattamento se quest'ultimo non dispone, e non può ragionevolmente ottenere, i mezzi per identificare l'interessato. La valutazione diventa quindi più soggettiva e incentrata sul titolare, ancorata alle reali capacità di identificazione dell'operatore specifico. La riforma si colloca nel solco di un orientamento già delineato dalla giurisprudenza della Corte di Giustizia UE, in particolare nella causa C-413/23 P (*EDPS v. SRB*), nella quale è stata valorizzata la rilevanza del contesto del titolare ai fini della valutazione dell'identificabilità dell'interessato. Rimane tuttavia incerto in che misura tale impostazione sia compatibile con l'esigenza di garantire un livello uniforme di tutela, sancita dall'art. 1, par. 2, del GDPR: una nozione di dato personale eccessivamente ancorata ai mezzi e alle capacità del singolo titolare rischierebbe infatti di dar luogo ad applicazioni disomogenee della disciplina, sia tra Stati membri sia tra operatori economici dotati di risorse differenti. Il legislatore europeo, poi, interviene sul delicato regime dell'art. 9 GDPR, introducendo due nuove eccezioni al divieto generale di trattamento di categorie particolari di dati, in particolare prevedendo che il GDPR ammetta espressamente: (i) il trattamento di dati biometrici per finalità di mera verifica dell'identità, purché i dati o i mezzi di verifica restino sotto il controllo esclusivo dell'interessato; (ii) il trattamento di categorie particolari di dati nello sviluppo e operatività di sistemi di AI, purché siano adottate misure idonee a prevenire la raccolta o l'ulteriore trattamento di dati oltre quanto necessario. Tale impostazione, pur coerente con l'obiettivo di semplificazione e riduzione degli oneri regolatori perseguito dalla Commissione europea, solleva rilevanti criticità sistematiche. In particolare, le autorità europee di protezione dei dati hanno evidenziato il rischio di una restrizione del perimetro applicativo del GDPR e della conseguente emersione di “zone grigie”, nelle quali il medesimo dato potrebbe essere qualificato come personale o meno a seconda delle capacità tecniche del soggetto che lo tratta (DE GREGORIO–PUPELLA 2026). La ridefinizione incide così su un elemento strutturale dell'intero sistema di tutela, con possibili effetti di frammentazione e incertezza giuridica, nonché con implicazioni dirette sulla protezione dei diritti fondamentali, in particolare nei contesti caratterizzati da trattamenti algoritmici e inferenze su larga scala. In tale prospettiva, il dibattito sul *Digital Omnibus* evidenzia una tensione di fondo fra esigenze di semplificazione normativa e salvaguardia dell'impianto universalistico della protezione dei dati personali. Se l'attenzione si concentra sui dati di input (spesso non qualificati come personali o particolari), si rischia di non intercettare adeguatamente l'output inferenziale (profilazioni psicologiche, stati emotivi, vulnerabilità), che costituisce il vero nucleo problematico. Questo effetto è particolarmente critico per i dati mentali, la cui “particolarità” emerge *ex post*.

in quanto tale, bensì la progettazione, l'immissione sul mercato e l'uso dei sistemi di intelligenza artificiale²⁷. La sua prospettiva è funzionale e fondata sul rischio, sicché ciò che rileva è la capacità del sistema di incidere sui diritti fondamentali, indipendentemente dalla specifica categoria di dati impiegata²⁸.

All'interno di questo schema, i sistemi di IA che possono influenzare in modo significativo la salute mentale o il comportamento degli individui sono qualificati come ad alto rischio o addirittura come pratiche vietate, laddove comportino forme di manipolazione che sfruttano specifiche vulnerabilità²⁹. Il legislatore europeo ha così riconosciuto, almeno in parte, che l'impiego di tecniche di valutazione emotiva e comportamentale in contesti quali il lavoro o l'accesso ai servizi pubblici può compromettere la dignità e la libertà di scelta, generando pressioni occulte o condizionamenti non consapevoli.

Lo studio STOA, da parte sua, suggerisce che l'introduzione dei *neurorights* come diritti umani non costituisce necessariamente la soluzione più efficace. Risulta preferibile, piuttosto, una calibratura di obblighi tecnici e organizzativi per i sistemi che trattano o inferiscono dati mentali, imponendo valutazioni d'impatto, audit indipendenti e forme di supervisione umana³⁰.

Il Regolamento sull'IA si muove in questa direzione, ma lascia aperte almeno due questioni.

In primo luogo, la qualificazione come sistema ad alto rischio dipende dal contesto di utilizzo e dalla finalità dichiarata, non dalla natura intrinseca dei dati psico-affettivi. Ciò comporta che trattamenti profondamente invasivi della sfera mentale possano sfuggire alla regolazione quando siano impiegati in contesti non espressamente ricompresi o quando vengano presentati in termini di "benessere", "coinvolgimento" o "personalizzazione"³¹.

In secondo luogo, la disciplina europea non affronta direttamente il problema della profilazione psicologica sistematica: essa si concentra sui

danni immediati (manipolazione, discriminazione, violazioni di diritti fondamentali), ma non considera pienamente gli effetti cumulativi di un ecosistema in cui decisioni pubbliche e private sono costantemente orientate da modelli predittivi degli stati mentali degli individui. È precisamente questa dimensione cumulativa e ambientale che sfugge tanto alla logica del consenso quanto a quella del rischio, rivelando come la profilazione psicologica non sia un evento isolato da governare, ma una condizione strutturale della soggettività digitale contemporanea.

La sottovalutazione degli effetti cumulativi della profilazione psicologica è tanto più problematica se si considera che i sistemi di intelligenza artificiale non operano primariamente su individui isolati, ma su insiemi di comportamenti collettivi. Come osservato in dottrina, invero, la soggettività che emerge dall'elaborazione algoritmica non coincide né con il soggetto liberale autonomo, né con la persona situata del pensiero giusfilosofico "sociale", ma con una costruzione statistica funzionale alla previsione, alla classificazione e alla gestione del rischio³². In tal senso, le inferenze sugli stati mentali contribuiscono a produrre nuove segmentazioni cognitive ed emotive, generando classi di vulnerabilità che sfuggono alle tradizionali categorie giuridiche, ma che incidono concretamente sull'accesso ai diritti, ai servizi e alle opportunità sociali.

Di conseguenza, pur rappresentando un progresso rispetto all'approccio data-centrico del GDPR, il Regolamento sull'IA non esaurisce la questione della protezione dei dati mentali, restando aperto l'interrogativo se la mente debba essere considerata, al pari del corpo, come un ambito di non disponibilità (sul modello dell'art. 3 della Carta di Nizza), entro il quale taluni usi tecnologici dovrebbero essere assolutamente vietati, piuttosto che semplicemente assoggettati a logiche di gestione del rischio. Il nodo, in definitiva, non è se questi strumenti siano sufficientemente sicuri, ma se la

27. Cfr. PIROZZOLI 2024.

28. Cfr. SANTOSUOSSO 2025, p. 229 ss.

29. DE GREGORIO-DUNN 2022, p. 59 ss.

30. MAIA DE OLIVEIRA WOOD-BERGER-JARKE et al. 2024.

31. IENCA-MALGIERI 2022.

32. MARINI 2024, specialmente p. 7 ss., il quale opportunamente parla di "soggettività algoritmica".

loro stessa legittimazione segni un ulteriore passo verso la disponibilità giuridica della mente.

L'impostazione del Regolamento sull'IA oltretutto, pur rafforzando le garanzie procedurali, lascia intatta la posizione di vantaggio degli attori che controllano l'infrastruttura inferenziale.

Una crescente parte della dottrina, d'altra parte, conferma la limitazione strutturale di un approccio puramente basato sul rischio³³. Come rilevato in recenti analisi sui dispositivi medici basati su IA, l'interazione fra la regolazione settoriale (quale il Regolamento (UE) 2017/745 sui dispositivi medici) e la logica orizzontale del Regolamento (UE) 2024/1689 richiede una valutazione del rischio duplice e in parte eterogenea, incentrata, da un lato, sulle funzioni cliniche e, dall'altro, sugli impatti sui diritti fondamentali³⁴. Questa letteratura mostra come la stessa classificazione di un sistema di IA – lungi dall'essere un'operazione meramente tecnica – contribuisca già a modellare la distribuzione delle responsabilità³⁵, l'ambito degli usi leciti e il livello di protezione dovuto ai soggetti vulnerabili.

Tale acquisizione, sviluppata nel contesto delle tecnologie sanitarie, rafforza quindi l'argomento secondo cui i sistemi di IA capaci di incidere sugli

stati mentali non possono essere governati adeguatamente attraverso un'unica e unitaria tassonomia del rischio.

In questa direzione, infine, si collocano anche le più recenti iniziative della Commissione europea volte a rafforzare la tutela dei consumatori negli ambienti digitali, fra cui il progetto di *Digital Fairness Act*³⁶. Tale proposta normativa, ancora in fase di elaborazione, mira a contrastare pratiche manipolative e sfruttamento delle vulnerabilità comportamentali, incidendo indirettamente anche sulle tecniche di inferenza psico-affettiva. In particolare, l'attenzione alla "fairness" delle interazioni digitali segnala un progressivo spostamento dalla protezione del dato in quanto tale alla regolazione delle architetture decisionali e persuasive che incidono sull'autonomia individuale.

5. Per una categoria autonoma di "dati mentali"

L'emersione dei dati psico-affettivi e delle inferenze sugli stati mentali ha indotto una parte crescente della dottrina giuridica a sostenere il riconoscimento di una categoria autonoma di "dati mentali" o di "informazioni neurali"³⁷. La *ratio* è, come anticipato, che le categorie esistenti (dati sanitari,

33. In dottrina si è già messo in luce come l'attuale strategia normativa europea in materia di dati e intelligenza artificiale tenda meno a porre limiti sostanziali all'uso delle tecnologie che a renderne l'impiego giuridicamente sostenibile. In questa prospettiva, è stato osservato come l'AI Act operi quale *travel companion* dello sviluppo tecnologico, assumendone l'inevitabilità e traducendo le istanze di tutela in requisiti di gestione del rischio e di conformità procedurale, con il rischio di una costituzionalizzazione debole dei diritti fondamentali (cfr. SANTOSUOSSO 2025). Analoga ambivalenza emerge nella costruzione dello spazio europeo dei dati sanitari, dove il rafforzamento delle garanzie individuali si accompagna alla strutturazione di un ecosistema orientato all'uso secondario e al riutilizzo dei dati, spostando il baricentro dalla protezione alla governance (MOLLO 2025, p. 11 ss.).

34. Da ultimo, diffusamente, cfr. la bella e documentata monografia di FERRETTI 2025. Nel contesto dei dispositivi medici e, più in generale, delle tecnologie sanitarie, Ferretti mostra con chiarezza che la rilevanza giuridica dell'informazione non è data in origine, ma dipende dalla funzione che essa assume nel processo decisionale e dagli effetti che può produrre sulla salute e sulla persona. Questo è particolarmente evidente nei sistemi software e nei dispositivi intelligenti, in cui il dato rilevante è spesso il risultato di elaborazioni e inferenze.

35. Cfr. CORSO 2025-B, p. 640 ss.; FACCIOLO 2023, p. 732 ss.; RUFFOLO 2022, p. 502 ss.

36. L'iniziativa normativa si fonda, invero, sulla constatazione delle lacune dell'attuale quadro normativo nel contrasto a fenomeni quali *dark patterns*, design manipolativo e tecniche di personalizzazione che sfruttano vulnerabilità cognitive ed emotive dei consumatori. In tale prospettiva, il *Digital Fairness Act* contribuisce a spostare il centro della tutela dalla dimensione informativa alla regolazione delle architetture di influenza, assumendo particolare rilievo anche rispetto ai dati psico-affettivi e alle tecniche di inferenza degli stati mentali, nella misura in cui queste ultime costituiscono il presupposto tecnico delle pratiche manipolative che la proposta intende disciplinare. Vedi, on-line, digitalfairnessact.com.

37. IENCA-MALGIERI 2022.

dati biometrici, ecc.) colgono solo frammenti del paesaggio neuro-cognitivo, ma non riescono a comprendere la natura distintiva delle informazioni che consentono un accesso diretto o algoritmicamente mediato agli stati interiori della persona. La categoria proposta mira invece ad articolare tale specificità, radicandola nella tutela della libertà cognitiva, dell'integrità mentale e della continuità psicologica³⁸.

Sotto questo punto di vista, i "dati mentali" non coincidono con i tradizionali dati sanitari o relativi alla salute. Tale categoria intende cogliere la peculiarità delle informazioni che permettono un accesso diretto o inferenziale agli stati interni di una persona, indipendentemente dai mezzi tecnici impiegati. Essa ricomprende dunque sia i dati neurali in senso stretto – provenienti da neurotecnologie invasive o non invasive – sia le inferenze psicologiche ricostruite mediante algoritmi che elaborano segnali comportamentali, biometrici o digitali. Ciò che accomuna tali informazioni è la loro capacità di incidere sulla soggettività individuale, anticipando o orientando le scelte personali.

La creazione di una categoria giuridica autonoma avrebbe conseguenze rilevanti. In primo luogo, consentirebbe di qualificare talune forme di trattamento come radicalmente incompatibili con la dignità umana, a prescindere dal consenso dell'interessato. In secondo luogo, favorirebbe l'introduzione di requisiti procedurali e sostanziali rafforzati per l'accesso e l'uso di tali dati, analoghi – o persino più stringenti – rispetto a quelli previsti per i dati genetici³⁹. In terzo luogo, permetterebbe un riconoscimento giuridico del rischio di profilazione psicologica invasiva, che rimane in parte invisibile all'interno delle attuali categorie del GDPR.

Gli sviluppi comparati mostrano una crescente convergenza normativa verso questa intuizione.

L'esperienza italiana, ad esempio, presenta tratti coerenti con tale quadro. La recentissima legge n. 132 del 23 settembre 2025⁴⁰, nel recepire e sviluppare ulteriormente gli orientamenti europei in materia di intelligenza artificiale, introduce principi generali – centralità della persona, trasparenza algoritmica, tutela della dignità e dei diritti fondamentali – che richiamano la concezione rodotiana di un diritto capace di anticipare i conflitti tecnologici emergenti⁴¹. La legge non si limita a ribadire l'applicazione del GDPR e del Codice privacy ai trattamenti basati su IA, ma stabilisce misure specifiche in settori ad alta vulnerabilità quali la sanità, la ricerca, il lavoro e la giustizia.

In particolare, ai fini che qui interessano, la legge introduce obblighi rafforzati per i sistemi di IA che trattano dati particolari, fra cui la consultazione preventiva obbligatoria del Garante per la protezione dei dati personali per i progetti fondati su dataset particolarmente delicati, misure tecniche e organizzative aggiuntive rispetto all'art. 32 GDPR per i sistemi ad alto rischio e specifici obblighi informativi quando i dati siano utilizzati per l'addestramento algoritmico. La disciplina richiede, inoltre, il coinvolgimento di comitati etici e la supervisione di professionisti qualificati per l'uso dell'IA in ambito diagnostico, terapeutico e di ricerca, riconoscendo così espressamente la particolare vulnerabilità della dimensione mentale nei contesti clinici e sanitari.

5.1. Suggestioni comparatistiche: California Consumer Privacy Act

Un ulteriore esempio rilevante proviene dagli Stati Uniti, in particolare dalla California, dove una recente modifica al *California Consumer Privacy Act* (CCPA) mira a chiarire espressamente che i dati cerebrali (*brain data*) devono essere considerati fra le informazioni personali più sensibili. Muovendo

38. È opportuno chiarire che la proposta di una categoria autonoma di "dati mentali" viene qui esaminata non come soluzione normativa auspicabile in sé, ma come snodo critico. Essa costituisce un banco di prova per comprendere se il diritto sia ancora in grado di porre limiti sostanziali all'accesso alla sfera interiore delle persone o se, al contrario, la raffinatezza categoriale finisca per normalizzare ciò che pretende di proteggerne.

39. Sui dati genetici cfr. RODOTÀ 2000, p. 584 ss.

40. Tale legge rappresenta un intervento normativo ambizioso, visto che non si limita a recepire i principi dell'AI Act europeo, ma introduce una disciplina specifica per settori chiave e delega al Governo il compito di definire aspetti cruciali, dall'addestramento degli algoritmi alla responsabilità civile.

41. RODOTÀ 1995.

dalla constatazione che le neuroscienze e le neurotecnologie consentono sempre più spesso l'accesso all'attività cerebrale, l'emendamento specifica che tali dati non possono essere assimilati a semplici informazioni biometriche o comportamentali e richiedono pertanto garanzie rafforzate⁴².

L'emendamento introduce una definizione giuridicamente significativa di dati neurali, qualificandoli come "[i]nformation that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information". In tal modo, il legislatore californiano traccia una distinzione netta fra i dati effettivamente derivanti dalla registrazione dell'attività neurale (EEG, potenziali evocati, segnali BCI) e le inferenze tratte da dati non neurali, quali il comportamento digitale o la vocalità, che possono avere contenuto psicologico ma non sono "neurali" in senso stretto.

Questa scelta normativa non è solamente classificatoria. Essa implica che chi intenda trattare dati cerebrali debba rispettare stringenti obblighi di trasparenza nei confronti di utenti e consumatori, chiarendo modalità di raccolta, finalità, rischi e possibili conseguenze. Inoltre, agli interessati deve essere garantito un controllo effettivo sui propri dati neurali attraverso meccanismi di opt-in rafforzati, diritti di limitazione e cancellazione e divieti di utilizzo non strettamente necessari. La *ratio* sottesa è che, quando è in gioco l'attività neurale, il consenso deve essere genuinamente informato e libero, e il titolare del trattamento deve dimostrare un livello elevato di *accountability*. Anche qui, tuttavia, la raffinatezza della definizione legislativa non elimina il rischio che l'attività neurale venga assunta come dominio regolabile piuttosto che come limite sostanziale al potere tecnologico.

Il parallelismo con il dibattito europeo è evidente. Nell'Unione europea, come mostra lo studio STOA, i dati mentali presentano un'incertezza classificatoria, dal momento che – come detto – non è chiaro se e quando essi rientrino fra i dati sanitari, biometrici o costituiscano una categoria nuova. La soluzione californiana, pur radicata in una tradizione di tutela del consumatore più che in un quadro di diritti fondamentali, riconosce espressamente la specificità dei dati cerebrali, attribuendo

loro un livello di protezione che si avvicina – se non anticipa – quanto la dottrina europea prospetta per i dati mentali.

L'esperienza californiana conferma dunque che una tutela rafforzata dell'attività neurale è considerata sempre più indispensabile anche al di fuori dell'Europa. Essa riflette una tendenza giuridica transnazionale che si muove lungo due traiettorie convergenti:

- (a) il riconoscimento della natura qualitativamente distinta delle informazioni che rivelano (o sono idonee a rivelare) stati mentali e processi cognitivi;
- (b) l'assoggettamento del trattamento di tali dati a garanzie rafforzate fondate su trasparenza, controllo individuale e responsabilità del titolare.

Questa convergenza normativa, pur emergendo all'interno di modelli giuridici differenti, suggerisce che la categoria dei "dati mentali" possieda una plausibilità intrinseca. Essa indica inoltre che la protezione della mente come sfera tendenzialmente indisponibile – fondata su dignità e autodeterminazione informativa – stia rapidamente emergendo come nuovo standard minimo internazionale.

Tuttavia, un'analisi giusrealista complica questa narrazione. La proposta di costruire una categoria giuridica autonoma non può essere letta soltanto come un affinamento tecnico del diritto della protezione dei dati. Come vedremo a breve, infatti, essa è anche un luogo in cui il diritto partecipa alla configurazione della distribuzione del potere tecnologico e istituzionale. Nel classificare i dati mentali come oggetto distinto di tutela giuridica, il diritto non si limita a descrivere una realtà preesistente, ma la produce. Delimita ciò che conta come mentalmente rilevante, quali attori possono legittimamente accedervi o interpretarlo e a quali condizioni. Come spiega Duncan Kennedy, la creazione delle categorie giuridiche è sempre mediata da *background rules*⁴³ che strutturano silenziosamente la posta in gioco della classificazione.

5.2. Quale normalizzazione per i dati mentali?

Secondo tale chiave di lettura, pertanto, la spinta verso una categoria autonoma di dati mentali

42. BROWNING 2025.

43. KENNEDY 1991.

risponde non solo ad aspirazioni normative, ma anche a pressioni strutturali. La crescente capacità delle neurotecnologie e dei modelli di IA di inferire stati mentali destabilizza le distinzioni tradizionali fra dati sanitari e non sanitari, fra rivelazioni volontarie e involontarie, fra comportamento osservabile e interiorità⁴⁴. L'incertezza classificatoria del diritto riflette tale instabilità. Tuttavia, il tentativo di stabilizzare il campo attraverso una nuova categoria rischia di riprodurre proprio quelle *background rules* che hanno generato l'incertezza, e cioè la centralità del dato come "oggetto" disponibile, il ricorso a tassonomie ex ante e la presunzione che la protezione discenda dalla classificazione.

Gli sviluppi comparati illustrano questa tensione. La traiettoria legislativa italiana, soprattutto dopo la riforma del 2025 sulla governance dell'IA, rafforza le garanzie per i sistemi ad alto rischio in sanità, ricerca, lavoro e giustizia. L'approccio californiano, invece, isola i *brain data* mediante un atto definitorio preciso che pone in primo piano l'attività neurale come dominio informativo di sensibilità unica. Entrambi i modelli cercano di anticipare le implicazioni etiche e sociali degli interventi sulla sfera mentale, ma entrambi, in modi diversi, riproducono una grammatica regolatoria più profonda: all'espansione della protezione si accompagna l'espansione delle condizioni alle quali l'accesso tecnologicamente mediato agli stati mentali diviene lecito, purché siano soddisfatti determinati requisiti procedurali e organizzativi.

Da una prospettiva critica, la questione non è dunque soltanto se i dati mentali meritino una tutela rafforzata – risposta che appare intuitivamente positiva – ma come l'atto stesso del riconoscimento giuridico rimodelli il perimetro degli interventi ammissibili. La costruzione di una categoria autonoma può operare come presidio di garanzia, ma può anche normalizzare una soglia di intrusione ritenuta accettabile, spostando il dibattito dalla legittimità dell'accesso agli stati mentali all'adeguatezza dei meccanismi di conformità. In altri termini, la categoria può al tempo stesso illuminare e occultare, considerato che, da un lato, rende visibile l'esigenza di protezione, ma dall'altro rischia di rafforzare l'assunto di fondo secondo cui l'inferenza degli stati mentali è una caratteristica

inevitabile, governabile e, in ultima analisi, disponibile della vita digitale contemporanea.

Il rischio, lo si vuol ribadire, è che la raffinazione delle categorie giuridiche finisca per normalizzare una soglia di intrusione considerata accettabile, spostando il baricentro del discorso dalla legittimità stessa dell'accesso alla sfera mentale alla correttezza delle procedure che lo regolano. Da questo punto di vista, la vera posta in gioco non è soltanto l'estensione della protezione, ma la capacità del diritto di interrogare criticamente le condizioni strutturali che rendono la mente un dominio tecnicamente leggibile e giuridicamente governabile.

Ne emerge un paradosso concettuale. Il diritto mira a difendere la mente come dominio di dignità rafforzata, eppure gli stessi strumenti che impiega – categorizzazione, proceduralizzazione, gestione del rischio – fanno parte di un'infrastruttura regolatoria che presuppone la governabilità dei dati mentali. Un approccio genuinamente giusrealista deve mantenere lo sguardo sulle forze strutturali (tecnologiche, economiche, istituzionali) che ridefiniscono continuamente i confini dell'interiorità e interrogare il modo in cui le categorie giuridiche possano tanto resistere a tali forze quanto, inavvertitamente, rafforzarle. La sfida consiste, allora, nell'assicurare che l'ambizione normativa della libertà cognitiva non si dissolva in un insieme più raffinato di autorizzazioni, assicurando semmai un completo divieto di trattamento di tali dati, onde preservare la sfera più intima della persona e garantirne effettivamente l'*habeas mentem*⁴⁵.

6. Brevi conclusioni: dati mentali e diritto privato

Da quanto detto emerge come l'accesso tecnologicamente mediato agli stati mentali della persona è reso possibile, prima ancora che da specifiche scelte regolatorie, da un insieme di *background rules* riconducibili al diritto privato, che strutturano in modo silenzioso ma decisivo la distribuzione del potere tecnologico e informativo negli ecosistemi neuro-digitali governati dalle *Big Tech*.

Contratti di consumo, rapporti di lavoro, assetti proprietari sulle infrastrutture digitali e regimi di responsabilità civile costituiscono il terreno giuridico ordinario entro cui, oggi sempre più, la

44. Sulle questioni poste, a più livelli, dall'IA cfr. i contributi di giuristi e filosofi raccolti in FALCONE–PILI 2025.

45. STANZIONE 2021.

mente diventa leggibile, prevedibile, influenzabile, governabile. In tali contesti, l'accesso ai segnali psico-affettivi non assume la forma di un'ingerenza eccezionale, ma quella di una prestazione accessoria, spesso tacita e funzionale, inserita in rapporti giuridici caratterizzati da asimmetrie di potere. Il diritto privato, lungi dall'essere un mero strumento tecnico di circolazione delle utilità, opera qui come dispositivo di normalizzazione dell'intrusione nella sfera interiore, trasformando l'inferenza degli stati mentali in una componente ordinaria dell'esperienza contrattuale, in più ambiti, da quello laburistico a quello assicurativo e consumeristico, e finanche a quello sportivo⁴⁶.

Questo dato problematizza radicalmente l'affidamento, spesso implicito, sugli strumenti di autodeterminazione individuale. La libertà contrattuale, il consenso informato e la possibilità di scelta presuppongono un soggetto in grado di valutare razionalmente le condizioni dell'interazione. Le pratiche di inferenza psico-affettiva, tuttavia, intercettano vulnerabilità cognitive ed emotive e operano a un livello antecedente rispetto alla decisione consapevole, orientando preferenze e comportamenti prima che essi si traducano in scelte giuridicamente rilevanti. Ne deriva una frizione fra l'antropologia sottesa al

diritto privato⁴⁷ e le forme di soggettività prodotte dagli ambienti tecnologicamente mediati⁴⁸.

Anche i tradizionali strumenti di tutela *ex post* mostrano, in questo ambito, una marcata insufficienza. I danni derivanti dalla profilazione psicologica sistematica non si manifestano necessariamente in eventi puntuali o immediatamente percepibili, ma si accumulano nel tempo, incidendo sulle opportunità, sull'autopercezione e sulle traiettorie decisionali degli individui. La responsabilità civile, ancorata a schemi causali e a standard di prevedibilità, rischia così di operare come una tecnica di gestione del rischio dell'estrazione mentale, piuttosto che come uno strumento capace di interrogare la legittimità stessa dell'accesso alla sfera interiore delle persone.

In questa prospettiva, la proposta di una categoria autonoma di "dati mentali" non può essere valutata unicamente in termini di rafforzamento delle garanzie. Essa incide direttamente sulle regole di fondo del diritto privato, ridefinendo ciò che può essere oggetto di scambio, di sfruttamento economico e di assunzione del rischio.

Le più recenti iniziative europee – dal Regolamento sull'intelligenza artificiale ai progetti in materia di *fairness* digitale e semplificazione normativa – confermano che la protezione della dimensione mentale non può essere affidata

46. In ambito sportivo, la tutela della dimensione mentale risulta particolarmente problematica (e non solo nei c.d. *E-Sport*): per atleti giovani o in fase di accesso al professionismo, l'accettazione di forme di monitoraggio neurale può tradursi in un consenso meramente formale. Inoltre, la crescente domanda di trasparenza che attraversa il sistema sportivo rende appetibile l'uso di dati mentali per valutazioni di performance o decisioni di mercato, con il rischio di un impiego di informazioni intime per finalità economiche o commerciali non strettamente giustificate. Il rischio non si esaurisce nella raccolta dei dati. L'impiego di tecniche di neuromodulazione, dalla stimolazione magnetica transcranica al *neurofeedback*, solleva interrogativi ulteriori circa la liceità del loro utilizzo per migliorare concentrazione, ridurre l'ansia o accelerare il recupero. In tali ipotesi, il confine fra supporto terapeutico e forme di doping cognitivo risulta particolarmente sfumato.

47. Cfr. MARELLA 2021, p. 71 ss. In questa prospettiva, la proposta di isolare una categoria autonoma di "dati mentali" si colloca entro un più ampio processo di trasformazione della soggettività giuridica, efficacemente descritto da Marella nei termini di un progressivo abbandono del modello universalistico del soggetto di diritto a favore di una sua frammentazione in una pluralità di identità giuridicamente rilevanti, ciascuna corredata da specifici diritti e regimi di tutela. In tale quadro, il soggetto di diritto non si presenta più come centro unitario e indifferenziato di imputazione, ma come esito di operazioni di selezione e qualificazione operate dal diritto, le quali intercettano condizioni personali, situazioni contingenti e, sempre più, tratti comportamentali e psicologici. La rilevanza giuridica dei dati psico-affettivi – specie quando derivanti da processi inferenziali algoritmici – sembra iscriversi precisamente in questa dinamica: essi non si limitano a rappresentare la persona, ma contribuiscono a costruirne versioni giuridicamente significative, attraverso classificazioni che individuano vulnerabilità, propensioni o stati cognitivi suscettibili di essere tradotti in differenziazioni di trattamento.

48. Sul punto cfr., ancora, MARINI 2024.

esclusivamente alle categorie tradizionali del diritto della protezione dei dati. Essa richiede, piuttosto, un coordinamento fra strumenti regolatori eterogenei, capace di incidere non solo sui dati, ma sulle infrastrutture tecniche e sulle condizioni di esercizio del potere informazionale.

La mente si rivela così come un nuovo spazio di conflitto fra poteri, fra logiche di mercato, promesse di benessere e istanze di dignità, in cui il diritto privato non è un semplice spettatore, ma uno dei principali luoghi di produzione e di legittimazione del potere stesso.

Riferimenti bibliografici

- AA.VV. (2021), *Privacy e neurodiritti. La persona al tempo delle neuroscienze. Atti del Convegno – 28 gennaio 2021*, in *garanteprivacy.it*, Doc-Web 9527139, 2021, 2021
- G. ALPA (1985), *Il diritto dei Computers*, in “Diritto dell’informazione e dell’informatica”, 1985, n. 1
- G. ALPA (1979), *Privacy e statuto dell’informazione*, in “Rivista di diritto civile”, 1979, n. 1
- D. AMRAM (2020), *Il ruolo del GDPR nella progettazione della strategia europea sull’intelligenza artificiale: le potenzialità legislative di una sineddoche ricorrente*, in “Opinio Juris in Comparatione”, 2020, n. 1
- M. BETZU (2021), *I poteri privati nella società digitale: oligopoli e antitrust*, in “Diritto Pubblico”, 2021, n. 3
- C.M. BIANCA (1977), *Le autorità private*, Jovene, 1977
- J.G. BROWNING (2025), *Are Technology and the Law on the Same “Wavelength”? Examining the New Frontier of Brainwaves and Data Privacy*, in “North Carolina Journal of Law & Technology”, vol. 26, 2025, n. 3
- G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di) (2021), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, 2021
- M.V. CATANZARITI (a cura di) (2025), *Lo spazio europeo dei dati sanitari: una riflessione interdisciplinare su diritto, etica e scelte pubbliche*, in “Notizie di Politeia”, vol. XLI, 2025, n. 158
- Y. CHAUDHARY, J. PENN (2024), *Beware the Intention Economy: Collection and Commodification of Intent via Large Language Models*, in “Harvard Data Science Review”, 2024, Special Issue 5
- F. CIRILLO (2023), *Neurodiritti: ambiguità della libertà cognitiva e prospettive di tutela*, in “Consulta Online”, 2023, n. 2
- S. CORSO (2025-A), *Autodeterminazione e dati sanitari*, Giappichelli, 2025
- S. CORSO (2025-B), *Responsabilità per causalità presunta. Intelligenza artificiale, responsabilità civile e diritto eurolunitario*, in “Responsabilità civile e previdenza”, 2025, n. 2
- G. DE GREGORIO, P. DUNN (2022), *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in “Common Market Law Review”, 2022
- G. DE GREGORIO, R. PUPELLA (2026), *Digital Omnibus: le condizioni poste da EDPB ed EDPS alla riforma del GDPR*, in “NTPLUS Diritto”, 5 marzo 2026
- M. DI MASI (2021), *Titolo V Trattamento dei dati personali in ambito sanitario*, in R. D’Orazio, G. Finocchiario, O. Pollicino, G. Resta (a cura di), “Codice della Privacy e Data Protection”, Giuffrè, 2021
- R. D’ORAZIO (2016), *Protezione dei dati by default e by design*, in S. Sica, V. D’Antonio, G.M. Riccio (a cura di), “La nuova disciplina europea della privacy”, Wolters Kluwer, 2016
- M. FACCIOLO (2023), *Intelligenza artificiale e responsabilità sanitaria*, in “Nuova giurisprudenza civile commentata”, 2023
- M. FALCONE (2023), *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, Editoriale Scientifica, 2023

- M. FALCONE, E. PILI (a cura di) (2025), *L'irriducibile umano. Etica e diritto delle intelligenze artificiali*, il Mulino, 2025
- M.R. FERRARESE (2022), *Poteri nuovi*, il Mulino, 2022
- F. FERRETTI (2025), *Tutela della salute, Intelligenza Artificiale e gestione del rischio*, Edizioni Scientifiche Italiane, 2025
- G. FINOCCHIARO (2024), *Intelligenza artificiale. Quali regole?*, il Mulino, 2024
- M. IENCA (2019), *Tra cervelli e macchine: riflessioni su neurotecnologie e su neurodiritti*, in "Notizie di Politeia", vol. XXXV, 2019, n. 133
- M. IENCA, G. MALGIERI (2022), *Mental Data Protection and the GDPR*, in SSRN, 2022
- DU. KENNEDY (1991), *The Stakes of Law, or Hale and Foucault!*, in "Legal Studies Forum", vol. 15, 1991
- G. MAIA DE OLIVEIRA WOOD, L. BERGER, J. JARKE, G. BARNARD, T. GREMSL, E. DOLEZAL, E. STAUDEGER, P. ZANDONELLA (2024), *The protection of mental privacy in the area of neuroscience. Societal, legal and ethical challenges*, European Parliament, 2024
- M.R. MARELLA (2021), *Antropologia del soggetto di diritto. Note sulle trasformazioni di una categoria giuridica*, in "Osservatorio del diritto civile e commerciale", 2021, n. 1
- G. MARINI (2024), *Editoriale*, in "Rivista critica del diritto privato", 2024, n. 1
- G. MARINI (2013), *Diritto alla privacy*, in A. Barba, S. Pagliantini (a cura di), "Commentario del codice civile", diretto da E. Gabrielli, UTET, 2013
- A.A. MOLLO (2025), *Prime riflessioni sul Regolamento europeo sullo spazio europeo dei dati sanitari: l'uso secondario e il diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali*, in "BioLaw Journal – Rivista di BioDiritto", 2025, n. 3
- A.A. MOLLO (2021), *La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici*, in "European Journal of Privacy Law & Technologies", 2021, n. 1
- R. PARDOLESI (2021), *Piattaforme digitali, poteri privati e concorrenza*, in "Diritto Pubblico", 2021, n. 3
- A. PIROZZOLI (2024), *The Human-centric Perspective in the Regulation of Artificial Intelligence*, in "European Papers", 2024, n. 1
- O. POLLICINO (2023), *Potere digitale*, in M. Cartabia, M. Ruotolo (diretto da), "Enciclopedia del diritto – I tematici, V, Potere e Costituzione", Giuffrè, 2023
- O. POLLICINO (2021), *Costituzionalismo, privacy e neurodiritti*, in "Medialaws", 2021, n. 2
- G. RESTA (2023), *Poteri privati e regolazione*, in M. Cartabia, M. Ruotolo (diretto da), "Enciclopedia del diritto – I tematici, V, Potere e Costituzione", Giuffrè, 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
- S. RODOTÀ (2020), *Of Machines and Men. The Road to Identity: Scenes for a Discussion*, in "Comparative Law Review", 2020
- S. RODOTÀ (2000), *Tra diritto e società. Informazioni genetiche e tecniche di tutela*, in "Rivista critica del diritto privato", 2000
- S. RODOTÀ (1995), *Tecnologie e diritti*, il Mulino, 1995
- S. RODOTÀ (1991), *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in "Politica del diritto", 1991
- S. RODOTÀ (1973), *Elaboratori elettronici e controllo sociale*, Zanichelli, 1973

- U. RUFFOLO (2022), *L'intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in "Giurisprudenza italiana", 2022
- M. RUOTOLO (2024), *Il potere, tra pubblico e privato. Tracce per un dialogo tra civilisti e costituzionalisti*, in "Costituzionalismo.it", 2024, n. 3
- R. SACCO (1991), *Legal Formants: A Dynamic Approach to Comparative Law*, in "The American Journal of Comparative Law", vol. 39, 1991, n. 1
- A. SANTOSUOSSO (2025), *The AI Act, its travel companion, and a constitutional question (of survival)*, in "BioLaw Journal – Rivista di BioDiritto", 2025, n. 3
- P. STANZIONE (2021), *Relazione introduttiva*, in Aa.Vv., "Privacy e neurodiritti. La persona al tempo delle neuroscienze. Atti del Convegno – 28 gennaio 2021", in garanteprivacy.it, Doc-Web 9527139, 2021
- L. TORCHIA (2024), *Poteri pubblici e poteri privati nel mondo digitale*, in "Il Mulino", 2024, n. 1
- G. VETTORI (2022), *Sui poteri privati. Interazioni e contaminazioni*, in "Diritto Pubblico", 2022, n. 3



FILIPPO ZATTI

Technology-based decentralization and the structural limits of legal attribution: Why adapting the law requires rethinking its foundations

This article examines whether blockchain-based decentralization poses challenges to the legal order amenable to incremental regulatory adaptation, or with structural inadequacies in its very foundations. Legal orders presuppose the identification of subjects – natural persons, legal entities, public authorities – to whom rights and obligations are attributed. Attribution unfolds across three constitutive dimensions: territory, language, and embodied legal subjectivity. Blockchain technology and autonomous decentralized systems – *Decentralized Autonomous Organizations*, *Decentralized Finance* protocols – destabilize each, operating without identifiable centres of accountable authority. The challenge is therefore structural, not regulatory: as centres of attribution recede, legal categories lose the referent that grounds their meaning. Regulatory responses – the MiCAR Regulation, US enforcement actions – vest accountability in identifiable subjects. Integrating decentralized technologies thus brings to light the need to reconstitute identifiable centres of attribution: not a mere adaptation of the existing normative framework, but an exercise in institutional innovation.

Blockchain technology – Decentralization – Smart contracts – Jurisdiction – Lex cryptography

Decentralizzazione tecnologica e presupposti strutturali dell'ordinamento. Ripensare i fondamenti del diritto prima di adeguarlo all'innovazione

Il presente contributo esamina se la decentralizzazione di matrice blockchain ponga all'ordinamento sfide risolubili tramite adeguamento incrementale, o riveli piuttosto un'adeguatezza strutturale nei suoi stessi fondamenti. Gli ordinamenti giuridici postulano l'individuazione di soggetti – persone fisiche, enti dotati di personalità giuridica, autorità pubbliche – cui attribuire diritti e obblighi. L'attribuzione si dispiega lungo tre dimensioni costitutive: territorio, linguaggio, soggettività giuridica incarnata. La tecnologia blockchain e i sistemi decentralizzati autonomi – organizzazioni autonome decentralizzate, protocolli di finanza decentralizzata – destabilizzano ciascuna di esse, operando senza centri identificabili di autorità responsabile. La sfida è dunque strutturale, non regolatoria: venendo meno i centri di attribuzione, le categorie giuridiche smarriscono il referente che ne fonda il significato. Le risposte regolatorie – il regolamento MiCAR, le decisioni di *enforcement* statunitensi – riconducono la responsabilità in capo a soggetti identificabili. L'integrazione delle tecnologie decentralizzate fa emergere la necessità di ricostituire centri di attribuzione identificabili: non un mero adeguamento del quadro normativo vigente, bensì un'opera di innovazione istituzionale.

Tecnologia blockchain – Decentralizzazione – Smart contract – Giurisdizione – Lex cryptography

The Author is Associate Professor of Economic Law at the University of Florence, Department of Economics and Management (DISEI), and serves as scientific coordinator of the Blockchain and Artificial Intelligence for Business, Economics and Law (BABEL) Research Unit. He is also Academic Fellow of the European Banking Institute

This paper was developed as part of the PRIN 2022 project “DeTOKoDE – Designing a Governance for the Tokenized Economy in a Decentralized Era” (Protocol No. 20225YEPCT), funded by the Italian Ministry of University and Research (MUR) under the National Recovery and Resilience Plan (NRRP)

SUMMARY: 1. The decentralization dilemma: reconciling Distributed Ledger Technology with “legal order”. – 2. Law without centres: the decentralization challenge. – 2.1. Displacement of foundational legal symbolics and imaginaries. – 2.2. Deterritorialization and the question of sovereign authority. – 2.3. The elusiveness of jurisdiction and the limits of enforcement. – 2.4. Disembodiment and the paradox of legal subjectivity. – 2.5. Regulatory responses. – 3. Law as a system founded on “centres of attribution”. – 3.1. The theoretical facilitation of constitutional ideals. – 3.2. The fundamental conflict with constitutional prerequisites. – 4. The necessity of hybridisation and legal anchoring. – 5. Beyond functional equivalence: the imperative of institutional innovation.

1. The decentralization dilemma: reconciling Distributed Ledger Technology with “legal order”

Traditional legal order depends fundamentally on the ability to identify subjects – whether natural persons, legal entities, or state authorities – to whom legal consequences can be attributed. This architectural principle underlies virtually every aspect of law: from criminal responsibility to contractual obligations, from property rights to regulatory enforcement, from territorial jurisdiction to legal personality.

Blockchain technology and decentralized autonomous systems challenge this foundational assumption by operating without identifiable centres or responsible authorities. These systems promise to create legal frameworks that function autonomously, without territorial boundaries, human intermediaries, or the institutional structures that have historically guaranteed legal certainty and enforcement. *Decentralized Autonomous Organisations* (DAOs) make collective decisions through smart contracts and token voting, cryptocurrencies transfer value without banks. *Decentralized finance* (DeFi) provides financial services without the need for licensed institutions. In each case, the system operates – or aspires to

operate – without centres to which traditional legal attribution can attach.

This resistance to centres of attribution is not incidental but constitutive: decentralization means the absence of identifiable controlling authorities. Nevertheless, law’s basic operations – determining applicable rules, adjudicating disputes, enforcing judgments, allocating responsibility – presuppose the existence of such centres. This creates a fundamental tension, perhaps even an incompatibility, between decentralization’s aspirations and law’s operational requirements.

How does technology-based decentralization challenge traditional legal paradigms, and can these challenges be reconciled with the law’s foundational requirements? More specifically, it examines whether legal systems can adapt their attribution mechanisms to accommodate genuinely centreless systems, or whether ostensibly decentralized systems must ultimately establish identifiable centres to achieve legal recognition and enforceability.

As mentioned above, the analysis employs the concept of “centres of attribution” (*Zurechnungs-subjekt*, as defined in Kelsen’s terminology) as an organising framework¹. Based on Kelsen’s pure theory of law and Romano’s institutional theory², it could be argued that law operates solely by attribut-

1. Kelsen 1945.

2. ITZCOVICH 2020.

ing rights, duties, and legal consequences to specific subjects. These attribution operations take place across three essential dimensions: the first being territory, which refers to the spatial dimension that anchors jurisdiction and enforcement. Another dimension is language, which serves as the symbolic medium for the articulation and interpretation of norms. Lastly, there is the body, which encompasses the embodied subjects that possess legal personality and experience legal consequences.

Decentralization challenges each of these dimensions while simultaneously highlighting their continued necessity. This framework facilitates a systematic analysis of the legal challenges posed by blockchain technology and offers a cohesive theoretical perspective for understanding issues that may appear disparate. The essay employs doctrinal legal analysis, supplemented by engagement with legal theory and empirical observation of blockchain systems. It examines how decentralization disrupts traditional legal concepts, evaluates regulatory responses, and assesses normative claims regarding constitutional benefits and conflicts. The analysis addresses the fundamental theoretical challenges that decentralization poses to law in general, rather than focusing on sector-specific applications. Although particular contexts such as financial regulation, corporate governance, and dispute resolution are referenced, the analysis seeks generality across applications. So, it concentrates on “public” permissionless blockchains rather than private permissioned systems, as these present the most significant challenges to traditional legal assumptions. Geographically, the analysis primarily considers European Union and US legal frameworks, while recognizing the global operation of blockchain.

2. Law without centres: the decentralization challenge

The rise of decentralized technologies, particularly blockchain with the support of smart contracts, presents a profound and multifaceted challenge to the traditional legal paradigm, which is fundamentally built upon centralized institutions, territorial sovereignty, human interpretation, and established

frameworks for accountability and liability³. The conflict lies in the core principles of decentralization, (pseudo)anonymity, and automation inherent in these technologies, which range from clashing directly with classic juridical standards concerning stability, liability, territory, and social order; to rarely exploring possible alliances with the law to achieve common objectives. The challenges posed by decentralization applications can be examined across several critical areas: the very symbolic foundations of law, the role and sovereignty of the State, the feasibility of enforcement and jurisdiction, and the applicability of traditional liability and regulatory frameworks.

It is important to note that these challenges are not merely regulatory inconveniences amenable to incremental adaptation. Rather, they strike at the structural presuppositions upon which legal reasoning itself depends. Traditional legal categories – contract, property, personality, jurisdiction – are not free-standing concepts but derive their operational capacity from the existence of identifiable subjects to whom they can be attributed. When that foundational condition is systematically absent, the categories do not merely become difficult to apply; they lose the very referent that gives them meaning⁴. This distinction between difficulty of application and structural inadequacy is central to the argument that follows.

2.1. Displacement of foundational legal symbolics and imaginaries

2.1.1. *Lex cryptography: nomen aut res?*

Blockchain technology, through its underlying ideology and technical architecture, initiates a potentially profound displacement of the symbolic and imaginary foundations upon which traditional legal systems have historically relied.

This emerging framework, often termed *lex cryptography*⁵, aspires to emancipate itself from three essential dimensions that have characterised modern legal systems: language, territory, and embodied legal subjectivity. However, whether *lex cryptography* constitutes an alternative form

3. COUTINHO–PIRES–CORREIA BARRADAS 2024; BECKER 2022; CAPPIELLO–CARULLO 2021; LAI 2021.

4. This distinction is developed further in Section 3 below. On the structural presuppositions of legal attribution, see Kelsen 1945; on the institutional dimension, ITZCOVICH 2020.

5. DE FILIPPI–WRIGHT 2018; DE FILIPPI–WRIGHT 2015.

of law or rather a novel regulatory tool operating *within* existing legal frameworks remains a contested question⁶.

On one hand, blockchain-based governance exhibits law-like functions – coordinating behaviour, algorithmically resolving disputes, and enforcing compliance through cryptographic constraints – indicating a functional equivalence with traditional legal systems. On the other hand, its reliance on territorial law for ultimate legitimation and enforcement, its lack of interpretive flexibility and institutional structure, and its operation primarily through technical architecture rather than normative authority suggest that it may be more accurately viewed as one regulatory modality among others⁷, serving to complement rather than displace state law.

This ambiguity extends beyond mere semantics and carries significant normative implications: to characterise blockchain as “law” may grant it undeserved legitimacy and obscure the private interests embedded within ostensibly neutral technical systems, whereas denying its legal character could close our eyes to genuine innovations in governance and the rise of alternative sources of normative authority. Whether this reflects a completed transformation of law or an ongoing contestation between different regulatory modalities remains an open question that warrants critical examination.

2.1.2. *Language as symbolic attribution, code as performative inscription*

Natural language provides the law’s symbolic medium, enabling the articulation of general norms, their interpretation in specific cases, and the communication of legal meanings across time and contexts.

The most immediate consideration is that traditional law has fundamentally relied on natural language as its primary medium, which is inherently

characterised by ambiguity, contextual sensitivity, and opportunities for interpretive flexibility⁸. *Lex cryptographia* aspires to revolutionise this paradigm by substituting linguistic articulation with computer code as the foundational substrate of legal systems. Proponents argue that this shift promises to eliminate subjective interpretation: legal frameworks such as smart contracts purportedly operate according to rigid “if-then” logical principles that would adhere to the rule of noncontradiction⁹.

However, this vision of code as determinate and interpretation-free warrants critical scrutiny. As legal scholars have observed, code itself requires interpretation at multiple levels¹⁰. During its creation, when ambiguities in requirements must be resolved; during execution, when edge cases arise; and during disputes, when questions of intent, error, and enforceability emerge. The notorious collapse of The DAO in 2016, which required human intervention and contentious debate despite operating through ostensibly autonomous code, illustrates the persistence of interpretive questions even within blockchain systems¹¹.

Furthermore, this framework embodies what might be termed an anti-representational logic. By attempting to collapse the distinction between word and action within the algorithm, the system seeks to eliminate the deliberative space that characterises traditional legal structures – the gap between norm and enforcement that permits negotiation, proportionality, and equitable adjustment¹². While proponents present this as establishing a more precise and predictable legal environment, critics contend that it risks sacrificing essential legal values: the capacity for contextual judgment, the protection of vulnerable parties, and the democratic contestability of legal outcomes¹³.

The normative implications of this shift remain contested. Does the elimination of interpretive

6. BLEMUS 2018.

7. LESSIG 2006.

8. HART–GREEN 2012; FISH 1989.

9. DORIA–BASSAN–RABITTI et al. 2024.

10. GRIMMELMANN 2021; SCHOLZ 2017.

11. UNGUREANU–BELLESIA–COCHIS 2025; DUPONT 2017.

12. HILDEBRANDT 2018.

13. DE FILIPPI–MANNAN–REIJERS 2022; VERSTRAETE 2020.

space represent progress toward efficiency and certainty, or does it constitute a dangerous impoverishment of law's capacity to serve justice and adapt to human complexity?

2.2. Deterritorialization and the question of sovereign authority

Decentralized blockchain (infra)structures also challenge traditional legal systems by aspiring to sever the intrinsic connections between law, political sovereignty, and territorial boundaries that have defined the Westphalian order since the seventeenth century¹⁴. These systems seek to establish legal frameworks that operate independently of the State's symbolic authority, effectively detaching legal validity from territorial jurisdiction.

In this evolving landscape, we observe the emergence of transnational, acephalous systems wherein *lex cryptographia* purports to operate autonomously across borders, emancipated from the cultural and national foundations that have traditionally conferred legal legitimacy¹⁵. Within these decentralized communities, legal authority remains both formally headless and spatially virtual, complicating conventional understandings of sovereignty, jurisdiction, and the enforcement of judgments.

Additionally, decentralization enables the development of what some theorists term "cloud communities"¹⁶ or state-like non-territorial polities that employ opt-in legal systems. This model ostensibly removes the need for compromise and deliberation on shared values – processes that have historically been regarded as essential to the democratic legitimacy of law¹⁷. Instead, legal authority would derive from voluntary participation and cryptographic verification rather than democratic authorisation.

However, the deterritorialized aspirations of blockchain systems encounter persistent constraints. Territorial states continue to assert jurisdictional authority over blockchain activities that produce effects within their borders¹⁸. Regulatory interventions – ranging from China's ban on cryptocurrency exchanges to the European Union's Markets in Crypto-Assets Regulation (MiCAR) and the US Genius Act – demonstrate that territorial sovereignty remains a formidable force shaping blockchain's actual operation, regardless of its ideological commitments¹⁹.

In this context, the European strategy for digital sovereignty deserves particular attention. The European Commission's policy framework – encompassing the Digital Decade Programme, the Data Governance Act, the Digital Services Act, and the AI Act – reflects a deliberate effort to reassert regulatory authority over transnational digital ecosystems, including blockchain-based systems²⁰. This strategy proceeds from the premise that territorial governance and digital innovation need not be mutually exclusive, and that the exercise of democratic sovereignty over technological infrastructure constitutes a precondition for the protection of fundamental rights. The digital sovereignty agenda thus provides an important counterpoint to the deterritorialization thesis: far from rendering territorial authority obsolete, the proliferation of decentralized technologies has prompted a renewed assertion of sovereign regulatory capacity, albeit adapted to the specificities of the digital environment.

Consequently, while code emerges as a novel symbolic referent in this legal framework – one that seeks to displace the trust traditionally invested in state institutions – this displacement remains incomplete and contested. The tension

14. JOHNSON-POST 1997.

15. WERBACH 2018.

16. ORGAD 2018.

17. HABERMAS 1999.

18. ZETZSCHE-BUCKLEY-ARNER-FÖHR 2018.

19. HOUBEN-SNYERS 2020.

20. On the European digital sovereignty strategy as a framework for asserting regulatory authority over digital ecosystems, see the European Commission's 2030 *Digital Compass: the European way for the Digital Decade* (COM(2021) 118) and the broader policy architecture encompassing the *Data Governance Act* (Regulation (EU) 2022/868), the *Digital Services Act* (Regulation (EU) 2022/2065), and the *Artificial Intelligence Act* (Regulation (EU) 2024/1689).

between blockchain's deterritorialized aspirations and the persistent relevance of territorial jurisdiction constitutes a central problematic requiring ongoing empirical and theoretical investigation.

2.3. The elusiveness of jurisdiction and the limits of enforcement

The core difficulty stems from the belief that blockchain technology can "fracture economic and social processes" and operate autonomously, "independently of any government or other centralized authority"²¹.

The decentralized and transnational nature of blockchain systems poses profound challenges to traditional concepts of jurisdiction and enforcement. These challenges operate at multiple levels: determining applicable law, establishing jurisdictional authority, and implementing effective enforcement mechanisms.

Traditionally, jurisdiction is defined either by the authority of a court to adjudicate cases or by the territory within which a court or government agency may exercise its power²². Decentralized systems deliberately challenge this geographical anchoring, leading to profound conflicts regarding applicable law and judicial authority. The decentralized blockchain structure is said to sever all legal ties to any specific territory²³.

This *a-territorial* and *a-spatial* dimension of the digital space means that decentralized networks operate across national borders, tending to remain scarcely regulated under domestic and supranational laws²⁴. The *a-territorial* character of blockchain networks fundamentally disrupts the geographic foundations upon which jurisdictional rules have historically been constructed.

2.3.1. Jurisdictional ambiguity and choice of law

Traditional private international law relies on connecting factors that link legal relationships to specific territories. The Rome I Regulation (EC 593/2008),

which governs choice of law for contractual obligations within the European Union, exemplifies this approach. Article 4 establishes a hierarchy of connecting factors, with particular emphasis on the "habitual residence" of the service provider or, in the absence of such identification, the place where the central administration is located.

However, these connecting factors become problematic – indeed, potentially meaningless – when applied to DAO or blockchain-based contractual arrangements. A DAO exists simultaneously everywhere and nowhere: its smart contracts execute on distributed nodes across multiple jurisdictions, its governance tokens may be held by pseudonymous participants globally dispersed, and its treasury may consist of cryptoassets with no physical location. Where is the "habitual residence" of such an entity? Where is its "central administration" when decision-making occurs through on-chain voting mechanisms without any physical headquarters?

The escape clause in Rome I (Article 4(3)) allows courts to apply the law of a country with which the contract is "manifestly more closely connected." However, this provision presupposes the existence of such a country – an assumption that decentralized systems deliberately challenge. The result is jurisdictional ambiguity that creates opportunities for regulatory arbitrage and forum shopping. Projects may structure their token distributions, governance mechanisms, and operational parameters specifically to avoid or minimise connections to jurisdictions with stringent regulatory requirements²⁵. This is achieved partly through jurisdictional ambiguity: DAOs are often designed without an official domicile, which complicates the application of corporate, tax, and capital market laws. Furthermore, the complexity of identifying parties in a distributed system makes it "almost impossible" to determine competent jurisdiction in a predetermined manner²⁶.

21. HUMMLER 2016.

22. THYSSE 2025.

23. BECKER 2022.

24. PONCIBÒ 2021.

25. ANUS-ALLAUDDIN 2025.

26. COUTINHO-PIRES-CORREIA BARRADAS 2024.

Moreover, DAOs present classification challenges that precede choice-of-law analysis. Are they partnerships? Unincorporated associations? Sui generis entities? The answer to this preliminary question determines which choice-of-law rules apply, yet the answer remains contested. This creates what might be termed “double indeterminacy”: uncertainty about both the applicable classification framework and the applicable substantive law.

A concrete illustration is provided by the litigation surrounding the bZx Protocol. Following a series of exploits in 2020 that resulted in losses exceeding USD 8 million, affected users faced the threshold question of whom to sue and where. The protocol had no incorporated entity, no registered office, and no identified governing body. Developers were pseudonymous or geographically dispersed, and governance token holders spanned multiple jurisdictions. Traditional connecting factors – domicile of the defendant, place of performance, place of the harmful event – yielded no clear answer, precisely because the system was designed to operate without the territorial anchoring upon which these factors depend²⁷.

2.3.2. Enforcement challenges in decentralized systems

Even when applicable law can be determined and jurisdiction established, enforcement presents formidable obstacles. Traditional legal enforcement presupposes the existence of identifiable defendants who can be served with process, whose assets can be located and seized, and who can ultimately be compelled to comply with judicial orders. Decentralized systems resist these assumptions at every step.

The concept of the “veil of decentralization” captures this dynamic: just as the corporate veil shields individual shareholders from liability, the architecture of decentralization creates a liability shield – but one without an identifiable entity behind it. There is no “DAO Inc.” to sue, no board of directors to hold accountable, no CEO to compel to testify. Legal process confronts a distributed network of pseudonymous participants, none of

whom may individually possess the authority or capacity to provide the relief sought.

Smart contract immutability compounds enforcement difficulties. Once deployed to the blockchain, code executes autonomously according to its programmed logic. A court order demanding that a smart contract cease operation, modify its behaviour, or reverse a transaction encounters a fundamental problem. There may be no party capable of implementing such an order. The code operates permissionlessly, continuing to execute regardless of legal judgments. While validators could theoretically coordinate to fork the blockchain and reverse transactions, such interventions contradict the ideology of immutability and face collective action problems.

The Tornado Cash saga offers a particularly instructive example. In August 2022, the US Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash, a decentralized mixing protocol used to anonymise cryptocurrency transactions. The sanctions targeted not an individual or a corporation but a set of smart contract addresses – marking the first time OFAC designated autonomous code as a sanctionable entity. Since the protocol operates autonomously on the Ethereum blockchain, the sanctions could not “shut down” the protocol itself; the smart contracts continued to function. Enforcement instead targeted peripheral human actors: the arrest of developer Alexey Pertsev in the Netherlands, who was subsequently convicted of money laundering by the Rechtbank Oost-Brabant, and the criminal prosecution of co-founder Roman Storm in the Southern District of New York. However, the legal framework underpinning the sanctions themselves proved fragile. In November 2024, the Fifth Circuit held in *Van Loon v. Department of the Treasury* that OFAC had exceeded its statutory authority, as immutable smart contracts lack the hallmarks of ownership and control required to constitute “property” under the International Emergency Economic Powers Act. OFAC subsequently delisted Tornado Cash in March 2025. Storm’s trial in August 2025 produced a mixed verdict: the jury convicted him of conspiracy to oper-

27. On the bZx Protocol exploits and the resulting jurisdictional difficulties, see the related litigation in *Sarcuni v. bZx DAO*, No. 22cv00618 (S.D. Cal. 2022), in which the court considered whether holders of the DAO’s governance tokens could be treated as general partners of a general partnership for purposes of liability and personal jurisdiction.

ate an unlicensed money transmitting business but deadlocked on the more serious money laundering and sanctions charges, with a retrial requested for October 2026. This sequence vividly illustrates both the limits of traditional enforcement when confronting genuinely decentralized code and the persistent tendency of regulators to re-centralise accountability by focusing on identifiable human actors at the system's periphery – even as courts increasingly question the legal basis for treating autonomous protocols as sanctionable entities²⁸.

Asset seizure – a traditional mechanism for satisfying judgments – becomes equally problematic. When smart contracts manage a DAO's treasury, private keys may be distributed via multi-signature arrangements or threshold cryptography. No single party may possess the unilateral capacity to transfer assets in compliance with a court order. Even if enforcement authorities could identify and compel cooperation from key-holders, cryptocurrency's censorship-resistant properties and the potential for assets to be transferred across chains create additional obstacles.

Cross-border coordination difficulties further undermine the effectiveness of enforcement. Blockchain networks operate globally, yet legal enforcement mechanisms remain primarily national. A judgment issued by a court in one jurisdiction may prove difficult or impossible to enforce in others, particularly when relevant parties or assets reside in jurisdictions with weak international cooperation frameworks or hostile attitudes toward such enforcement actions.

2.4. Disembodiment and the paradox of legal subjectivity

Decentralization significantly challenges traditional conceptions of legal subjectivity, which have

historically been constructed around the juridical concept of legal personality. This concept abstracts the legal person from biological particularity while simultaneously depending upon embodied human agency²⁹. Within the aspirational framework of *lex cryptographia*, the physical body is conceptually rendered as a non-programmable entity, ostensibly excluded from direct representation in blockchain legal systems, even as these systems continue to produce effects on embodied subjects.

This creates what might be understood as a dual movement: the body loses its authoritative position as the presumptive locus of legal agency while simultaneously being relegated to the status of a mere biological object external to the system's primary operations³⁰. Legal personality becomes increasingly detached from human embodiment, potentially migrating instead to algorithmic agents (such as agentic AI), smart contracts, or DAOs that operate according to programmatic logic rather than human will³¹.

However, this disembodiment proves paradoxical and incomplete in practice. Bodies remain stubbornly relevant to blockchain systems in multiple ways: through biometric identity verification systems that increasingly govern access; through the embodied labor of developers, miners, and users whose physical actions sustain the infrastructure; through the material consequences of algorithmic decisions that affect nutrition, healthcare, housing, and physical security; and through the legal recourse available when code produces harmful outcomes that territorial legal systems may still remedy³².

Furthermore, the fantasy of disembodied legal agency obscures important questions about power, inequality, and access. Who possesses the technical literacy, economic resources, and social capital

28. On the Tornado Cash sanctions and subsequent proceedings, see US Department of the Treasury, OFAC, Designation of Tornado Cash (8 August 2022), subsequently delisted on 21 March 2025 following the Fifth Circuit's ruling in *Van Loon v. Department of the Treasury* (26 November 2024); *United States v. Storm*, No. 1:23-cr-00430 (S.D.N.Y. 2023), in which a jury convicted Storm of conspiracy to operate an unlicensed money transmitting business but deadlocked on the money laundering and sanctions charges (6 August 2025), with a retrial requested for October 2026; *Rechtbank Oost-Brabant*, 14 May 2024, ECLI:NL:RBOBR:2024:2069 (conviction of Alexey Pertsev, currently under appeal before the Gerechtshof 's-Hertogenbosch).

29. NAFFINE 2009.

30. ROUVROY-BERNS 2013.

31. HACKER 2024; SCHOLZ 2017.

32. CENGIZ 2023; WATTERS 2023.

to participate meaningfully in supposedly neutral blockchain systems? Whose bodies are rendered more vulnerable by the withdrawal of interpretive flexibility and institutional oversight?³³ The unrepresented but consequential presence of the human body thus creates a constitutive tension within blockchain legal systems – a tension between the ideology of algorithmic autonomy and the persistent materiality of embodied human existence.

This transformation does not simply replace one form of legal subjectivity with another. Instead, it generates a complex field of competing modes of agency: the robotised presence of smart objects seamlessly integrated into algorithmic frameworks coexists uneasily with the excluded-yet-affected presence of biological bodies³⁴. Understanding this paradox requires moving beyond technological determinism to examine how different actors negotiate, resist, or are subjected to these new configurations of legal power.

2.5. Regulatory responses

Regulators and courts have begun developing strategies to address these challenges, though the approaches remain experimental and their efficacy is uncertain. Two developments merit particular attention so far: the Ooki DAO enforcement action and the European Union's Markets in Crypto-Assets Regulation.

2.5.1. The Ooki DAO Case

In September 2022, the US CFTC filed an enforcement action against Ooki DAO, marking a significant regulatory development. The CFTC alleged that Ooki DAO offered illegal leveraged trading of digital assets and failed to implement proper KYC and AML procedures³⁵. Rather than identifying individual defendants, the CFTC named the DAO itself and, critically, served the DAO's token holders collectively through governance forums and online platforms. The CFTC's theory rested

on functional control: token holders who participate in governance effectively control the DAO and therefore bear responsibility for its legal compliance. In June 2023, following Ooki DAO's deliberate non-appearance, the Northern District of California granted a default judgment, finding the DAO to be an unincorporated association under the Commodity Exchange Act and imposing a civil monetary penalty of \$643,542 alongside injunctive relief. The decision was hailed by the CFTC as precedent-setting, yet its practical significance remains uncertain. The judgment has not been enforced against individual token holders, and the broader regulatory landscape has shifted markedly: in April 2025, the CFTC Acting Chairman directed enforcement staff to align with the DOJ's "Ending Regulation by Prosecution" memorandum, which instructs prosecutors to cease "superimposing regulatory frameworks on digital assets" and to refrain from targeting platforms for the acts of their end users. The Ooki DAO case thus stands as a cautionary precedent from a regulatory era that may already be receding – though the underlying questions about the extent to which passive governance participants can be held liable for organisational misconduct remain unresolved.

2.5.2. EU MiCAR framework

MiCAR, which became fully applicable on 30 December 2024³⁶, seeks to identify functional equivalents to traditional financial actors and impose corresponding obligations on them. It establishes a typology of cryptoassets (e-money tokens, asset-referenced tokens, and other crypto-assets) with tailored requirements for each category; creates an authorisation regime for cryptoasset service providers (CASPs), capturing activities such as exchange services, custody, portfolio management, and investment advice; and – most relevant to the enforcement challenges discussed above – requires the identification of responsible "issuers" and "offerors" who bear legal obligations regarding dis-

33. ATZORI 2017.

34. EUBANKS 2018; SCHOLZ 2017; HAYLES 1999.

35. CFTC 2023.

36. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCAR). Titles III and IV on asset-referenced tokens and e-money tokens applied from 30 June 2024; the remaining provisions, including Title V on CASPs, became applicable on 30 December 2024.

closure, governance, and operational standards³⁷. For ostensibly decentralized projects, MiCAR's approach involves piercing through the rhetoric of decentralization to identify *de facto* controllers. Projects claiming to lack any responsible party will find such claims receive limited credence. Regulators may identify core developers, foundation entities, large token holders, or others exercising meaningful influence as responsible parties for regulatory compliance purposes³⁸.

Crucially, however, MiCAR itself acknowledges the limits of this approach. Recital 22 of Regulation (EU) 2023/1114 provides that cryptoasset services provided “in a fully decentralised manner without any intermediary” fall outside the Regulation's scope, and that cryptoassets without an identifiable issuer – such as Bitcoin – are excluded from Titles II through IV governing issuance obligations³⁹. Yet the exclusion is far from absolute: CASPs providing services in relation to such cryptoassets remain fully subject to MiCAR's requirements⁴⁰, thereby reasserting regulatory control through the intermediary layer even where the underlying protocol eludes direct regulation. This structure confirms the re-centralising dynamic analysed above: regulation gravitates toward the identifiable nodes at the system's periphery. The

notion of “full decentralization” is itself indeterminate, as MiCAR provides no definition of the concept, leaving the boundary between regulated and unregulated activity to case-by-case assessment by national competent authorities⁴¹. The coherence of this framework remains under review: Article 142 of MiCAR mandated the Commission to report, by 30 December 2024, on the “appropriate regulatory treatment of decentralised crypto-asset systems without an issuer or crypto-asset service provider”; EBA and ESMA published their Joint Report contributing to this assessment in January 2025, but the Commission's own report – which may include legislative proposals – had not been published as of early 2026⁴².

The early implementation data offers a preliminary assessment of this framework in operation. By late 2025, over 70 CASP authorisations had been granted across the EEA, with Germany and the Netherlands leading in licence issuance, alongside some 570 cryptoasset white papers submitted to national regulators⁴³. However, no MiCAR enforcement actions had been reported as of early 2026, and the transitional regime – under which existing providers may continue operating under national laws until 1 July 2026 – has revealed significant fragmentation, with Member States adopt-

37. See Arts. 4–15 (Title II, public offerings of crypto-assets other than ARTs and EMTs), Arts. 16–47 (Title III, ARTs), Arts. 48–58 (Title IV, EMTs), and Arts. 59–83 (Title V, CASPs), Regulation (EU) 2023/1114. On the general approach of functional equivalence, see HOUBEN–SNYERS 2020; ZETZSCHE–BUCKLEY–ARNER–FÖHR 2018.

38. CENGİZ 2023; DE FILIPPI–MANNAN–REIJERS 2022. On the concept of “decentralization theatre” in the context of governance structures that claim to be decentralized while retaining effective control by identifiable actors, see ARAMONTE–HUANG–SCHRIMPF 2021.

39. Recital 22, Regulation (EU) 2023/1114: “Where cryptoasset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation” See also *ibid.*, second sentence: “Where cryptoassets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation”. Art. 4(2) further exempts from Title II cryptoassets automatically created as a reward for the maintenance of the DLT or the validation of transactions.

40. Recital 22, third sentence, Regulation (EU) 2023/1114: “Cryptoasset service providers providing services in respect of such cryptoassets should, however, be covered by this Regulation”.

41. On the interpretive difficulties, see DE FILIPPI–MANNAN–REIJERS 2022; ARAMONTE–HUANG–SCHRIMPF 2021. MiCAR does not define “full decentralisation”, leaving open the question of at which layer of the DeFi stack an intermediary must operate in order to bring the service within the Regulation's scope.

42. Art. 142, Regulation (EU) 2023/1114. ESMA 2025: The Joint Report found that DeFi remains a niche phenomenon, with value locked in DeFi protocols representing approximately 4% of total crypto-asset market capitalisation globally.

43. Data from ESMA Interim MiCA Register, updated December 2025. On the licensing landscape see also the EBA 2026 Work Programme (published 1 October 2025).

ing grandfathering periods ranging from 6 to 18 months⁴⁴. This disparity undermines MiCAR's harmonising ambition and has created uneven market access across the Union. Moreover, in December 2025, the European Commission announced plans to centralise supervision of the most significant CASPs under ESMA⁴⁵ – a development that, if adopted, would further illustrate the re-centralising dynamic at work: even a regulation designed to accommodate decentralized technologies ultimately gravitates toward the identification of accountable centres.

2.5.3. *Emerging strategies*

These regulatory responses reflect broader strategies to address decentralisation's enforcement challenges.

First, functional analysis: looking beyond formal structures to identify who actually controls systems and allocating responsibility accordingly.

Second, participant liability: extending liability to ecosystem participants – validators, liquidity providers, governance participants – based on their roles and degree of involvement.

Third, service provider regulation: focusing enforcement on centralized points of contact with the traditional financial system, such as exchanges and custodians, even when the underlying protocols remain decentralized.

Fourth, technical mandates: requiring that smart contracts and protocols incorporate compliance functionality, such as transaction monitoring or the ability to respond to legal orders, as a condition of regulatory approval.

These strategies represent adaptations of traditional legal tools to novel technological circumstances. Their long-term efficacy remains uncertain, dependent on international coordination, technical feasibility, and the willingness of courts to accept novel theories of responsibility and control.

3. Law as a system founded on “centres of attribution”

The inevitable question is that the traditional legal paradigm operates fundamentally as a system founded upon and necessitating identifiable “centres of attribution”, a structure essential for realising the primary function of law as the main tool for social order. This system of centralized law is typically characterised by being imposed from above by an authoritative institution whose power to rule is both genuine and legitimate, deriving from political action and the will of the rulers. This political authority grants the State, or its designated agencies, the requisite monopoly of coercive power for the ultimate enforcement and application of legal sanctions. This structured exercise of force, balanced against individual rights, constitutes the core mechanism of the rule of law.

The efficacy and certainty indispensable to this traditional legal system rely on defining and fixing these centres across several critical domains. Organisational law provides the necessary “impermeable barriers” and frameworks for groups of people, allowing the system to structure accountability and risk. This institutional anchoring of accountability is non-negotiable within the current paradigm.

Furthermore, this reliance on fixed centres allows the legal system to act as a crucial “supplier of fictional certainty” where technology or reality itself cannot provide absolute deterministic outcomes. This “institutional backstop” is critical, particularly in complex commercial spheres. For instance, concepts fundamental to modern finance, such as achieving absolute “operational finality” in transactions, are acknowledged as nearly impossible⁴⁶; therefore, the law intervenes to impose “legal finality” through presumptions and rules, providing the certainty required to mitigate systemic risks, particularly those arising in insolvency or bankruptcy proceedings⁴⁷. The coherence of the rule of law is thus preserved by defining these ex-

44. Art. 143(3), Regulation (EU) 2023/1114, provides a maximum grandfathering period of 18 months (until 1 July 2026) but allows Member States to reduce or opt out of the transitional regime. Several Member States adopted shorter periods of 6 to 12 months, creating asymmetric market access.

45. European Commission, Market Integration Package within the Savings and Investments Union Strategy, 4 December 2025, proposing to confer on ESMA the supervision of the most significant CASPs.

46. BARRESI 2023.

47. MARTINO-RINGE 2024.

plicit points of connection and control, enabling reliable adjudication and the protection of established rights.

The core challenge posed by technology-based decentralization, and the concept of *lex cryptographia*, lies in their foundational ethos, which seeks radical emancipation from the constitutive legal dimensions: territory, language, and the physical body. The challenge, therefore, is not simply one of regulatory adaptation but of confronting whether law as we have understood it – as a system of centred attribution – can meaningfully operate in a genuinely acephalous, distributed environment, or whether the persistence of legal order necessarily requires the (re)imposition of identifiable centres, even within ostensibly decentralized structures.

It should be acknowledged, however, that not all scholars regard this tension as irresolvable within existing legal frameworks. A significant strand of legal scholarship maintains that the difficulty of applying traditional attribution mechanisms to decentralized systems does not demonstrate their structural inadequacy, but rather the need for creative adaptation. Authors such as Werbach have argued that blockchain systems inevitably produce identifiable *loci* of control – core developers, foundation entities, dominant token holders – and that existing legal tools, properly deployed, can reach these actors⁴⁸. Similarly, the functional analysis employed by regulators in the Ooki DAO case and under MiCAR proceeds from the premise that behind every “decentralized” system there exist human agents exercising meaningful influence, and that legal attribution can attach to their conduct. From this perspective, the problem is not that centres of attribution have disappeared, but that they have become less visible and must be identified through more sophisticated analytical methods. This counter-position deserves serious engagement. The question, however, is whether the cen-

tres of attribution that regulators and courts manage to identify within decentralized ecosystems are structurally equivalent to those presupposed by traditional legal paradigms, or whether they represent a qualitatively different – and potentially less stable – form of legal anchoring. The functional identification of *de facto* controllers, while practically useful, may not fully substitute for the formal, institutionally defined centres that underpin the systematic operation of legal order⁴⁹.

To address this need for research, it is necessary to verify that decentralization does not hinder but rather facilitates the achievement of the constitutional objectives of centralized legal systems. In addition, it is key to ensure that this technological decentralization does not erode the fundamental principles and values upon which Constitutions are founded. In a technologically decentralized context, power is not merely granted but rather intercepted through solutions that begin with fragmentation and ultimately converge towards unity. This approach stands in contrast to the more conventional top-down approach, where power is assumed and then organised to serve the community.

3.1. The theoretical facilitation of constitutional ideals

Having examined the fundamental challenges that decentralization poses to traditional legal paradigms – the displacement of foundational symbolics, the deterritorialization of authority, the elusiveness of jurisdiction, the paradoxes of legal subjectivity, and the resistance to centres of attribution – we must now consider the normative claims made on behalf of blockchain technology. Proponents argue that decentralized systems may facilitate certain constitutional ideals even as they challenge traditional legal structures. This subsection examines these claims while maintaining critical awareness of tensions with the preceding critique.

48. WERBACH 2018, particularly chapters 4–6, where the author argues that blockchain systems generate new forms of trust rather than eliminating the need for institutional anchoring. See also CENGİZ 2023, who observes that the governance structures of ostensibly decentralized protocols consistently converge towards identifiable centres of decision-making.

49. For a nuanced analysis of the gap between functional and formal centres of attribution, see DE FILIPPI-MANNAN-REIJERS 2022, who characterise blockchain technology as “alegal” – operating in a space that is neither fully within nor fully outside the legal order, and therefore requiring novel conceptual tools rather than mere adaptation of existing ones.

Decentralization, in its ideal form, embodies features that resonate strongly with modern constitutional and democratic ideals, particularly concerning transparency, efficiency, and participation.

One primary objective of any modern legal system is to ensure predictable, fair, and accountable governance. Decentralization proponents argue that the technology achieves this through algorithmic transparency and the elimination of traditional “Single Points of Failure” associated with human-centric centralized institutions. According to this perspective, the use of open-source code and on-chain records in decentralized systems ensures data is publicly verifiable and difficult to manipulate. This enhances accountability by allowing real-time monitoring of decisions and financial flows, an objective that many state-based systems struggle to meet, especially in complex bureaucratic or financial operations⁵⁰. Decentralization would aim to disperse power away from a central entity that might otherwise be susceptible to regulatory capture, corruption, or misuse of power. This would align with the constitutional goal of preventing authoritarian drift and ensuring that the government is subject to the rule of law⁵¹.

Moreover, decentralized applications (dApps) and DAOs, which promote models of direct and collaborative decision-making, would offer new ways to realise the constitutional ideals of political participation and effective justice. DAOs and platforms like *Kleros* and *Jur* would enable liquid democracy and collective dispute resolution, leveraging consensus mechanisms to govern resource allocation and resolve conflicts. This can be interpreted as facilitating participatory governance, enhancing citizen involvement beyond traditional representative structures. Decentralized dispute resolution systems specifically target low-value, high-volume transactions, providing affordable mechanisms to solve “micro-claims” that often lack affordable recourse in traditional, expensive court systems. This expands access to justice, a core constitutional objective.

3.2. The fundamental conflict with constitutional prerequisites

Despite these potential benefits, the core claim of technological decentralization fundamentally clashes with essential constitutional objectives, particularly those concerning sovereignty, legal certainty, and accountability.

Constitutional systems presuppose the existence of ultimate authority – a sovereign capable of making binding collective decisions and resolving conflicts authoritatively. Decentralized systems resist this requirement. By design, they lack ultimate authority: no entity can unilaterally modify protocols, reverse transactions, or resolve disputes authoritatively. This refusal of sovereignty is presented as a virtue – liberation from hierarchical power. Nevertheless, it creates fundamental problems for constitutional governance. How are constitutional amendments adopted? How are irreconcilable conflicts resolved? How is the boundary between permissible and impermissible conduct authoritatively determined?

Constitutional authority traditionally operates through territorial jurisdiction: the State exercises sovereign power within defined borders. As seen, Blockchain aspires to transcend such territorial limitations, creating legal orders without geographic anchoring. However, this deterritorialization should eliminate one of constitutionalism’s foundational mechanisms: the definition of a political community bound together by shared subjection to common authority.

Moreover, governance rights derive from token ownership, which reflects economic power rather than equal citizenship. The initial distribution of tokens typically occurs through sales or airdrops that favour early participants, insiders, or those with capital to invest – not through any process claiming democratic legitimacy. Subsequent distributions through the market further concentrate tokens in the hands of those with greater resources. “Governance by numbers”⁵² replaces deliberative democracy with algorithmic aggregation of preferences but eliminates the deliberative process through which preferences are formed, refined,

50. NABBen 2023; DE FILIPPI-WRIGHT 2018; WERBACH 2018.

51. REIJERS-MANNAN-DE FILIPPI 2024; ATZORI 2017; DE FILIPPI-LOVELUCK 2016; MUMFORD 1964.

52. ROUVROY-BERNS 2013.

and synthesised into collective judgments. Cloud communities and opt-in systems allow fragmentation: those who disagree can exit rather than compromise. While this may satisfy individuals' preferences, it abandons the constitutional project of constructing shared frameworks for collective life despite disagreement.

Empirically, ostensibly decentralized systems often exhibit significant power concentration. Core developers exercise disproportionate influence over protocol evolution: while anyone can formally propose changes, practical authority resides with those possessing technical expertise and credibility within developer communities. Their decisions about which improvements to implement, which bugs to prioritise, and how to respond to crises shape system evolution more profoundly than token holder votes. Token distribution patterns reveal similar concentration. "Whales" – holders of prominent token positions – dominate governance outcomes when they choose to participate. Analysis of DAO voting patterns consistently shows highly unequal participation and influence⁵³.

These distributional inequities may give rise to oligarchic governance structures beneath decentralization's egalitarian rhetoric⁵⁴. The plutocratic character of token voting means that those who already possess wealth can entrench their advantages by controlling protocol governance, putting them in a position to evade accountability. By disclaiming the existence of any controlling party, they deny that anyone owes fiduciary duties. Token holders disclaim responsibility despite exercising governance rights. Developers claim merely to propose code changes that others are free to reject. Platform operators assert they simply facilitate access to decentralized protocols. Everyone disclaims control, yet collectively the system operates and produces consequences for participants. This structure creates a moral hazard: those who exercise effective control over systems escape the legal obligations traditionally accompanying such power. They enjoy the benefits of governance partici-

pation – the ability to shape protocols in ways that advantage their interests – without bearing corresponding responsibilities to those affected by their decisions.

The enforcement blind spots discussed in Section 2 compound these accountability deficits. Even when legal duties theoretically attach, enforcement proves difficult or impossible when responsible parties cannot be identified or when their pseudonymity and distributed coordination frustrate the legal process.

4. The necessity of hybridisation and legal anchoring

This analysis demonstrates that pure decentralization risks undermining constitutional accountability mechanisms. Consequently, pragmatic approaches favor hybrid arrangements that leverage blockchain's technical advantages while preserving essential legal safeguards.

DLTs require institutional and legal anchors to function responsibly within the broader economy. As a result, the approach so far has primarily been for law to engage actively with these new organisational solutions, as the Ricardian contract approach confirms, enabling smart contracts to function seamlessly within established legal frameworks. Another adaptation is to evolve regulatory frameworks to ensure that technological innovations can coexist with traditional legal functions. Jurisdictions are tasked with defining rules that establish the functional equivalence of these technologies, all while safeguarding fundamental rights. An exemplary initiative highlighting this need is the EU's DLT Pilot Regime, which mandates the presence of an identifiable and liable operator for DLT market infrastructures⁵⁵. This requirement underscores the importance of having a centralized, accountable entity that can interface with the legal system, even within decentralized contexts. Another solution to gain traction is to address governance through a polycentric lens⁵⁶. This means recognising that multiple governing

53. FRITSCH-MÜLLER-WATTENHOFFER 2024; NABBen 2023.

54. MESSIAS-IDE 2025; WEIDENER-LAREDO-KUMAR-COMPTON 2025; MESSIAS-PAHARI-CHANDRASEKARAN et al. 2023.

55. Regulation (EU) 2022/858; ZACCARONI 2022.

56. EUROPEAN UNIVERSITY INSTITUTE 2024; GAZI-TRECCANI-MORINI-SAHDEV 2022; CARLISLE-GRUBY 2019; ALIGICA-TARKO 2012; OSTROM 2010.

bodies – spanning local, national, international, and private decentralized networks – must interact and coordinate effectively. Establishing clear rules for how on-chain regulations align with off-chain national or international laws becomes crucial in this framework.

Concrete examples from the financial sector illustrate the practical necessity of such hybridisation. The experience of decentralized lending protocols such as *Aave* and *Compound* demonstrates that, even within architectures designed to eliminate intermediaries, governance structures progressively re-centralise around identifiable actors. *Aave*'s governance framework, for instance, relies on a delegated voting system in which a small number of prominent delegates exercise disproportionate influence over protocol parameters. Similarly, blockchain-based supply chain management initiatives – such as those deployed in the agri-food sector for traceability and food safety certification – have required the identification of responsible data custodians and legal guarantors to satisfy regulatory requirements under EU food safety law (Regulation (EC) 178/2002). These cases confirm that the integration of decentralized technologies into legally regulated domains invariably demands the reconstitution of identifiable centres of attribution⁵⁷.

Nevertheless, efforts to harness the benefits of decentralization without reverting to a pre-political state dominated by unaccountable private interests require deliberate and constructive cooperation with existing legal structures. Such cooperation should prioritize regulations that mandate governance transparency, enforce accountability, and protect fundamental rights. Embracing decentralization should be viewed as an organizational theory that enhances the effectiveness of the legal order, rather than as a standalone political theory capable of supplanting it.⁵⁸ The solution is necessarily multi-layered, involving both the adaptation of existing legal frameworks and the strategic introduction of new, technology-aware legal and institutional mechanisms. This approach seeks to balance the code-based *lex cryptographia* with the state-based rule of law.

5. Beyond functional equivalence: the imperative of institutional innovation

The nature of decentralized systems, transcending territorial boundaries and relying on code for execution, would demand flexibility in legal classification and execution.

For tokenization, legal fitness requires moving beyond rigid conceptual definitions towards a functional analysis. Tokens are often polyhedral, potentially fulfilling multiple legal roles depending on their characteristics and the context⁵⁹. While technological neutrality and functional equivalence provide the indispensable lens for jurists to analyse and classify new digital phenomena, they function best when the latest technology aligns with existing institutional logic (e.g., highly centralized, entity-based DLTs). When encountering truly disruptive elements – such as the inherent probabilistic finality of PoW consensus⁶⁰, the anonymity of users, or the anti-institutional ethos of DAOs – these principles reveal their inadequacy. They provide a descriptive analysis (what the technology *does* economically) but falter in prescribing solutions for the new normative concerns (how to assign accountability and ensure justice when political and territorial constraints are deliberately circumvented).

The theoretical and practical implications suggest that regulatory frameworks need to adopt a nuanced approach. First and foremost, it is essential to embrace functional regulatory standards. However, it is not a convincing argument that regulations should focus on the economic activities being performed rather than the technological specifics, such as defining a token as a security irrespective of its underlying code. Additionally, there is a need to mandate legal bridges that address the challenges posed to core legal principles like property rights, liability, and finality. The law should actively work to create these “legal links”, which may involve establishing new legal categories for decentralized entities and categories or explicitly connecting on-chain technical realities to off-chain legal frameworks through complete tokenization.

57. On the re-centralisation dynamics in DeFi governance, see FRITSCH–MÜLLER–WATTENHOFER 2024.

58. ACHEBE–ONYEKA–ANYANWU–UMEH 2024.

59. ESMA 2019.

60. BARRESI 2023; NAKAMOTO 2008.

Moreover, legal intervention must acknowledge the inherent trade-offs involved in these scenarios. Efforts to impose conventional accountability mechanisms, such as requiring a liable operator, could unintentionally undermine decentralization that these technologies aim to achieve, leading to increased centralization⁶¹. Therefore, the objective is not to achieve total technological integration but rather to foster a constructive dialogue in which

legal safeguards are introduced to uphold fundamental values, such as human dignity and fairness, within these emerging transnational regimes.

In conclusion, technological norms and functional equivalence are far from obsolete; instead, they need to be thoughtfully balanced with the introduction of tailored legal rules and institutional requirements, particularly in areas where technological design choices pose unique and unacceptable societal risks.

References

- V.C. ACHEBE, M.C. ONYEKA, A.C. ANYANWU, A.C. UMEH (2024), *Blockchain as a Legal Compliance Infrastructure: Reinventing Corporate Governance and Internal Control Systems*, in “International Journal of Scientific Research in Science and Technology”, vol. 11, 2024, n. 4
- P.D. ALIGICA, V. TARKO (2012), *Polycentricity: From Polanyi to Ostrom, and Beyond*, in “Governance”, vol. 25, 2012, n. 2
- M. ANUS, A. ALLAUDDIN (2025), *The Legal Fiction Of “Decentralization”: How DAOs Are Accidentally Creating Unregulated Financial Entities*, in SSRN, 2025
- S. ARAMONTE, W. HUANG, A. SCHRIMPF (2021), *DeFi Risks and the Decentralisation Illusion*, in “BIS Quarterly Review”, 2021
- M. ATZORI (2017), *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, in “Journal of Governance and Regulation”, vol. 6, 2017, n. 1
- R.G. BARRESI (2023), *The Evolution of the Finality of Payment or “How RTGSs, Instant Payment Systems, and DLT Platforms Change the Concept of Money”*, in F. Zatti, R.G. Barresi (a cura di), “Digital Assets and the Law”, Routledge, 2023
- K. BECKER (2022), *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, in “Law and Critique”, vol. 33, 2022, n. 2
- S. BLEMUS (2018), *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, in SSRN, 2018
- B. CAPPIELLO, G. CARULLO (2021), *Introduction: The Challenges and Opportunities of Blockchain Technologies*, in B. Capiello, G. Carullo (a cura di), “Blockchain, Law and Governance”, Springer, 2021
- K. CARLISLE, R.L. GRUBY (2019), *Polycentric Systems of Governance: A Theoretical Model for the Commons*, in “Policy Studies Journal”, vol. 47, 2019, n. 4
- F. CENGIZ (2023), *Blockchain Governance and Governance via Blockchain: Decentralized Utopia or Centralized Dystopia?*, in “Policy Design and Practice”, vol. 6, 2023, n. 4
- CFTC (2023), *Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory*, 2023
- F.P. COUTINHO, M.L. PIRES, B. CORREIA BARRADAS (2024), *Blockchain and the Law: Dogmatics and Dynamics*, T.M.C. Asser Press, 2024
- P. DE FILIPPI, B. LOVELUCK (2016), *The Invisible Politics of Bitcoin*, in “Internet Policy Review”, vol. 5, 2016, n. 3

61. WERBACH 2018.

- P. DE FILIPPI, M. MANNAN, W. REIJERS (2022), *The A legality of Blockchain Technology*, in “Policy and Society”, vol. 41, 2022, n. 3
- P. DE FILIPPI, A. WRIGHT (2018), *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018
- P. DE FILIPPI, A. WRIGHT (2015), *Decentralised Blockchain Technology and the Rise of Lex Cryptographia*, in SSRN, 2015
- M. DORIA, F. BASSAN, M. RABITTI, A. SCIARRONE ALIBRANDI, U. MALVAGNA (2024), *Caratteristiche degli smart contracts*, in “Questioni di Economia e Finanza (Occasional Papers)”, 2024, n. 683
- Q. DUPONT (2017), *Experiments in Algorithmic Governance*, in “Bitcoin and Beyond”, Routledge, 2017
- ESMA (2025), *Joint EBA-ESMA Report on the recent developments in crypto-assets (Article 142 of MiCAR)*, in esma.europa.eu, 2025
- ESMA (2019), *Advice on Initial Coin Offerings and Crypto-Assets*, in esma.europa.eu, 2019
- V. EUBANKS (2018), *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2018
- EUROPEAN UNIVERSITY INSTITUTE (2024), *Blockchain Technology and Polycentric Governance*, Publications Office of the European Union, 2024
- S.E. FISH (1989), *Doing What Comes Naturally: Change, Rhetoric, and the Practice of Theory in Literary and Legal Studies*, Duke University Press, 1989
- R. FRITSCH, M. MÜLLER, R. WATTENHOFER (2024), *Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?*, in “Internet Computing”, vol. 28, 2024, n. 3
- S. GAZI, M. TRECCANI, M. MORINI, N. K. SAHDEV (2022), *Blockchain as Commons: Applying Ostrom's Polycentric Approach to Blockchain Governance*, in SSRN, 2022
- J. GRIMMELMANN (2021), *All Smart Contracts Are Ambiguous*, in “Journal of Law & Innovation”, vol. 2, 2021, n. 1
- J. HABERMAS (1999), *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*, MIT Press, 1999
- P. HACKER (2024), *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence: Complementary Impact Assessment*, European Parliamentary Research Service Study, PE 762.861, 2024
- H.L.A. HART, L. GREEN (2012), *The Concept of Law*, 3rd edn, Oxford University Press, 2012
- N.K. HAYLES (1999), *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*, University of Chicago Press, 1999
- M. HILDEBRANDT (2018), *Algorithmic Regulation and the Rule of Law*, in “Philosophical Transactions of the Royal Society A”, vol. 376, 2018, n. 2128
- R. HOUBEN, A. SNYERS (2020), *Crypto-Assets – Key Developments, Regulatory Concerns and Responses*, PE 648.779, European Parliament, 2020
- K. HUMMLER (2016), *Blockchain – der nächste Wohlstandsschock*, in “Neue Zürcher Zeitung”, 2016
- G. ITZCOVICH (2020), *“Something More Lively and Animated Than the Law”: Institutionalism and Formalism in Santi Romano's Jurisprudence*, in “Ratio Juris”, vol. 33, 2020, n. 2
- D.R. JOHNSON, D.G. POST (1997), *Law And Borders – The Rise of Law in Cyberspace*, in SSRN, 1997
- H. Kelsen (1945), *General Theory of Law and State*, Harvard University Press, 1945

- T. LAI (2021), *Blockchain, Law and Governance: General Conclusion*, in B. Cappiello, G. Carullo (eds.), "Blockchain, Law and Governance", Springer, 2021
- L. LESSIG (2006), *Code: Version 2.0*, 2nd edn, Basic Books, 2006
- E.D. MARTINO, W.G. RINGE (2024), *The Social Cost of Blockchain: Externalities, Allocation of Property Rights, and the Role of the Law*, Institute of Law and Economics Working Paper 2024 No. 80, 2024
- J. MESSIAS, A. IDE (2025), *Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs*, in arXiv, 2510.05830, 2025
- J. MESSIAS, V. PAHARI, B. CHANDRASEKARAN, K.P. GUMMADI, P. LOISEAU (2023), *Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts*, in arXiv, 2305.17655, 2023
- L. MUMFORD (1964), *Authoritarian and Democratic Technics*, in "Technology and Culture", vol. 5, 1964, n. 1
- K. NABBEN (2023), *Blockchain Governance: Accountability in Decentralised Technology Communities*, in Kelsie – on the cataclysmia of digital infrastructure – Substack, 2023
- N. NAFFINE (2009), *Law's Meaning of Life: Philosophy, Religion, Darwin and the Legal Person*, Bloomsbury Publishing, 2009
- S. NAKAMOTO (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008
- L. ORGAD (2018), *Cloud Communities: The Dawn of Global Citizenship?*, in Globalcit, 2018
- E. OSTROM (2010), *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, in "American Economic Review", vol. 100, 2010, n. 3
- C. PONCIBÒ (2021), *Blockchain and Comparative Law*, in B. Cappiello, G. Carullo (eds.), "Blockchain, Law and Governance", Springer, 2021
- W. REIJERS, M. MANNAN, P. DE FILIPPI (2024), *The Emergence of Blockchain Constitutionalism*, in G. De Gregorio, O. Pollicino, P. Valcke (eds.), "The Oxford Handbook of Digital Constitutionalism", Oxford University Press, 2024
- A. ROUVROY, T. BERNS (2013), *Gouvernementalité Algorithmique et Perspectives d'émancipation*, in "Réseaux", vol. 177, 2013
- L.H. SCHOLZ (2017), *Algorithmic Contracts*, in "Stanford Technology Law Review", vol. 20, 2017
- W. THYSSE (2025), *Decentralized Law: The Power of Blockchain to Transform the Broken Legal System*, Thyse Publishing, 2025
- P. UNGUREANU, F. BELLESIA, C. COCHIS (2025), *Dealing with Blame in Digital Ecosystems: The DAO Failure in the Ethereum Blockchain*, in "Technological Forecasting and Social Change", vol. 215, 2025
- M. VERSTRAETE (2020), *The Stakes of Smart Contracts*, in "Loyola University Chicago Law Journal", vol. 50, 2020, n. 3
- C. WATTERS (2023), *When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment*, in "Laws", vol. 12, 2023, n. 33
- L. WEIDENER, F. LAREDO, K. KUMAR, K. COMPTON (2025), *Delegated Voting in Decentralized Autonomous Organizations: A Scoping Review*, in "Frontiers in Blockchain", vol. 8, 2025
- K. WERBACH (2018), *The Blockchain and the New Architecture of Trust*, MIT Press, 2018
- G. ZACCARONI (2022), *Decentralized Finance and EU Law: The Regulation on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology*, in "European Papers", vol. 7, 2022

D.A. ZETZSCHE, R.P. BUCKLEY, D. W. ARNER, L. FÖHR (2018), *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, in SSRN, 2018



DAVIDE BALDINI

Between the theory and practice of human oversight: Towards specialized AI regulatory sandboxes

Human oversight has become a flagship safeguard in AI governance frameworks, yet its real-world performance is uneven. Empirical studies show that humans supervising automated systems are vulnerable to automation bias and organizational incentives that reduce oversight to a box-ticking exercise. More fundamentally, humans and machines reason in profoundly different ways, making their integration far from straightforward. EU secondary law – most notably the GDPR and the AI Act – requires ‘meaningful’ and ‘effective’ human oversight, but offers limited operational guidance on how to achieve it. This paper argues that specialized AI regulatory sandboxes for human oversight can bridge this theory-practice gap. After mapping the legal obligations and practical shortcomings of human oversight, the paper argues how the AI Act’s regulatory sandbox regime can be leveraged to test concrete oversight models, metrics, and workflows in controlled conditions. It further provides recommendations for the governance of human oversight-specific sandboxes. The paper thus offers a policy proposal to convert open-textured legislative mandates on human oversight into evidence-based practices, reduce fragmentation across Member States, and strengthen both innovation and fundamental-rights protection in the EU’s AI governance.

Human oversight – AI Act – GDPR – Regulatory sandboxes – European Union

Tra teoria e pratica della sorveglianza umana dei sistemi di IA: verso sandbox regolatorie specializzate

La sorveglianza umana dei sistemi di IA (“human oversight”) è diventata una delle principali misure di governance dell’IA, ma la sua efficacia pratica risulta disomogenea. Studi empirici mostrano che gli esseri umani chiamati a supervisionare sistemi automatizzati sono vulnerabili all’*automation bias* e a incentivi organizzativi che riducono l’attività di sorveglianza umana a un mero adempimento formale. Ancora più radicalmente, esseri umani e sistemi di IA ragionano in modi profondamente diversi, rendendo l’integrazione tra i due particolarmente complessa. Il diritto dell’Unione – in particolare il GDPR e l’AI Act – richiede forme di human oversight “significative” ed “effettive”, offrendo però indicazioni operative limitate su come realizzarle. Questo contributo sostiene che sandbox regolatorie specializzate per la sorveglianza umana dei sistemi di IA possano colmare tale divario tra teoria e pratica. Dopo aver analizzato gli obblighi normativi e le principali criticità applicative della sorveglianza umana, il paper illustra come il regime delle sandbox previsto dall’AI Act possa essere utilizzato per testare modelli di supervisione, metriche e processi operativi in condizioni controllate. Vengono inoltre fornite raccomandazioni sulla governance di sandbox specificamente dedicate alla sorveglianza umana. Il contributo delinea così una proposta di policy volta a convertire obblighi legislativi ampi e indeterminati in pratiche basate sull’evidenza, ridurre la frammentazione tra Stati membri e rafforzare sia l’innovazione, sia la tutela dei diritti fondamentali nella governance UE dell’IA.

Sorveglianza umana – AI Act – GDPR – Sandbox regolatorie – Unione europea

The author is a PhD candidate in European and Transnational Legal Studies, pursuing a double PhD degree between Florence University (Italy) and Maastricht University (the Netherlands)

SUMMARY: 1. Introduction. – 2. Human oversight obligations under EU law. – 2.1. Human oversight in the GDPR. – 2.2. Human oversight in the AI Act. – 3. The practical shortcomings of human oversight. – 3.1. Cognitive and psychological limits. – 3.2. Organizational and systemic constraints. – 4. AI regulatory sandboxes under the AI Act. – 4.1. Origins and rationale of regulatory sandboxes. – 4.2. Design and operation in the EU context. – 5. A Proposal for specialized AI regulatory sandboxes for human oversight. – 5.1. Governance and institutional design. – 5.2. Selection criteria and operational focus. – 6. Conclusions and path forward.

1. Introduction

Human oversight has long been one of the primary legislative responses to the growing use of AI systems for automated decision-making in our society. Human oversight measures have been embedded in policy discourse as a safeguard against inaccurate and discriminatory algorithmic outputs, as a tool to maintain human accountability over the final decision, and as a symbolic guarantee that critical decisions remain under meaningful human control¹.

In legal and policy terms, human oversight of AI systems comes in different flavours and may take different operational forms. The main ones identified in the literature are the “human-in-the-loop”, where the overseer needs to validate each algorithmic output before it can take effect (in which case, the AI system acts as a decision support),

“human-on-the-loop”, where the overseer has full visibility and power to intervene at any time, for example on request from the affected individual, and “human-in-command”, where the overseer retains ultimate decision-making authority over when and how to use the system².

Intuitively, human oversight is often framed as offering the best of both worlds: the efficiency, scale, and data-processing capabilities of machines combined with the moral reasoning, contextual understanding, and discretionary judgment of humans. This “Better Together” argument aligns with a long-standing regulatory instinct to counterbalance the perceived dehumanising risks of automation with a reassertion of human agency and is often underpinned by a rhetoric of “trustworthy” and “human-centric” AI, as is notably the case in the context of the EU’s Artificial Intelligence Act (“AI Act”)³.

1. For an overview of the widespread adoption of human oversight as a safeguard in many supranational legal instruments related to AI regulation, see: PANEZI 2024, pp. 9-11.
2. This tripartition has been endorsed by the influential High-Level Expert Group’s Guidelines for Trustworthy AI, which provided the groundwork for the European Commission’s first draft of the AI Act (HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE 2019 p. 16), and subsequently adopted by many AI Act commentators, including: FINK 2025, pp. 2-3; PANEZI 2024, p. 12; ENQVIST 2023, p. 513.
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, in particular Rec. (1), (27) and (176).

Yet, as emerging empirical research⁴ and insights from cognitive psychology⁵ demonstrate, this intuition is often misplaced or, at the very least, overly optimistic. Research reveals that simplistic assumptions about inserting human review into algorithmic decision-making often fail to address its underlying gigantic complexities⁶, and may even worsen already-present algorithmic bias and discrimination or introduce unlawful human bias over unbiased algorithmic decisions⁷. In this respect, it emerges that humans do not simply act as neutral “quality-control” agents: they are prone to their own conscious or unconscious biases, misunderstanding how the underlying technology works, often showing over-reliance and under-scrutiny of algorithmic outputs (automation bias), or the inverse problem of algorithmic aversion, when algorithmic outputs are unjustifiably disregarded.

One of the main reasons of these shortcomings is that humans and machines reasoning, despite being apparently similar, function in dramatically different ways; as a consequence, humans and machines are not readily compatible decision-making partners: algorithms mimic human reasoning capabilities, but in fact operate as “prediction machines”, operating inferences and pro-

ducing outputs from extremely vast and obscure (at least, for a human) statistical correlations⁸. This remains true even when they carry out seemingly human-like tasks such as producing natural language outputs, which is the case for AI systems based on Large-Language Models (LLM) that have increasingly been popularized since the launch of ChatGPT in late 2022. Humans, by contrast, do not draw inferences from billions of data points like machines do, but instead rely on qualitative, contextual, and often morally charged reasoning processes⁹. Despite the intuitive appeal of human oversight, the integration of these divergent modes of reasoning is therefore neither straightforward, nor inherently effective.

These structural limits call for regulatory approaches capable not only of imposing abstract oversight duties, but of testing in practice whether said duties can realistically fulfil their intended function. The question, therefore, is not only whether human oversight should exist, but how it can be operationalised in a verifiable and legally coherent manner.

In light of these challenges and given the clear legislative *favor* for human oversight – which has also been openly embraced by the EU legislator in many digital legislative instruments including the

4. *Inter alia*: GAUDEUL et al. 2025, which provide compelling evidence that human oversight fails to identify and correct algorithmically generated discrimination when it is not supported by appropriate measures, such as a well-designed human-machine interface, adequate authority and training for the overseer, clear operational guidelines, sufficient time and resources to perform the review.
5. *Inter alia*: SOLOVE-MATSUMI 2024, arguing that human and algorithmic reasoning operate according to fundamentally different logics, often making hybrid human and machine decision-making not readily compatible. The analysis demonstrates that human reviewers tend to misinterpret, over-trust, or insufficiently scrutinize algorithmic outputs, meaning that human oversight, if not supported by adequate design, training, and organizational safeguards, fails to correct errors.
6. *Inter alia*: GREEN 2022, which demonstrates that existing policies mandating human oversight rest on a flawed assumption that humans can reliably detect and correct algorithmic errors. The analysis shows that human-algorithm interaction involves complex cognitive, organizational, and structural constraints; in this context, adding a human reviewer often leaves the underlying problems intact and may even reproduce or exacerbate them rather than mitigate risk.
7. GAUDEUL et al. 2025.
8. WACHTER 2022. The author gives the compelling example of algorithmically-made statistical inferences that make no sense for a human, but nonetheless correlate with important decisions: “AI also creates seemingly incomprehensible groups defined by parameters that defy human understanding such as pixels in a picture, clicking behavior, electronic signals, or web traffic. These algorithmic groups feed into important automated decisions, such as loan or job applications, that significantly impact people’s lives”.
9. SOLOVE-MATSUMI 2024.

General Data Protection Regulation (“GDPR”)¹⁰, AI Act, Digital Services Act (“DSA”)¹¹ and Platform Work Directive (“PWD”)¹² – it is necessary to ensure that the concept is not merely rhetorical, but that it meaningfully mitigates the risks associated with automated decision-making, rather than legitimising them. This gap between normative expectations and practical feasibility raises the need for human oversight mechanisms to be experimented with, scrutinised, and refined before being deployed at scale.

It is precisely at this problematic intersection that regulatory sandboxes become relevant. Although usually presented as, primarily, innovation-support tools, sandboxes also serve a second function: they create evidence-generating environments in which regulators and AI operators can jointly test how vague or open-textured legal requirements should work in practice¹³. Because human oversight is one of the most open-textured requirements in EU digital law, and one whose practical shortcomings have been extensively documented, it becomes an ideal candidate for such structured experimentation. This perspective also aligns with the increasing attention that EU digital regulation devotes to experimental governance tools¹⁴, signalling an institutional shift towards more adaptive, evidence-based regulatory ap-

proaches to keep up with the pace of technological developments, without hindering innovation.

Originating in the fintech sector and now explicitly embedded in new EU digital regulation including the AI Act, Cyber Resilience Act¹⁵ and Interoperable Europe Act¹⁶ regulatory sandboxes provide controlled environments in which novel technological applications can be tested under the close supervision of competent authorities for a limited time and under defined conditions. Their main purpose is twofold: on the one hand, they allow innovators to experiment with new AI systems while receiving real-time regulatory guidance, thereby fostering legal certainty and supporting compliance; on the other, they enable regulators to gain hands-on knowledge of emerging technologies through a process of “regulatory learning”, before such technologies are placed on the market. Such environments are especially useful when laws mandate open-textured or vague obligations, allowing practical testing of how legal requirements might be translated operationally. This seems to be exactly the case of legally mandated requirements of “meaningful” human oversight under the GDPR¹⁷ and “effective” human oversight under the AI Act¹⁸, which remain vague, open-textured, and operationally difficult to implement in light of the inherent issues of human oversight measures. As

10. 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).

11. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

12. Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work.

13. OECD 2023, p. 13.

14. EUROPEAN COMMISSION 2023.

15. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Art. 33(2).

16. Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), Art. 11.

17. The “meaningfulness” requirement for human oversight is not explicitly set forth in the GDPR text, but has been carved out by the Article 29 Working Party as a minimum threshold to ascertain whether a decision is based solely on automated processing under the meaning of Art. 22(1) GDPR. See ARTICLE 29 WORKING PARTY 2017. This concept of “meaningful human oversight” has then been widely adopted by case-law, as noted by LAZCOZ-DE HERT 2022.

18. More precisely, Art. 14(1) AI Act requires that high-risk AI systems “can be effectively overseen by natural persons during the period in which they are in use”.

they offer a structured setting for supervised experimentation, sandboxes may hold the potential to bridge the gap between the law's mandatory safeguards on oversight, and the complex, challenging realities of supervising algorithmic decision-making processes in practice, thereby contributing to the development of clearer practices, more effective oversight mechanisms, and ultimately more trustworthy AI governance.

In light of the above, this paper seeks to contribute to the current academic and policy debate around both human oversight and regulatory sandboxes in EU law, by introducing and advancing the concept of specialized regulatory sandboxes as a means to enable competent authorities and AI operators to design and implement effective and meaningful human oversight in an evidence-based way. We depart from a general-purpose and even a sector-based sandbox regime, by proposing the establishment of "requirement-centric" sandboxes, focused on human oversight requirements under the AI Act and connected EU digital legislation such as GDPR's Article 22 and PWD's Article 10. Unlike existing vertical and sector-specific regulatory sandboxes (e.g., for automotive, healthcare, etc.), our model centres on the oversight requirement itself.

To do so, the paper is structured in five parts. While Section 1 provides the introduction and sets the stage for the following sections, Section 2 situates human oversight in the broader international landscape and then details the EU framework, focusing on the GDPR and the AI Act overlapping requirements, with a view to clarify the respective roles of providers and deployers (also as data controllers under the GDPR). Section 3 reviews the empirical and theoretical work on the practical shortcomings of human oversight – cognitive, organizational, and systemic. Section 4 introduces regulatory sandboxes: it defines the instrument,

traces its emergence, and sets out the EU legal basis and design under the AI Act, highlighting their potential for achieving regulatory learning and advancing legal certainty in the context of human oversight requirements. Section 5 advances the core proposal for specialized AI regulatory sandboxes for human oversight, also sketching some high-level policy advice on how to operationalize them. The conclusions in Section 6 present the main findings and propose a path for further research and policy development.

2. Human oversight obligations under EU law

Human oversight has become a common feature across the main international instruments developed in multilateral forums to regulate or guide the governance of artificial intelligence at both global and regional levels¹⁹. Most notably, the Council of Europe's Framework Convention on AI²⁰, the UN General Assembly Resolution on AI adopted on 21 March 2024²¹, and UNESCO's Recommendation on the Ethics of Artificial Intelligence of 23 November 2021²² all enshrine explicit provisions on human oversight. The influential OECD Recommendation on AI, first adopted on 21 May 2019 and amended on 4 May 2024, also refers to the need for human agency and oversight²³.

In line with this worldwide trend, one of the defining features of EU digital regulation is its insistence on having humans oversee the functioning of algorithmic systems. From data protection to artificial intelligence governance, the EU's approach is explicitly human-centric²⁴, aiming to ensure that rapid technological advances remain aligned with fundamental rights²⁵. This focus on human oversight is evident in cornerstone EU digital laws like the GDPR and – as anticipated and even more so – the AI Act. Both instruments boast a large,

19. Further regional or national initiatives are further analysed by PANEZI 2024, pp. 9-11.

20. COUNCIL OF EUROPE 2024. The Convention is the first binding international treaty on AI regulation.

21. UNITED NATIONS 2024.

22. UNESCO 2021.

23. OECD 2024.

24. This concept is explicitly referred to in the AI Act as a cornerstone of the EU approach to AI regulation. See: Rec. (1), (6), (8), (27), (176) and Art. 1.

25. FINK 2025.

horizontal scope of application²⁶, and embed requirements for human supervision of automated processes if certain thresholds are met²⁷ – a legal safeguard reflecting the conviction that even in an age of AI-enabled automated-decision making, critical decisions should not be left entirely to machines. Other, narrower digital regulations, notably including the PWD (Art. 10), also mandate overlapping human oversight requirements, adding weight to the EU’s legislator favourable approach to human oversight as one of the main remedies against algorithmic harms. By requiring a human hand on the controls, EU law seeks to preserve accountability, prevent harm to fundamental rights, and ensure trust in digital technologies²⁸.

2.1. Human oversight in the GDPR

The GDPR, directly applicable since 25 May 2018, was among the first laws worldwide to recognize, in its Article 22, both a prohibition²⁹ of fully automated decisions that produce legal or similar effects (subject to some exceptions), and a right to contest the fully automated decision, when such exceptions are met. This provision equips individuals with a *prima facie* right not to be subject to a decision based solely on automated processing, if said decision produces legal or similarly significant effects over them, thus expressly requiring a

human-in-the-loop³⁰. Even when such automated decisions are exceptionally allowed under paragraph 2 of the Article (i.e., based on data subject’s explicit consent, contractual necessity, Union or Member State legal provision), the controller must provide “suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests” including as a minimum the right to obtain human intervention, to express their viewpoint, and to contest the decision, thereby producing an “on request” human-on-the-loop obligation³¹. In other words, whenever algorithms make important determinations about people, the GDPR mandates that a human can step in to review (before it takes effect) or override (after it has taken effect) the outcome. Recital 71 underscores the rationale: it notes that purely automated decisions need to include mechanisms for human oversight and the ability for individuals to challenge the outcomes on request, via a right to human intervention³². This was a landmark statement of principle in data protection law – and one tracing its roots to the already influential Directive 95/46/EC³³ –, as it expressly bridged data protection and automated decision-making regulation, showcasing the EU’s early legislative response to concerns of “black box” algorithms producing inscrutable and unaccountable decisions. By requiring “meaningful” human

26. Although the AI Act decouples its (very large) formal scope of application from its (very narrow) material scope of application: broad notion of “AI system” is leveraged to establish the law’s boundaries, but actual obligations are then placed on a much smaller subset of AI systems (mostly, high-risk ones), as critically noted by VEALE–ZUIDERVEEN BORGESIU 2021, pp. 108–110.

27. Such thresholds being, in the case of the GDPR, having automated systems take decisions with legal or similarly significant effects on individuals under Art. 22, while, in the case of the AI Act, having AI systems qualifying for the “high-risk” category under Art. 6.

28. FINK 2025; HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE 2019; See also Rec. (27) of the AI Act, which strongly underlines the link between the AI Act and the principles developed by the High-Level Expert Group on AI.

29. The text of Art. 22(1) GDPR, is worded in positive terms, rather than as a prohibition; however, it was interpreted as such firstly by the EU data protection authorities in 2017 (ARTICLE 29 WORKING PARTY 2017, pp. 19–20), then endorsed by the Court of Justice (Court of Justice, *Land Hessen/SCHUFA Holding AG*, case C-634/21, p. 52), despite some resistance in the literature (TOSONI 2021).

30. LAZCOZ–DE HERT 2022, pp. 12–14.

31. Art. 22(3) GDPR. LAZCOZ–DE HERT 2022, pp. 12–15. The authors characterize this obligation as a type of “human-out-of-the-loop” measure, in contrast with the “human-in-the-loop” requirement in Art. 22(1) GDPR.

32. DIRUTIGLIANO–BALDINI 2025. Rec. (71) is also notable for expressly linking Art. 22 GDPR, to non-discrimination objectives, requiring data controllers to mitigate the risk of inaccuracies and discriminatory outputs.

33. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

review, the GDPR aims at embedding fairness, redress mechanisms, and – ultimately – dignity, namely the values that human judgment can intuitively provide³⁴.

The practical application of the provision has cemented this approach: Article 22 GDPR has been extensively interpreted by both the Member States' courts and data protection authorities at the outset of GDPR applicability³⁵ and, subsequently, further expanded by the Court of Justice of the EU by leveraging the fundamental rights-based foundation of the GDPR in the treaties³⁶. These favourable interpretative developments of the provision have, in turn, spurred numerous concrete applications of Article 22 by Member States' supervisory authorities and national courts³⁷ – with a particular relevance in the labour law domain, where it has been strategically leveraged by workers' associations to challenge algorithmic surveillance practices by employers³⁸ – significantly influencing practices around automated decision-making, both within the EU and internationally, thanks to the EU's regulatory influence in the digital domain.

2.2. Human oversight in the AI Act

Building and expanding on this foundation, the AI Act considers human oversight as an explicit obligation for high-risk AI systems. The central provision in this respect is Article 14, aptly titled "Human oversight". This Article places obligations aimed at providers, in line with the AI Act's overarching nature as a product-based legislation³⁹,

essentially requiring that all high-risk AI systems – meaning, those AI systems that fulfil the requirements laid down in Article 6 of the AI Act – be designed and developed so that "they can be effectively overseen by natural persons" during their use, by means of appropriate safeguards such as human-machine interfaces, and by illustrating the chosen safeguards in the system's instructions⁴⁰. Deployers of AI systems are then required to assign human oversight in practice, by making use of the aforementioned providers' safeguards, and in line with the provider's instructions, which must also indicate the measures aimed at enabling effective oversight⁴¹.

According to the letter of the provision, human oversight measures to be envisaged by providers must aim at preventing or minimising "risks to health, safety, and fundamental rights" that might emerge from the system's operation, in particular where such risks persist despite the application of other requirements aimed at high-risk AI system providers⁴². This seemingly entails an inverse relationship between human oversight and other obligations aimed at high-risk AI system providers⁴³, tracing its origin to the work of the High-Level Expert Group on AI⁴⁴, which set the basis for the AI Act. This inverse relationship conceptualizes human oversight as a "safety net" within the broader context of the AI Act, namely, a safeguard whose significance grows as other risk management mechanisms prove insufficient or fail to adequately mitigate the risks posed by a given AI system.

34. Although, as shall be seen in Section 3, *infra*, the actual effectiveness of human oversight to achieve these aims is – to say the least – heavily debated.

35. For a summary of national cases concerning the application of Art. 22 GDPR, see: BARROS VALE–ZANFIR-FORTUNA 2022; for the interpretation adopted by EU data protection authorities, see: ARTICLE 29 WORKING PARTY 2017.

36. Court of Justice, *Land Hessen/SCHUFA Holding AG*, case C-634/21.

37. BARROS VALE–ZANFIR-FORTUNA 2022.

38. CANSU–FARRAR 2021, which showcase many instances where data protection legislation – and especially Art. 22 GDPR – has been leveraged by platform workers and their representatives to challenge unfair algorithmic management practices by gig economy platforms.

39. VEALE–ZUIDERVEEN BORGESIUUS 2021.

40. Art. 13(3)(d) AI Act.

41. See Art. 26, para. 1 and 2 AI Act.

42. Art. 14(2) AI Act.

43. This elevates human oversight as a key safeguard in the overall context of the AI Act, as noted by FINK 2025, and ENQVIST 2023.

44. HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE 2019.

This arrangement goes to show the high trust that the EU legislator has put on human oversight as a safeguard against algorithmic harm, elevating it as a key component of the EU's human-centric approach to AI, in line with the High-Level Expert Group on AI's position⁴⁵.

As noted, the bulk of the legal obligations are placed on the provider, to whom Article 14 is entirely addressed. However, in doing so, and in contrast to other obligations, the provision leaves much flexibility to the provider. Article 14(3) AI Act leaves to the latter the choice between integrating built-in oversight mechanisms into the AI system or specifying measures to be implemented by the deployer, or a combination of both, depending on the specific risks associated with the AI system's intended use.

Furthermore, and contrary to Article 22 GDPR which does not expressly prescribe oversight measures for data controllers, Article 14(4) AI Act lists five specific human oversight measures, spanning from the obligation to develop the AI system in a way that enable humans to interpret its outputs, or to remain aware of automation bias, to a built-in "stop" button that allows the overseer to suspend the system use. However, much room for flexibility is present also in this case, as the provider is required to choose and implement such measures "as appropriate and proportionate". As noted in the literature, whether this flexibility extends to "which" measures to implement or remains limited to the "how" is unclear, although a teleological interpretation may suggest the latter option⁴⁶.

Finally, an enhanced human oversight regime in the form of a human(s)-in-the-loop requirement is established for remote biometric identification systems, where identification of a natural person by the system must be separately verified and confirmed by at least two natural persons⁴⁷, subject to targeted exemptions for AI systems used in law enforcement and migration.

Although Article 14 remains the central provision, the human oversight framework is completed

by two other provisions that are in a strict relation with it, and that contribute to extend human oversight obligations to the deployer.

Firstly, Article 13 – titled "Transparency and provision of information to deployers" – requires the provider to include within the AI system's instructions for use the human oversight measures adopted pursuant to Article 14, including the technical measures to ensure the system's interpretability⁴⁸. Lastly, as already recalled, Article 26 completes the framework by mandating deployers to use the system in accordance with said instructions, as well as to specifically "assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support"⁴⁹.

In a nutshell, while the provider must equip the system to enable human oversight, the deployer is then required to make full use of the oversight functionalities. The legal design around human oversight in the AI Act seems sound and well-structured: by "hard-wiring" human oversight into the high-risk AI system lifecycle, from its design phase (where the provider is the main actor) all over to the deployment phase (where the deployer takes the lead), the EU legislator aims to avoid scenarios where algorithmic tools operate unchecked and to reassure the public that accountable humans remain ultimately in charge of critical decisions. Nevertheless, many issues loom over the effective achievement of the EU's stated goals regarding human oversight, as will be discussed in the next section.

3. The practical shortcomings of human oversight

However well-crafted the EU's legal provisions on human oversight are, a growing body of research suggests that effective oversight is often more aspirational than real, and that human oversight measures – even when they carefully follow the letter of law – can sometimes even exacerbate existing issues. One recent study, for instance, found that humans tasked with revising AI systems' outputs

45. *Ibidem* p. 16.

46. ENQVIST 2023 p. 10.

47. Art. 14(5) and Rec. (73).

48. Art. 13(3)(d).

49. Art. 26(2).

in the context of hiring recommendations added their own “human-made” bias on top of discriminatory outputs produced by the AI system⁵⁰, or even introduced *ex novo* bias and discrimination where the AI system had not done so⁵¹: for example, judges in several jurisdictions were found to override algorithmic risk assessments in ways that increased racial disparities, compared to the original algorithmic output⁵². Such findings highlight that simply having a human in the loop is no panacea: the human can fail to catch the algorithm’s mistakes or can even aggravate them.

3.1. Cognitive and psychological limits

There are a few reasons for this. Cognitive biases pose a first major hurdle. Human decision-makers tend to place undue trust in algorithmic outputs – a phenomenon known as “automation bias”, where people defer to automated recommendations and apply less independent scrutiny than they otherwise would. Research shows that even trained personnel tasked with reviewing machine suggestions can become passive, failing to double-check or countermand the algorithm’s output⁵³. On the other side of the spectrum lies “algorithmic aversion” where individuals unjustifiably reject AI-generated outputs, potentially replacing fair and consistent algorithmic decisions with discretionary judgments tainted by human error or unlawful bias⁵⁴.

The fundamental issue is that, although AI outputs may closely resemble human logic, they are derived from statistical inferences, which differ significantly from moral and contextual judgments taken by humans⁵⁵. Although AI systems – including generative AI systems – may appear to closely replicate human reasoning, in reality they function primarily as predictive tools, generating

outputs based on statistical inferences and correlations drawn from vast amounts of data. As a result of this stark diversity, humans often perform badly when reviewing algorithmic outputs: in practice, the human overseer may exhibit only nominal vigilance, typically by rubber-stamping the algorithm’s decision due to over-confidence in the machine’s capabilities, responsibility avoidance, lack of training, resources or time pressure. Notably, empirical studies find that people struggle to judge when an AI’s recommendation is erroneous, often overestimating the accuracy of the system, or ignoring contradictory cues⁵⁶. Depending on the features of the AI system, this can lead to omission errors (failing to act because the system gave no alarm) and commission errors (uncritically following a flawed recommendation). Crucially, although Article 14 of the AI Act explicitly acknowledges automation bias as an issue to be addressed by the provider⁵⁷, inherent human cognitive limitations cannot be easily “legislated away”: despite the express legal obligation in the AI Act to account for automation bias, the way in which this problem is to be addressed in practice is not fully clear.

The complexity and opaqueness of advanced AI systems present further practical limitations to meaningful oversight. AI systems often operate as complex black-box models, making it exceedingly difficult for human overseers to understand the rationale behind a given output. The AI Act also addresses this issue, by requiring that providers design systems to be “effectively overseen” by humans⁵⁸, and that the provider’s instructions regarding human oversight include explanations of technical measures to make algorithmic outputs interpretable to humans⁵⁹. However, while this assumes that explanations or transparency measures

50. For an overview of the challenges faced by the EU anti-discrimination law framework vis-à-vis the rise of automated decision-making, see ADINOLFI 2022.

51. GAUDEUL et al. 2025.

52. GREEN 2022.

53. GAUDEUL et al. 2025.

54. *Ibidem*.

55. SOLOVE–MATSUMI 2024.

56. GAUDEUL et al. 2025.

57. Art. 14(4)(b) AI Act.

58. Art. 14(1) AI Act.

59. Art. 13(3)(d) AI Act.

will enable comprehension, evidence casts doubt on that assumption: studies show that providing algorithmic explanations or other transparency tools does not necessarily improve an operator's ability to detect errors or biases⁶⁰. Ironically, interpretability and explanations can instead have the perverse effect of even increasing human trust in the AI system's decisions – leading oversight personnel to become more confident in the algorithmic outputs, even when they are wrong or discriminatory.

3.2. Organizational and systemic constraints

Furthermore, and perhaps most troubling, are the organizational and systemic shortcomings that can pressure human overseers into rendering their activity a purely symbolic exercise. Despite frequent policy claims that human oversight redresses algorithmic harms, empirical support for such claims remains limited and often anecdotal⁶¹. Conversely, empirical research overwhelmingly indicates that humans cannot reliably perform the safeguarding functions envisioned by law⁶². In practice, human oversight frequently provides only the appearance of control – what some scholars have labelled a “skeuomorphic” humanity⁶³ – giving the impression of a human choice, but without its substance. The human overseer may technically have discretion to override or alter an automated decision, but organizational norms and the design of the workflow often discourage deviation: most commonly, the human overseer is nudged into passively accepting the algorithmic output, to avoid assuming responsibility in cases where the decision proves wrong or harmful in practice. As a result, oversight can deteriorate into a merely formal requirement, where the human's role is nudged into confirming the machine's output rather than critically reviewing it.

Ultimately, existing research warns that current reliance on human oversight as a safeguard is not delivering on its intuitive promise to remedy algorithmic injustice. On the contrary, oversight measures may legitimize the deployment of flawed algorithms by cloaking them in a veneer of human review, all the while shifting responsibility for any harm away from providers, and onto lower-level human operators, acting as “liability sponges”⁶⁴.

The EU's ambitious framework thus confronts a paradox: it elevates human oversight as one of the central pillars to safeguard fundamental rights when operating high-risk AI systems, yet cognitive barriers, real-world human frailties and systemic pressures all conspire together to prevent that oversight from being genuinely effective. This tension sets the stage for exploring alternative approaches – a task the following section will undertake – but it reinforces a critical point: without acknowledging and addressing these practical shortcomings, human oversight risks remaining an attractive principle on paper that, in the best case, delivers only modest safeguards in practice, while in the worst case exacerbates algorithmic harms.

The considerable issues and shortcomings explored above do not mean, however, that human oversight is bound to remain an ineffective safeguard. Furthermore, the fact remains that EU secondary law explicitly requires AI system operators to implement oversight in a manner that is both meaningful and effective, as illustrated in the previous section. This situation implies that when establishing oversight measures, operators must adequately consider and address the shortcomings discussed above. This requirement applies both within the AI Act framework, where obligations are allocated between providers and deployers, and under the GDPR, where obligations rest on the data controller and are underpinned by the foundational principle of accountability⁶⁵, albeit with different level of intensity,

60. GAUDEUL et al. 2025.

61. GREEN 2022, p. 2.

62. *Ibidem*.

63. BRENNAN-MARQUEZ-SUSSER-LEVY 2019.

64. GREEN-KAK 2021.

65. Arts. 5(2) and 24 GDPR. Applied in the case at hand, this principle arguably mandates data controllers to identify and implement measures aimed at ensuring meaningful human oversight is achieved in practice, taking into account and solving its relevant shortcomings.

as discussed in the previous paragraph. In this respect, it is essential to recall that the AI Act and GDPR typically operate concurrently when high-risk systems are developed or deployed, as processing of personal data is almost invariably present in these types of systems.

This combination of a strong and horizontal legal mandate, on the one hand, and persistent practical and interpretative indeterminacy, on the other, calls for regulatory instruments capable of producing empirical and operational knowledge on how legally-mandated human oversight obligations can be meaningfully implemented in practice. In the absence of such instruments, there is a tangible risk that human oversight remains either under-specified in abstract guidance or over-formalised in compliance practices, without any genuine benefit in addressing the risks it seeks to mitigate.

It is precisely at this junction between normative ambition and operational uncertainty that regulatory sandboxes acquire particular relevance. By design, sandboxes provide a structured and supervised setting in which legally mandated requirements can be experimented with in concrete technical and organisational contexts, allowing regulators and AI operators to jointly observe how those requirements function in practice, where they fall short, and under which conditions they may be rendered effective. As such, sandboxes are uniquely positioned to translate legal obligations on human oversight into evidence-based practices that can later inform guidance, standard-setting and enforcement, before such obligations are generalised and applied at scale.

4. AI regulatory sandboxes under the AI Act

4.1. Origins and rationale of regulatory sandboxes

Regulatory sandboxes are an innovative legislative experimentation tool which has emerged during the last decade as a response one of the main issues inherent to the regulation of new technologies, namely the so-called “pace problem” where technological innovation evolves significantly faster than the ability of legislators and regulators to adapt existing legal frameworks⁶⁶. This challenge is further compounded by the “Collingridge dilemma”⁶⁷, which highlights the difficulty of regulating emerging technologies early on – when intervention is easier, but knowledge is limited – and the corresponding difficulty of intervening later, when the consequences are better understood, but the technology has become entrenched and resistant to change⁶⁸.

In this respect, regulatory sandboxes have emerged as a promising solution in many jurisdictions. No commonly shared definition of this instrument exist⁶⁹, but it can be broadly framed as supervised testing spaces that allow organizations to trial new and innovative technological products, overseen by regulators and restricted to a set period of time⁷⁰.

Beyond definitional uncertainties, regulatory sandboxes may take two main forms regarding their scope of operation: horizontal and vertical sandboxes⁷¹. On the one hand, the former (also called “cross-sector” or “cross-domain” sandboxes), are general-purpose environments open to a wide range of technologies and industrial sectors⁷²; they

66. BAGNI-SEFERI 2025, p. 19; DOWNES 2009.

67. COLLINGRIDGE 1980.

68. MORAES 2023, pp. 2-4.

69. CIRONE 2025, p. 262, where the author observes that a plethora of different definitions are given by policy documents and relevant sectoral legislations that establish regulatory sandboxes; ultimately, the definition varies depending on the context of use.

70. *Ex multis*, a similar definition is provided by MADIEGA-VAN DE POL 2022.

71. LANAMÄKI et al. 2025, p. 42, noting that the AI Act implicitly allows both domain-specific and horizontal sandboxes. RANCHORDAS-VINCI 2024, pp. 9-11; LONGO 2021.

72. In the Italian context, a salient example is the regulatory sandbox named “*Sperimentazione Italia*” (“Italy experimentation”), set forth by Art. 36 of Law Decree No. 76/2020, as converted by Law No. 120/2020. For a comment, see: RANCHORDAS-VINCI 2024.

aim to facilitate innovation broadly and to support regulatory learning across diverse use cases, but their breadth inherently limits the depth of experimentation on any single requirement. On the other hand, vertical sandboxes (also called “sector-specific” or “domain-specific” sandboxes), focus on a defined domains such as healthcare, connected vehicles or public administration⁷³. This specialisation allows regulators to develop sector-specific expertise through regulatory learning, and to generate more granular and operational guidance, as illustrated by several national experiences⁷⁴.

First pioneered in the fintech sector by the UK Financial Conduct Authority’s sandbox in 2015⁷⁵, as noted above, regulatory sandboxes promise to bridge the longstanding gap between rapid technological evolution, on the one hand, and the inherently slower pace of traditional legislative processes and enforcement, on the other. One of the primary advantages of regulatory sandboxes is their capacity to allow both regulators and innovators to examine and better understand innovative technological applications and their risks, before these enter the market: a process known as “regulatory learning”⁷⁶. By enabling a proactive, *ex-ante* scrutiny, sandboxes significantly reduce the risk of regulatory approaches rapidly becoming obsolete or inadequate in the face of emerging technological applications, allowing regulators to adjust their interpretation of existing norms, or even prompt the legislator to revise the regulatory framework itself. On the other hand, organizations that attend

the sandbox benefit from the possibility to develop and test their innovative solutions with real-time guidance from regulators, thus facilitating legal certainty, easing compliance requirements and accelerating market entry⁷⁷.

4.2. Design and operation in the EU context

Due to these and other benefits, as of late sandboxes have seen widespread global adoption⁷⁸ across diverse technological sectors – extending far beyond their original fintech origins – as flexible tools that effectively balance technological advancement with responsible regulatory oversight. The EU makes no exception, as it has followed this global trend and incorporated this instrument into some of its recent digital law acquis, including the AI Act⁷⁹, which explicitly foresees “AI regulatory sandboxes” within its Chapter VI (“Measures in support of innovation”), indirectly defining them in Article 57 as supervised frameworks that “provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market”⁸⁰. These provisions anchor sandboxes in EU law as a means to spur AI innovation in a compliant, well-monitored setting. Eligibility for sandbox participation is open to AI providers (particularly, startups and SMEs, who are given priority access) that meet criteria that are still to be detailed in EU Commission’s implementing acts in accordance with Article 58.

73. Still in the Italian context, an example is the Italian FinTech Regulatory Sandbox, established by Art. 36 of Law Decree No. 34/2019, converted into Law No. 58/2019. RANCHORDAS–VINCI 2024, pp. 10–11.

74. One example is the French Data Protection Authority’s sandbox, further explored in section 5, *infra*. See also BAGNI 2023.

75. OECD 2023, p. 15.

76. RANCHORDAS–VINCI 2024; BAGNI 2023.

77. BAGNI–SEFERI 2025.

78. For example, as noted by MADIEGA–VAN DE POL 2022, Japan introduced in 2018 a regulatory sandbox framework open to organizations and companies, both domestic and international, interested in experimenting with emerging technologies such as blockchain, artificial intelligence (AI), and the Internet of Things (IoT). This framework applies across various sectors, including financial services, healthcare, and transportation.

79. This concept is not limited to AI: the EU Cyber Resilience Act, in its Art. 33(2), likewise envisages cybersecurity sandboxes, allowing novel digital products to be developed and tested under regulatory supervision for a limited time before market entry (with an emphasis on supporting SMEs). However, while each Member State is required to establish at least one regulatory sandbox under the AI Act, the Cyber Resilience Act leaves the establishment of cybersecurity regulatory sandboxes as a mere possibility.

80. Art. 57(5) AI Act.

Under the AI Act, each sandbox operates pursuant to a specific testing plan agreed between the high-risk AI system providers, as participants, and the national competent authority, and is time-bound, with extensions possible based on project needs. The sandbox's supervisory structure entrusts national market surveillance authorities to oversee the experiments, in coordination with other relevant bodies where necessary. Most notably, Article 57(1) expressly requires that the competent national Data Protection Authority ("DPA") be involved in case where AI systems involve the processing of personal data, which is bound to happen in most cases given that high-risk AI systems envisaged under the AI Act often involve the processing of personal data in the context of their training, testing and/or operation⁸¹.

Importantly, involved authorities retain full oversight powers: participation in a sandbox does not exempt AI operators from fundamental legal requirements or from civil liability in case it arises, but administrative fines cannot be imposed in case of *bona fide* failure to comply with the law. Moreover, participating authorities are required to provide guidance on regulatory expectations and are expected to exercise their oversight in a flexible, innovation-friendly manner.

In addition, the AI Act has foreseen further incentives for attending an AI regulatory sandbox, most notably by producing legal effects aimed at encouraging participation: most notably, once a specific sandbox experiment has been successfully attended, the competent authority is required to provide an "exit report", which providers may then leverage to demonstrate their compliance with the AI Act⁸².

In this context, AI regulatory sandboxes seem intuitively well-suited to solve the practical problems posed by human oversight, discussed in Sec-

tion 3, above. In light of their features, sandboxes are arguably the main tool to achieve one of the AI Act's stated aims, namely, supporting innovation⁸³: from this perspective, they act as a pragmatic regulatory learning instrument, supporting an evidence-based regulatory approach to addressing ambiguous, problematic and operationally challenging requirements, which is precisely the case for human oversight requirements for high-risk AI systems. Through dialogue with relevant AI Act and GDPR enforcers – which are required to provide feedback on regulatory expectations to participants – and testing within these controlled environments, sandboxes may help to operationally clarify many of the legislative requirements in practice.

In this respect, the express obligation to involve Data Protection Authorities in the operation and supervision of sandboxes appears crucial. DPAs are in this case mandated to provide interpretative guidance on GDPR requirements, together with the national AI Act's Market Surveillance Authority⁸⁴. The joint participation of GDPR and AI Act enforcement authorities is particularly significant, as it creates an unprecedented institutional forum for addressing cross-cutting compliance challenges in real time. If successful, the joint operation of sandboxes may help to inform new, evidence-based interpretations of the law, with specific regard to legislative overlaps between the AI Act and the GDPR. This is especially relevant in the case of human oversight, as the requirement simultaneously serves as a safeguard under Article 22 GDPR and as a design and deployment obligation under Article 14 AI Act, thereby making coordinated guidance a *de facto* mandatory element to ensure coherent and practicable implementation of both laws.

81. This requirement gives rise to a number of interpretative issues in light of the overlap between GDPR and AI Act provisions on the processing of personal data, particularly Art. 59 of the AI Act. For an analysis, see *inter alia*: BAGNI–SEFERI 2025, pp. 70–84, concluding that the stringent conditions established by Art. 59, as well as its cumulative applications with other GDPR and AI Act provisions on data governance, may invertedly discourage personal data re-use in the sandbox; HOLTZ–LEDENDAL 2026, pp. 11–12, highlight instead that Art. 59 even provides a legal basis to process special category data pursuant to Art. 9(2)(g) GDPR.

82. Art. 57(7) AI Act.

83. Art. 1(1) AI Act.

84. It should be noted, depending on the Member State's choice, the Data Protection Authority and Market Surveillance Authority may coincide on the same entity (Art. 70(1) AI Act).

Despite these potential benefits, some challenges stand in the way. Regulatory sandboxes foreshadow the possibility of regulatory capture⁸⁵, they may inadvertently produce regulatory fragmentation at the national or even regional and local level in case where the results of sandboxes are not sufficiently publicized and generalized. Furthermore, they require extensive resources, and expertise from both the attendees and the regulators, in order to function properly. Despite this, the clear legislative endorsement at the EU level, combined with heavy investments already foreseen under initiatives such as the Digital Europe Programme and related Coordination and Support Actions, suggests that these practical barriers may soon be addressed, paving the way for more robust, specialized regulatory sandboxes under the AI Act. These problems and relevant solutions have been extensively explored and are acknowledged by the EU legislator, which has envisaged various tools to deal with them⁸⁶.

In sum, by closing the gap between high-level legal mandates and operational realities, regulatory sandboxes hold the promise to mitigate interpretative uncertainties and leave open the possibility for more targeted initiatives. This leaves the door open to the establishment of one or more specialized “human oversight sandboxes”, a proposal to be addressed at a high-level in the following section.

5. A proposal for specialized AI regulatory sandboxes for human oversight

To optimize their effectiveness and to help them achieve their aims, this paper suggests that AI regulatory sandboxes should be organized around thematic streams, while remaining at the same time aligned with the flexible legal requirements and safeguards of the AI Act’s sandbox regime, outlined in its Chapter 6. It argues, in particular, to go beyond the traditional “horizontal versus vertical sandboxes” dichotomy, so far limited to distinctions between broad cross-sector and industry-specific sandboxes; instead, it suggests advancing a model of vertical specialization grounded in AI-specific regulatory requirements, in this case devoted explicitly to testing and refining human oversight mechanisms for high-risk AI systems.

While regulatory sandboxes traditionally take as their starting point a specific product or service and then derive the applicable legal obligations, the model advanced in this paper deliberately reverses this logic. Here, the analytical anchor is not the technological application, but a single, cross-cutting regulatory requirement of the EU digital acquis, that is, human oversight. This inversion reflects the particular nature of human oversight obligations, and their relevant shortcomings, as discussed in Sections 2 and 3.

For this reason, the traditional product-based approach inherent in most regulatory sandboxes is, arguably, insufficient. The feasibility and effectiveness of human oversight depend on a constellation of factors – technical design choices, organisational arrangements, user capabilities, contextual constraints, and the interplay between multiple legal regimes (most notably: AI Act, GDPR, PWD). It is suggested that these elements cannot be meaningfully captured by examining all requirements applicable to an AI system. A requirement-centric sandbox, by contrast, would allow regulators to isolate the oversight obligation itself, observe its operationalisation across heterogeneous technological and organisational environments, and identify recurring patterns that a product-centric experiment is structurally unable to reveal. In this sense, reversing the traditional sandbox logic is not only justified; it is necessary to generate evidence-based, generalisable guidance on a horizontal obligation whose proper implementation is central to the EU’s human-centric approach to AI governance.

This shift in perspective should also be positioned in the context of existing experimentation practices in the EU. While no Member State has yet deployed a sandbox explicitly centred on specific requirements such as human oversight, some EU Member States have already conducted data protection-related sandboxes on specific sectors; one recent example is the French Data Protection Authority’s sandbox frameworks, which focused sequentially on healthcare, education, and public administration⁸⁷. These initiatives have already yielded promising results despite not being yet able

85. BAGNI–SEFERI 2025, pp. 192–206.

86. For example: *Ibidem*; RANCHORDAS–VINCI 2024.

87. COMMISSION NATIONALE DE L’INFORMATIQUE ET DES LIBERTÉS 2025.

to rely on relevant EU law provisions, such as those included in the AI Act, and thus enjoying very limited regulatory flexibility⁸⁸.

In this respect, one notable and recent illustration comes from the abovementioned French Data Protection Authority's sandbox framework on public administration⁸⁹. In particular, the Authority examined *Conseils Personnalisés*, an AI-based recommendation tool deployed within the *France Travail*, the French public employment services. The system, built around a locally-hosted large language model enhanced through Retrieval-Augmented Generation (RAG), suggested tailored training opportunities to jobseekers based on their profile and on inputs provided by employment advisers. Although the tool did not directly take binding decisions, it shaped the options that advisers present to users and thus raised questions linked to Article 22 GDPR, especially in light of the recent Court of Justice of the EU's *SCHUFA*⁹⁰ case, and to the threshold above which human intervention could be deemed "meaningful"⁹¹. The most delicate issue concerned the requirement that decisions must not be based solely on automated processing, under Article 22(1) GDPR, thereby mandating the presence of a human-in-the-loop mechanism⁹². In this respect, while some measures were already put in place by the data controller, such as internal guidelines, training modules, and appropriate working conditions ensuring that no pressure was placed on advisers to follow the system's recommendations, the sandbox experiment identified further measure to ensure that the "meaningfulness" requirement was achieved:

France Travail developed an AI-awareness pathway including continuous training, specific internal support for the use of the *Conseils Personnalisés* tool, and the appointment of "AI correspondents" acting as intermediaries between local agencies and the central administration. Under these conditions, as identified during the course of the sandbox, the Authority concluded that proposing training opportunities via the tool did not appear to constitute fully automated processing⁹³.

Drawing from this and other experiences at national level⁹⁴, scholars have recently highlighted the practical benefits of sector-specific approaches to sandbox design, emphasizing that such targeted arrangements allow deeper and more focused regulatory learning on the specific field and, thus, enable specialization from the involved regulators⁹⁵. This approach is expected to allow the provision of more precise guidance from regulators to organizations, thereby facilitating the efficient use of resources and expertise, generating empirical and measurable insights that inform clearer guidance and future regulatory adjustments⁹⁶.

However, unlike these sector-specific initiatives, this paper proposes to go one step further and establish requirement-specific sandboxes, with a particular focus on human oversight⁹⁷. While sectoral sandboxes concentrate regulatory learning within a given industry or domain, a human-oversight sandbox would cut horizontally across sectors, targeting one of the most ambiguous and operationally challenging legal requirements contained in both the AI Act, the GDPR and other EU sectorial digital laws as applicable. Such a model would retain

88. Due to the fact that, in principle, national law may not derogate EU Law except where EU Law expressly allows for this, pursuant to the fundamental principle of primacy of EU law. For this reason, EU secondary law provisions on regulatory sandboxes such as those in the AI Act and Cyber Resilience Act are aimed at providing this flexibility, by allowing certain obligations to be derogated in the context of sandboxes, or to prevent the application of pecuniary fines by competent authorities. BAGNI-SEFERI 2025, pp. 29-43.

89. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS 2025, pp. 3-5.

90. Court of Justice, *Land Hessen/SCHUFA Holding AG*, case C-634/21.

91. See n. 18, *supra*.

92. See Section 2.1, *supra*.

93. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS 2025, p. 5.

94. For an overview of existing regulatory sandbox schemes in the EU and UK: CIRONE 2025, pp. 263-266.

95. LANAMÄKI et al. 2025.

96. *Ibidem*.

97. A similar possibility has recently been suggested by LANAMÄKI et al. 2025 p. 41.

the benefits of specialization observed in national experiences – namely, more focused regulatory learning, concentration of expertise, and more precise guidance – but would channel them towards clarifying a single, cross-cutting obligation.

The advantage of establishing this type of sandboxes is intuitively apparent. By creating a safe space for regulators and AI operators to jointly probe how human oversight legal requirements may successfully be translated in practice, such sandboxes would primarily limit the elements to be tested in the sandbox to those related to Article 14 AI Act, hence facilitating targeted regulatory learning outcomes on how to implement effective and meaningful human oversight. The specialized, evidentiary feedback loop generated in a “human-oversight sandbox” could thus refine the interpretation of oversight obligations across legal instruments, ensuring that the legally mandated requirements of achieving – respectively – “effective” and “meaningful” oversight are translated into verifiable, evidence-based practices. In this respect, the operational advantage would lie in the possibility for the authorities operating the sandbox to specialize in human oversight, thus concentrating expertise, reducing the resources needed for fragmented or duplicative experimentation, and enabling faster and more efficient guidance to providers and deployers.

What is more, where relevant in light of the specific AI system tested within the sandbox, any overlapping or sector-specific human oversight provisions should likewise be incorporated in the sandbox perimeter. As noted above, such provisions can be found in other instruments pertaining to the EU digital acquis: for instance, an AI system aimed at allocating tasks to online platform workers would arguably fall into the scope of application of Article 14 AI Act (as a high-risk AI system under Annex III, point 4), Article 22 GDPR (as it processes workers’ personal data to function), and Article 10 PWD, thereby triggering the human oversight requirements mandated by each of the three laws.

Despite the potential benefits, a first possible criticism is that the establishment of this kind of specialized sandboxes finds no justification in the relevant provisions of the AI Act. However, a closer look at the relevant provisions and recitals of the AI Act supports the view that specialized sandboxes for human oversight would not only be consist-

ent with, but also directly advance, the objectives of the sandbox regime established under the law.

Not only no relevant provision of the AI Act on regulatory sandboxes appears to prevent the establishment of regulatory sandboxes that are “specialized” in one or more legal requirements, but several elements seem instead to leave open this possibility, and even to encourage it. For instance, in the context of the implementing acts which the Commission is mandated to adopt in order to complete the relevant framework for sandboxes, Article 58(2) (c) explicitly requires that AI regulatory sandboxes support, to the best extent possible, flexibility for national competent authorities to establish and operate their AI regulatory sandboxes. In this context, the concept of “flexibility” should be understood as encompassing the possibility of setting up both “general-purpose” sandboxes, covering the full set of legal requirements applicable to high-risk AI systems, and specialized ones focusing on particular obligations such as human oversight.

Even more importantly, Article 58(2)(i) mandates that sandboxes “facilitate the development of tools and infrastructure for testing, benchmarking, assessing and explaining dimensions of AI systems relevant for regulatory learning, such as accuracy, robustness and cybersecurity, as well as measures to mitigate risks to fundamental rights and society at large”. Despite not being expressly cited in the exemplificatory list, human oversight is undoubtedly a key area where regulatory learning to the benefit of both regulators and providers can take place, since – as discussed previously – research and academic discourse show that effective oversight mechanisms remain elusive and highly contested in practice, requiring iterative, evidence-based experimentation to be meaningfully implemented. This is further compounded by Recital 139, which underlines that “participation in the AI regulatory sandbox should focus on issues that raise legal uncertainty for providers and prospective providers to innovate, experiment with AI in the Union and contribute to evidence-based regulatory learning”. Again, as discussed in previous Sections of this paper, human oversight is an area where legal uncertainty is widespread – both due to practical issues and overlapping legal requirements stemming from EU law – and where, as a consequence, regulatory learning is much needed with a view to achieve legal certainty.

5.1. Governance and institutional design

However, in order to successfully meet their objectives, it is of paramount importance that the governance aspects are carefully considered, especially in light of the intersecting legal requirements around human oversight in EU law. The institutional setup of human oversight-specific sandboxes should thus foresee joint governance and responsibility between the competent AI market surveillance authority and the national DPA – which is always competent for human oversight requirements stemming from the GDPR and the Platform Work Directive⁹⁸ – with the possible involvement of further stakeholders, where relevant. In this latter respect, the role of competent standardization bodies that have been mandated by the EU Commission under Article 40 AI Act, to draw up technical standards which also encompass human oversight must also be emphasized. Within the New Legislative Framework, on which the AI Act is explicitly modelled⁹⁹, technical standards provide the concrete technical specifications through which essential legal requirements can be operationalized and verified, offering both state-of-the-art solutions and a presumption of conformity. This fundamental role of standards is all the more important in the field of human oversight, as they are expected to provide at least some degree of much needed operational guidance. Thanks to sandboxes, lessons learned from experimentation can directly feed into the standardization process, ensuring that emerging standards on open issues such as interpretability, robustness, and – crucially – human oversight, reflect real-world operational challenges. In this respect, the early involvement of standardization bodies in sandbox governance can help to align experimental practices with the forthcoming body of harmonized standards, enabling from the outset a feedback loop between reg-

ulatory learning and technical standard-setting¹⁰⁰. This approach is supported by Article 58(2)(f) AI Act, which requires that implementing acts ensure the involvement of, *inter alia*, standardization organizations in the operation of AI regulatory sandboxes, thereby confirming their central role in this co-regulatory ecosystem.

5.2. Selection criteria and operational focus

Additionally, given the strict correlation between human oversight obligations applicable to providers under Article 14 and those incumbent upon deployers under Article 26¹⁰¹, as discussed in Section 2.2 above, the possibility for providers to submit applications in partnerships with deployers, foreseen by Article 58(2)(b), should be especially emphasized and operationalized in the context of human oversight-specialized regulatory sandboxes. Bringing deployers into the sandbox environment adds considerable value, as they bear ultimate responsibility in ensuring that oversight mechanisms designed by providers are effectively translated into practice when AI systems are put to use. In line with this approach, Article 26 explicitly requires deployers to use high-risk AI systems in line with the provider's instructions for use, which – crucially – shall include human oversight measures¹⁰², and to assign human oversight to natural persons with adequate competence, training, authority, and support. This structural dependency between the design obligations of the provider and the operational duties of the deployer can be tested to its full extent when both actors jointly participate in the sandbox. A cooperative approach between providers and deployers would thus not only facilitate a more realistic assessment of how human oversight operates in practice but also generate evidence-based insights to inform more coherent and actionable guidance for both categories of AI operators.

98. In particular, Art. 24(1) of the Directive states that: “The supervisory authority or authorities responsible for monitoring the application of Regulation (EU) 2016/679 shall also be responsible for monitoring and enforcing the application of Articles 7 to 11 of this Directive as far as data-protection matters are concerned [...]”.

99. For a thorough analysis, see: VEALE–ZUIDERVEEN BORGESIUUS 2021.

100. BAGNI–SEFERI 2025.

101. Deployers may also be required to implement further oversight measures as data controllers or as digital labour platforms, where applicable, under, respectively, Article 22 GDPR and Article 10 of the Platform Work Directive, thus creating further complexity.

102. Art. 13(3)(c) AI Act.

To fully optimize the advantages of oversight-specific sandboxes, especially to foster legal certainty and regulatory learning, it is further suggested that competent authorities should operate strategically when considering which submissions to accept, by giving precedence to those applications that raise the most significant operative and/or interpretative challenges for the implementation of human oversight obligations. This approach would closely align with AI regulatory sandboxes' rationale and objectives: by prioritizing cases where the interpretation and/or operationalization of human oversight obligations are most uncertain, authorities would maximize the sandbox's added value as a vehicle for regulatory learning and evidence-based guidance for both competent authorities and AI operators. The European Commission's implementing acts on AI regulatory sandboxes, foreseen by Article 58 AI Act, should thus include the presence of legal barriers and interpretative challenges as an eligibility and selection criterion for prioritizing participation.

In practice, a human oversight-specific sandbox would operate not unlike a "traditional" sandbox, that is, through phased cycles (typically, application phase, testing and experimentation, and exit), for a limited time and with the issuance of a final exit report, to be leveraged by participants to demonstrate compliance with the relevant obligations and to be accessed by the Commission and other competent authorities¹⁰³. These reports would moreover produce reusable deliverables and should hence preferably be made public to enhance regulatory learning outcomes, as foreseen by Article 57(8) AI Act: in case where the individual sandbox application is successful, they may contain practical insights and guidelines for the application of human oversight requirements, such as organizational playbooks to carry out oversight activities successfully, training materials for overseers, best practices for drafting and implementing providers' instructions for use, standardized documentation formats and potential suggestions for amendments to current laws and technical standards could emerge from sandbox testing. At a minimum, insights into best practices and lessons learned from operating the sandbox

should be included in the yearly reports to be sent by competent authorities to the AI Office under Article 57(16) AI Act. Ideally, to further favour their dissemination and uptake across the Union, such insights should also be integrated into the AI literacy initiatives coordinated by the AI Office, thereby ensuring that the lessons learned translate into broader capacity-building for both regulators and AI operators.

On the operational side, the specific sandbox plan to be agreed *ex ante* between competent authorities and the applicant should specify: (i) the chosen model of oversight (e.g., human-in-the-loop/on-the-loop/in-command, or a combination thereof) together with its technical measures and safeguards (e.g., granular logging to ensure accountability, kill switches, threshold alerts for bias detection, minimum interpretability requirements); (ii) organizational procedures for the allocation of oversight roles, to be included by the provider in the instructions for the deployer, recommended training requirements for human overseers (also in light of AI literacy requirements under Article 4 AI Act), maximum review times, traceability of overrides or deviations; (iii) metrics to measure oversight effectiveness, including error detection rates, justified overrides, timeliness of interventions, consistency of decision-making, levels of unlawful bias mitigated, and indicators of automation reliance; and (iv) in light of the overlapping GDPR requirements, a Data Protection Impact Assessment with a focus on data protection-mandated human oversight requirements under Article 22¹⁰⁴.

If carefully planned, also in light of the aforementioned policy recommendations, specialized sandboxes for human oversight could play a decisive role in addressing the gap between the EU legislator's aspirations on human oversight and the real-world shortcomings thereof. Their introduction would thus represent a crucial step towards transforming human oversight from a largely rhetorical safeguard into a verifiable practice.

The following conclusions will summarize the main findings of this paper and point to possible avenues for further research and policy development.

103. See, respectively, Art. 57 paras. 7 and 8.

104. A clear example of such processing activities would be the generation and retention of logs related to the human overseer's activities, as also mandated by Arts. 12 and 26 of the AI Act.

6. Conclusions and path forward

Drawing from current literature and research, this paper has argued that while human oversight has become one of the EU legislator's leading safeguards against algorithmic harms, its practical effectiveness is far from guaranteed and, if not carefully implemented, may even worsen already-present issues. Cognitive, organizational, and structural shortcomings, together with regulatory overlap, undermine the very safeguard that the law places so much trust in. In this respect, regulatory sandboxes – as foreseen in the AI Act – offer a promising venue to transform human oversight from a rhetorical safeguard into a verifiable, evidence-based practice.

The analysis carried out in Section 3 has shown that while human oversight remains one of the central safeguards in EU regulation of automated decision-making, its practical implementation is not without its shortcomings. Cognitive limitations, organizational pressures, and systemic biases all compound to render oversight often more symbolic than effective, thus undermining the very objective of the GDPR and AI Act to protect fundamental rights when deploying automated decision-making. It is against this problematic scenario that specialized AI regulatory sandboxes for human oversight emerge as a particularly promising avenue to reap the full benefits that are promised by human oversight measures. This kind of tailored sandboxes would foster “specialized” regulatory learning on human oversight, generate empirical evidence to inform coherent, EU-wide guidance and technical standardization in this sector, both to shape current interpretation and understanding of legal measures on oversight, and to consider possible future adjustments to the legal framework.

In this respect, the forthcoming European Commission's implementing acts under Article 58 AI Act, offer a unique opportunity to embed this specialization into the sandbox framework. The Commission should ensure that the implementing rules explicitly allow sandboxes to focus on specific legal requirements such as human oversight and promote the systematic dissemination and mutual recognition of sandbox results across Member States.

Specialized sandboxes tailored for human oversight could help regulators and AI operators experiment with concrete models, metrics, benchmarks, and practices to actually meet legally-mandated requirements for human oversight, while also enabling regulatory learning from involved authorities. In this latter respect, by concentrating and stimulating specialized expertise in competent authorities, reducing fragmented experimentation, and directly feeding lessons learned into forthcoming technical standards, common specification and AI literacy initiatives, these sandboxes could accelerate the correct operationalization of horizontal human oversight obligations under Articles 14 and 26 AI Act, Article 22 GDPR, as well as other sectorial and overlapping human oversight obligations, notably Article 10 of the Platform Work Directive, including their overlapping application.

At a broader policy level, sandboxes also represent an important opportunity for the EU to reaffirm its fading global leadership in digital regulation at a moment when that leadership is being questioned. As underlined in the Draghi Report, excessive and overlapping regulation in the digital sphere risks eroding the Union's competitiveness¹⁰⁵; yet, the same report singles out sandboxes as innovation-friendly mechanisms that can enable continuous assessment of regulatory hindrances¹⁰⁶. If the EU manages to effectively operationalize human oversight through specialized sandboxes, it could decisively influence other jurisdictions currently adopting (and, possibly, struggling with the operationalization of) similar requirements, thus regaining its lost momentum in setting global standards for digital regulation.

Member States, and even regional or local authorities, have a unique opportunity to build sandboxes dedicated to human oversight, possibly linked to sector-specific experimentation frameworks (e.g., those already existing in the field of FinTech, healthcare, automotive, etc.). This could create an EU network of oversight sandboxes that leverages diversity of contexts while ensuring coherence through coordination by the AI Office under Article 57 AI Act.

105. DRAGHI 2025, p. 79.

106. *Ivi*, p. 84.

This paper aims to stimulate a debate on whether such an approach is desirable and, if so, how it could be structured and governed, also offering some recommendations and policy proposals. Much will depend on the political will and resources that the EU and its Member States devote to these instruments. In any case, this path seems preferable than the current drift towards deregulation in EU digital policy which has taken place in the last year, amidst the Draghi Report and geopolitical tensions with the United States¹⁰⁷, as it provides a venue for

the EU to maintain and even advance its regulatory leadership on digital regulation.

Further research should provide a closer look on how experimentation within regulatory sandboxes can best support the adoption and testing of human oversight requirements, in particular by operationalizing Article 14 AI Act, and other oversight obligations through forthcoming technical standards or common specifications, and by identifying measurable benchmarks and metrics for oversight effectiveness across different sectors¹⁰⁸.

References

- A. ADINOLFI (2022), *Processi decisionali automatizzati e diritto antidiscriminatorio dell'Unione europea*, in A. Adinolfi, A. Simoncini (a cura di), "Protezione dei dati personali e nuove tecnologie – Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche", Edizioni Scientifiche Italiane, 2022
- ARTICLE 29 WORKING PARTY (2017), *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Wp251rev.01)*, 2017
- F. BAGNI (2023), *The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act*, in "Rivista Italiana di Informatica e Diritto", 2023, n. 2
- F. BAGNI, F. SEFERI (Eds.) (2025), *White Paper on Regulatory Sandboxes for AI and Cybersecurity*, CINI's Cybersecurity National Lab, 2025
- S. BARROS VALE, G. ZANFIR-FORTUNA (2022), *FPF Report: Automated Decision-Making Under the GDPR – A Comprehensive Case-Law Analysis*, in Future of Privacy Forum, 2022
- K. BRENNAN-MARQUEZ, D. SUSSEY, K. LEVY (2019), *Strange Loops: Apparent versus Actual Human Involvement in Automated Decision-Making*, in SSRN Scholarly Paper, 2019
- S. CANSU, J. FARRAR (2021), *Managed by Bots Report*, in "Worker Info Exchange", 2021
- E. CIRONE (2025), *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative*, in "Rivista Italiana di Informatica e Diritto", vol. 7, 2025, n. 1
- D. COLLINGRIDGE (1980), *The Social Control of Technology*, Frances Pinter Publisher Ltd., 1980
- COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (2025), *Artificial intelligence and public services: the CNIL publishes the results of its "sandbox"*, in cnil.fr, 18 April 2025
- COUNCIL OF EUROPE (2024), *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, 2024
- J. DIRUTIGLIANO, D. BALDINI (2025), *The Right to Explanation: Legal Challenges and the Future of Fairness in Automated Decision-Making*, in "Journal of AI Law and Regulation", vol. 2, 2025, n.2

¹⁰⁷. POLITICO.EU 2025.

¹⁰⁸. An example of metrics concerning human oversight effectiveness in reducing (or indeed worsening) algorithmic discrimination has been devised and deployed by GAUDEUL et al. 2025. Other metrics could be developed and applied in other contexts, for example in order to measure human oversight effectiveness in reducing safety incidents for highly autonomous systems, and so on, to be tested in a specialized regulatory sandbox.

- L. DOWNES (2009), *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age*, Basic Books, 2009
- M. DRAGHI (2025), *The Future of European Competitiveness – In-depth analysis and recommendations (Part B)*, 2025
- L. ENQVIST (2023), *Human Oversight, in the EU Artificial Intelligence Act: What, When and by Whom?*, in “Law, Innovation and Technology”, vol. 15, 2023, n. 2
- EUROPEAN COMMISSION (2023), ‘Better regulation’ toolbox, July 2023 edition
- M. FINK (2025), *Human Oversight under Article 14 of the EU AI Act*, in SSRN Scholarly Paper, 2025
- A. GAUDEUL et al. (2025), *The Impact of Human-AI Interaction on Discrimination*, Publications Office of the European Union, 2025
- B. GREEN (2022), *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, in “Computer Law & Security Review”, vol. 45, 2022
- B. GREEN, A. KAK (2021), *The False Comfort of Human Oversight as an Antidote to A.I. Harm*, in SSRN Scholarly Paper, 2021
- HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (2019), *Ethics Guidelines for Trustworthy AI*, 2019
- H.M. HOLTZ, J. LEDENDAL (2026), *AI Data Governance – Overlaps Between the AI Act and the GDPR*, in “Law, Innovation and Technology”, 2026 (forthcoming)
- A. LANAMÄKI et al. (2025), *What to Expect from the Upcoming EU AI Act Sandboxes: Panel Report*, in “Digital Society” vol. 4, 2025, n. 2
- G. LAZCOZ, P. DE HERT, (2022), *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems. Essential Pre-Requisites against Abdicating Responsibilities*, in SSRN Scholarly Paper, 2022
- E. LONGO (2021), *Time and Law in the post-COVID-19 Era: the usefulness of Experimental Law*, in “Law and Method”, Special Issue: Experimental Legislation in Times of Crisis, edited by S. Ranchordàs, B. van Klink, 2021
- T. MADIEGA, A.L. VAN DE POL (2022), *Artificial intelligence act and regulatory sandboxes*, EPRS – European Parliamentary Research Service, 2022
- T. MORAES (2023), *Regulatory Sandboxes as Tools for Ethical and Responsible Innovation of Artificial Intelligence and Their Synergies with Responsive Regulation*, in SSRN Scholarly Paper, 2023
- OECD (2024), *Recommendation of the Council on Artificial Intelligence*, OECD Legal Instruments, 2024
- OECD (2023), *Regulatory Sandboxes in Artificial Intelligence*, OECD Digital Economy Papers, 2023
- A. PANEZI (2024), *Requirements of High-Risk AI Systems: AI Act. Article 14. Human Oversight*, in SSRN Scholarly Paper, 2024
- POLITICO.EU (2025), *Trump threatens ‘substantial’ new tariffs against countries with ‘discriminatory’ digital rules*, 2025
- S. RANCHORDAS, V. VINCI (2024), *Regulatory Sandboxes and Innovation-Friendly Regulation: Between Collaboration and Capture*, in “Italian Journal of Public Law”, vol. 1, 2024
- D.J. SOLOVE, H. MATSUMI (2024), *AI, Algorithms, and Awful Humans*, in “Fordham Law Review”, vol. 92, 2024, n. 5
- L. TOSONI (2021), *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation*, in “International Data Privacy Law” vol. 11, 2021, n. 2

UNESCO (2021), *Recommendation on the Ethics of Artificial Intelligence*, UNESDOC Digital Library, 2021

UNITED NATIONS (2024), *Resolution on AI*, United Nations General Assembly Resolutions, 2024

M. VEALE, F. ZUIDERVEEN BORGESIU (2021), *Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, in “Computer Law Review International”, vol. 22, 2021, n. 4

S. WACHTER (2022), *The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law*, in “Tulane Law Review”, vol. 97, 2022, n. 2



BENEDETTO PONTI

Il tool ACOI per lo screening del conflitto d'interessi e il gap italiano da colmare nei sistemi AI di prevenzione della corruzione

Il saggio, attraverso lo studio di caso del progetto PNRR “ACOI-Assessing Conflicts of Interest”, esamina le condizioni che renderebbero un sistema AI anticorruzione operativo nell'ordinamento italiano. ACOI — sviluppato in partnership dall'Università di Perugia e da Transcrime (Università Cattolica del Sacro Cuore), in collaborazione con il Ministero dell'Interno — ha verificato empiricamente la praticabilità tecnica di uno strumento di screening automatizzato del conflitto d'interessi su un campione di 485 dirigenti pubblici, incrociando dati di ANPR, Registro delle Imprese, Catasto e Orbis, confermando la fattibilità del modello. L'analisi individua tuttavia le condizioni abilitanti necessarie per il passaggio dalla sperimentazione all'operatività sistematica: sul piano normativo, la designazione legislativa delle banche dati autorizzate e la specificazione del trattamento AI secondo il requisito di legalità funzionale (art. 2-ter Codice privacy); sul piano giuridico-infrastrutturale, l'accesso strutturato attraverso la PDND; sul piano tecnico, la conformità ai requisiti AI Act per i sistemi ad alto rischio, pseudonimizzazione embedded e supervisione umana degli alert. La conclusione — anche in prospettiva comparata internazionale — è che il gap italiano non è tecnologico ma normativo e organizzativo, e che colmarlo costituisce oramai un dovere imposto dalla Direttiva (UE) 2026/1021 sulla prevenzione e il contrasto della corruzione.

Anticorruzione – Intelligenza artificiale – Conflitto d'interessi – Screening automatizzato – ACOI

The ACOI tool for conflict-of-interest screening and the Italian gap to be closed in AI-based corruption prevention systems

This article examines, through the case study of the PNRR project “ACOI – Assessing Conflicts of Interest”, the conditions that would make an AI-based conflict-of-interest prevention system operationally viable in Italy. ACOI — developed in partnership by the University of Perugia and Transcrime (Università Cattolica del Sacro Cuore), in collaboration with the Ministry of the Interior — empirically tested an automated screening tool on 485 public managers, cross-referencing data from the National Population Register, the Companies Register, the Land Registry, and Orbis, confirming the model's feasibility. The analysis identifies the enabling conditions still required for the transition to systematic operation: legislative designation of authorised data sources and specification of AI-based processing under the functional legality standard (Art. 2-ter Privacy Code); structured access through the National Digital Data Platform (PDND); and compliance with AI Act requirements for high-risk systems, including embedded pseudonymisation and meaningful human oversight. The conclusion — also from a comparative perspective — is that Italy's gap is not technological but normative and organisational, and that closing it is an obligation imposed by Directive (EU) 2026/1021 on the prevention and combating of corruption.

Anti-corruption – Artificial intelligence – Conflict of interest – Automated screening – ACOI

SOMMARIO: Introduzione. – Parte prima. L'AI nell'anticorruzione: una mappa comparata. – 1. I contributi epistemici dell'AI alla prevenzione della corruzione. – 1.1. L'estensione volumetrica. – 1.2. Il rilevamento di anomalie statistiche. – 1.3. La sintesi di conoscenza eterogenea. – 1.4. La topologia delle reti corruttive. – 1.5. La conoscenza anticipatoria. – 1.6. La percezione sensoriale estesa. – 1.7. La democratizzazione dell'accesso all'analisi anticorruzione. – 2. Le applicazioni mature: settori e casi. – 2.1. I contratti pubblici. – 2.2. L'antiriciclaggio e l'intelligence finanziaria. – 2.3. Le dichiarazioni patrimoniali e i conflitti di interesse. – 2.4. Il monitoraggio della spesa pubblica. – 2.5. L'amministrazione fiscale. – 3. Le applicazioni sperimentali: promesse e limiti. – 3.1. L'AI nelle indagini giudiziarie sulla corruzione. – 3.2. La governance delle risorse naturali. – 3.3. L'AI generativa e i Large Language Models. – 3.4. Il riconoscimento facciale, la biometria e i droni. – Parte seconda. La governance dei dati in Italia: forze e debolezze. – 4. I vincoli della tutela dei dati personali. – 4.1. Il GDPR come doppio binario: tutela e circolazione. – 4.2. Lo *strict legality standard* e l'evoluzione verso la legalità funzionale. – 4.3. La base di liceità "compito di interesse pubblico". – 5. La Piattaforma Digitale Nazionale dei Dati e il PNRR. – 5.1. L'architettura della PDND. – 5.2. Potenziale e limiti per i sistemi AI anticorruzione. – 6. L'AI Act e la legge 9 luglio 2025, n. 132. – 6.1. I sistemi AI ad alto rischio nella pubblica amministrazione. – 6.2. La disciplina italiana della legge 132/2025. – Parte terza. Il gap da colmare: il tool ACOI come studio di caso. – 7. Il divario su piano generale: confronto internazionale e focus sui contratti pubblici. – 8. Lo studio di caso: il progetto ACOI. – 8.1. La metodologia ACOI. – 8.2. La base giuridica nella ricerca. – 8.3. Le condizioni abilitanti: piano normativo, giuridico e tecnico. – 8.4. Un imperativo europeo non più differibile. – 9. Conclusioni: un'agenda non più rinviabile.

Introduzione

La governance dei dati¹ si configura come uno degli snodi fondamentali affinché il patrimonio informativo pubblico possa essere pienamente sfruttato, entro il nuovo paradigma abilitato dalle intelligenze artificiali. La letteratura internazionale documenta con crescente sistematicità l'impiego di sistemi algoritmici nella prevenzione della corruzione: sistemi di machine learning analizzano in tempo reale le procedure di affidamento dei contratti pubblici in Brasile, in Ucraina e in Portogallo; modelli predittivi stimano la probabilità di manipolazione delle gare prima che queste vengano aggiudicate; strumenti di elaborazione del

linguaggio naturale processano decine di migliaia di segnalazioni di operazioni sospette nell'arco di settimane che un ufficio tradizionale impiegherebbe anni a gestire; immagini satellitari elaborate con algoritmi di computer vision rilevano il disboscamento illegale con mesi di anticipo e con un'accuratezza che non ha precedenti nella storia del monitoraggio ambientale².

Eppure l'Italia – che dispone di un'architettura normativa anticorruzione tra le più articolate d'Europa, di patrimoni informativi pubblici di straordinaria ricchezza e di infrastrutture di interoperabilità in fase di implementazione, grazie agli investimenti del PNRR – sconta un ritardo

1. Il presente contributo è stato realizzato anche sulla scorta dei risultati del progetto di ricerca "Assessing conflict of interest – ACOI", finanziato dall'Unione europea – NextGenerationEU, Missione 4 "Istruzione e ricerca", Componente 2 "Dalla ricerca all'impresa", Investimento 1.1 – PRIN 2022 PNRR, progetto P2022JSLZW, CUP J53D23018880001. Università degli Studi di Perugia (resp. Benedetto Ponti, PI di progetto) e Università Cattolica del Sacro Cuore di Milano (resp. Francesco Calderoni).

2. RESIMIC 2025.

sistematico nell'integrazione degli strumenti digitali avanzati a supporto dei meccanismi di prevenzione. Questo ritardo non si spiega (solo) con l'assenza di risorse o con una carenza di competenze tecniche disponibili nel sistema pubblico: si spiega, anche, se non soprattutto, con l'assenza di un'architettura normativa e istituzionale che definisca con sufficiente chiarezza le condizioni alle quali i dati pubblici e, tra questi i dati personali, detenuti dalle diverse amministrazioni possono essere integrati, messi in relazione e analizzati con strumenti AI a fini di prevenzione della corruzione³.

Il presente saggio si propone un obiettivo duplice. Sul primo versante, intende offrire una ricognizione sistematica delle applicazioni internazionali dell'AI nell'anticorruzione, organizzata lungo due assi analitici: quello della maturità delle applicazioni – distinguendo tra sistemi già operativi in contesti reali con risultati misurabili e sistemi ancora sperimentali con significative incertezze non risolte – e quello del tipo di contributo epistemico offerto, poiché non tutte le applicazioni AI producono lo stesso tipo di conoscenza e le implicazioni istituzionali, giuridiche e di governance cambiano notevolmente a seconda del contributo in gioco. Tale ricognizione è utile per verificare il gap accumulato in sede nazionale riguardo alle applicazioni di AI dedicate all'anticorruzione, anche con riferimento alle soluzioni più mature e consolidate. Sul secondo versante, il saggio intende analizzare il sistema italiano di governance dei dati nelle sue articolazioni di forza e di debolezza rispetto alle esigenze che l'impiego dell'AI nella prevenzione della corruzione pone: i vincoli derivanti dalla tutela dei dati personali alla loro circolazione integrata tra banche dati pubbliche; le opportunità aperte dall'infrastruttura di interoperabilità abilitata dagli investimenti del PNRR attraverso la Piattaforma Digitale Nazionale dei Dati (PDND); i rischi connessi all'impiego dell'AI nell'azione pubblica, anche alla luce del Regolamento (UE) 2024/1689 (AI Act) e della legge 9 luglio 2025, n. 132.

La chiave di lettura che permea il saggio muove dalla constatazione che il nodo problematico principale non è tecnologico ma giuridico-istituzionale: l'Italia dispone delle infrastrutture informatiche

e del patrimonio di dati necessari per costruire sistemi AI anticorruzione di alto profilo, ma non dispone ancora dell'architettura normativa di governance che renderebbe questi sistemi praticabili a regime. Colmare questo gap non è soltanto un'opportunità di policy: è una necessità imposta dal diritto sovranazionale ed eurounitario, tenuto conto in particolare degli impegni derivanti dalla recente direttiva Ue sulla prevenzione e il contrasto della corruzione che richiede agli Stati membri di dotarsi di misure efficaci di prevenzione, presidiate da organismi dotati delle risorse finanziarie, di staff e tecnologiche necessarie a renderle effettive⁴.

Il saggio si è articolato in tre parti. La prima parte offre la mappa comparata: una tassonomia dei contributi epistemici dell'AI all'anticorruzione (§1) e una ricognizione delle applicazioni mature (§2) e sperimentali (§3). La seconda parte analizza la governance dei dati in Italia: i vincoli della tutela dei dati personali (§4), le opportunità della PDND (§5) e il quadro regolatorio dell'AI (§6). La terza parte traduce la ricognizione comparata in analisi del gap italiano su un piano generale (§7) e attraverso uno studio di caso specifico – il progetto di ricerca ACOI sullo screening automatizzato dei conflitti di interesse (§8) – che consente di apprezzare in termini concreti le condizioni giuridiche per l'implementazione sistematica di un sistema AI anticorruzione nell'ordinamento italiano.

Parte prima. L'AI nell'anticorruzione: una mappa comparata

1. I contributi epistemici dell'AI alla prevenzione della corruzione

Prima di analizzare settori e gradi di maturità, è necessario comprendere che cosa fa l'intelligenza artificiale in termini di produzione di conoscenza. Le applicazioni AI di anticorruzione non sono tutte epistemicamente equivalenti, e distinguerle tra loro secondo questo parametro è importante. Infatti, i rischi, i requisiti istituzionali e le implicazioni giuridiche cambiano radicalmente a seconda del tipo di contributo epistemico in gioco. Si identificano di seguito sette tipologie, che attraversano

3. APEC 2025; v. anche la tassonomia “prevention, detection, sanction” adottata come framework di riferimento.

4. Direttiva (UE) 2026/1021, del 29 aprile 2026, sulla lotta contro la corruzione. Per il profilo della verifica del conflitto di interessi nel testo della direttiva, cfr. PONTI 2026.

trasversalmente i vari settori interessati e i diversi livelli di maturità, e costituiscono una chiave di lettura preliminare all'analisi svolta nel saggio⁵.

1.1. L'estensione volumetrica

Il contributo più accessibile e al tempo stesso più diffuso è quello che potremmo definire di estensione volumetrica: l'AI processa volumi di dati – documenti, transazioni, segnalazioni, dichiarazioni, atti amministrativi – che nessuna struttura di controllo umana potrebbe gestire con le risorse ordinarie. La quantità, in questo contesto, genera qualità: un sistema di controllo che esamina il 100% delle gare, anziché un campione del 3%, non è semplicemente più efficiente, ma produce un tipo diverso di evidenza, statisticamente e giuridicamente più robusta⁶.

I casi documentati sono significativi. Transparency International UK ha classificato con strumenti di machine learning oltre 140.000 voci del registro del lobbying britannico, costruendo per la prima volta una mappa sistematica delle reti di influenza sui processi legislativi. In Perù, il sistema Inspector AI elabora in un anno circa 23.000 segnalazioni di operazioni sospette (SARs), un volume che i revisori umani dell'UIF peruviana non avrebbero mai potuto processare con tempi comparabili. Nel procedimento contro Rolls-Royce condotto dallo Serious Fraud Office britannico (SFO), strumenti AI hanno esaminato un corpus documentale di milioni di pagine, consentendo di ridurre i tempi di analisi preliminare da anni a mesi⁷.

Il limite epistemico di questo tipo di contributo è tuttavia altrettanto preciso quanto la sua forza.

L'estensione volumetrica replica e amplifica il giudizio umano: se i criteri di classificazione sono sbagliati – se il modello ha imparato a riconoscere le forme di corruzione già identificate nel passato, anziché la corruzione effettiva – li applica a milioni di casi invece che a mille, moltiplicando l'errore sistematico anziché correggerlo. Il problema, che la letteratura specialistica denomina *selective labelling problem*, non è tecnico ma epistemologico: riguarda la qualità della conoscenza di partenza su cui il sistema viene addestrato, non la potenza computazionale con cui viene applicato⁸.

1.2. Il rilevamento di anomalie statistiche

Il secondo tipo di contributo è quello del rilevamento di anomalie statistiche: il sistema apprende la distribuzione statistica di un fenomeno – gare d'appalto, rimborsi spese, concessioni, pratiche edilizie – e segnala le deviazioni significative rispetto alla norma. A differenza di un sistema basato su regole scritte da esperti, che i soggetti corrotti imparano rapidamente ad aggirare modificando i comportamenti che attivano gli alert, il modello statistico non ha una teoria della corruzione: ha una teoria della normalità, e segnala tutto ciò che si discosta da essa in modo statisticamente rilevante. Questa neutralità statistica costituisce al tempo stesso il punto di forza e il punto di debolezza del contributo⁹.

In Brasile, il sistema Rosie – sviluppato dall'organizzazione civica Operação Serenata de Amor – applica algoritmi di machine learning alle note spese dei parlamentari: il solo effetto di pubblicazione degli alert ha prodotto una riduzione del 10% nelle richieste di rimborso per pasti, senza che

5. L'impianto analitico basato sulle sette tipologie di contributo epistemico è sviluppato, nella letteratura internazionale, a partire dalla distinzione tra usi "banali" e usi qualitativamente caratterizzati dell'AI proposta in RESIMIC 2025; e ZINNBAUER 2025. Cfr. anche APEC 2025; OECD 2025-A.

6. RESIMIC 2025, dove l'Autore utilizza l'espressione "mundane uses of AI" per designare le applicazioni di estensione volumetrica, avvertendo tuttavia che la denominazione è fuorviante: "the quality of evidence changes when you achieve 100% coverage instead of sampling".

7. Il sistema Inspector AI è documentato in GIZ 2024; cfr. anche RESIMIC 2025. Per il caso Rolls-Royce/SFO e il ricorso a strumenti AI per l'e-discovery su corpus documentali di milioni di pagine, cfr. OpenText 2018; APEC 2025.

8. Sul selective labelling problem come limite epistemologico strutturale delle applicazioni ML anticorruzione cfr. ASH-GALLETTA-GIOMMONI 2025; GALLEGO-RIVERO-MARTÍNEZ 2021; v. anche GERLI 2026.

9. I dati sul sistema Rosie (riduzione del 10% nelle richieste di rimborso per pasti) sono documentati in ODILLA 2023; cfr. anche ODILLA-MATTONI 2023. Per DOZORRO e il risparmio stimato di 133 milioni di UAH nel primo semestre 2025, cfr. RESIMIC 2025.

fosse necessario alcun procedimento sanzionatorio. In Ucraina, il sistema DOZORRO – integrato nella piattaforma di e-procurement Prozorro – ha prevenuto nel primo semestre del 2025 sprechi stimati in 133 milioni di UAH, rilevando pattern anomali nelle procedure di affidamento. In Ungheria, modelli di machine learning applicati alle gare pubbliche hanno raggiunto un'accuratezza dell'82% nella previsione delle offerte singole prima della loro pubblicazione, partendo dall'accuratezza di base del 77% dei sistemi a regole fisse.

Il tratto epistemico specifico di questo contributo – la neutralità statistica – si traduce in un deficit di interpretabilità che pone questioni di legittimità giuridica non trascurabili: il sistema non spiega perché qualcosa è anomalo, ma solo che lo è. Questa opacità è meno grave quando il modello viene usato per selezionare fascicoli da approfondire, ma diventa molto problematica quando l'alert produce effetti diretti su soggetti specifici, perché priva il destinatario della possibilità di comprendere e contestare le ragioni della segnalazione. I modelli più interpretabili tendono a essere meno accurati, e i più accurati meno interpretabili, generando un trade-off che non è tecnico ma politico: riguarda quanto rischio di opacità si è disposti ad accettare in cambio di prestazioni migliori, e la risposta a questa domanda non può essere delegata alla tecnologia¹⁰.

1.3. La sintesi di conoscenza eterogenea

Il terzo tipo di contributo è forse il più potente sul piano epistemico: la sintesi di conoscenza eterogenea, ossia la capacità di mettere in connessione archivi separati – registro delle imprese, catasto, dati fiscali, banche dati dei contratti pubblici, anagrafi degli eletti, registri del credito – e di generare, dall'incrocio, conoscenza che non preesisteva in nessuna delle fonti originali. Si tratta di un contributo qualitativamente diverso dall'amplificazione: non si tratta di fare più velocemente ciò che un funzionario potrebbe fare in linea di principio, ma di produrre connessioni che, per ragioni strutturali di

complessità cognitiva e di organizzazione per silos dei sistemi informativi pubblici, sarebbero impossibili da ottenere altrimenti. Il fatto che il titolare formale di un'impresa aggiudicataria sia il cognato di un funzionario che ha presieduto la commissione, che un immobile non dichiarato nelle disclosure patrimoniali appaia nel catasto, che una società offshore sia la stessa già oggetto di un'indagine penale in un'altra giurisdizione: nessuna di queste informazioni è segreta, ma tutte rimangono invisibili finché non vengono messe in relazione.

I casi documentati illustrano la portata di questo contributo. Il sistema cinese Zero Trust – che suscita comprensibili perplessità sul piano della governance e dei diritti fondamentali – incrocia più di 150 banche dati per monitorare oltre 8.700 funzionari pubblici, producendo connessioni che nessun ufficio ispettivo tradizionale potrebbe costruire. Secondo il final report del progetto DATACROS, coordinato da Transcrime e cofinanziato dalla Commissione europea nell'ambito dell'Internal Security Fund – Police, l'analisi ha riguardato le strutture proprietarie di oltre 56 milioni di imprese in 29 Paesi europei e il prototipo sviluppato è stato in grado di identificare correttamente fino all'83% delle imprese collegate a persone soggette a sanzioni o con precedenti penali¹¹.

Sul piano tecnico, questo tipo di contributo richiede un'infrastruttura che nella maggior parte dei sistemi pubblici non è ancora disponibile nella forma necessaria: data lake integrati, API interoperabili, standard tecnici comuni per la rappresentazione dei dati, regole di data governance che definiscano chi può accedere a quali dati e in quale forma. Il problema non è computazionale ma istituzionale e politico: i sistemi informativi delle amministrazioni pubbliche sono stati costruiti nel tempo per servire la singola amministrazione, non il sistema nel suo complesso, e la loro integrazione richiede non solo investimenti tecnologici ma una revisione profonda delle logiche organizzative che li governano. È

10. Sul trade-off tra interpretabilità e accuratezza dei modelli ML in ambito anticorruzione, e sulla natura politica (non meramente tecnica) di questa scelta, cfr. KÖBIS–STARKE–RAHWAN 2022; GERLI 2026. Per la letteratura sull'Explainable AI (XAI), si rinvia alla rassegna citata in RESIMIC 2025.

11. Sulla sintesi di conoscenza eterogenea come contributo epistemico e sull'uso di approcci data-driven per la valutazione del rischio di corruzione, cfr. OECD 2019; PARVANOV 2025. Per il sistema DATACROS (I, II e III) cfr. <https://www.transcrime.it/>. Per il sistema cinese Zero Trust, cfr. SOUTH CHINA MORNING POST 2019 e U4 ANTI-CORRUPTION RESOURCE CENTRE 2023.

precisamente questo il nodo che il sistema italiano di governance dei dati deve sciogliere.

1.4. La topologia delle reti corruttive

Il quarto tipo di contributo va oltre la sintesi eterogenea: non si limita a identificare singole connessioni anomale, ma rivela la struttura – la topologia – di reti corruttive. Chi occupa posizioni centrali, quali nodi fungono da intermediari obbligati, dove si concentra il controllo sull'intera rete, quali sono i legami più vulnerabili la cui rimozione comporta la disgregazione del sistema: si tratta di conoscenza che non riguarda singoli episodi o singole transazioni, ma l'architettura complessiva del fenomeno corruttivo. Per ragioni strutturali di complessità cognitiva, una rete di migliaia di entità con relazioni di secondo e terzo grado è semplicemente inaccessibile all'analisi umana, anche con risorse investigative illimitate: l'AI non amplifica la capacità umana di vedere, ma la sostituisce in un dominio in cui essa non opera affatto¹².

Un caso paradigmatico è ContÁgil, sviluppato dalla Controladoria-Geral da União brasiliana nell'ambito dell'Operação Lava Jato: basato su machine learning e analisi delle reti, ha ridotto da una settimana a un'ora il tempo necessario per mappare le reti di intermediari corruttivi, consentendo agli investigatori di identificare i nodi strategici del sistema e di concentrare le risorse nei punti di massima vulnerabilità. La letteratura accademica sulla *network analysis* applicata alla corruzione documenta con rigore come colpire nodi centrali di una rete corruttiva sia sistematicamente più efficace, in termini di risorse impiegate e di effetti sulla capacità operativa del sistema, di smantellarne un numero equivalente di nodi periferici¹³.

1.5. La conoscenza anticipatoria

Il quinto tipo di contributo epistemico rompe con la logica fondamentale del controllo anticorruzione

tradizionale, che è sempre stato reattivo: si interviene dopo che la corruzione è avvenuta, spesso molto tempo dopo. I sistemi di *predictive analytics* producono invece conoscenza sul futuro: la probabilità che una gara non ancora aggiudicata sia soggetta a manipolazione, che un funzionario in una certa posizione sia a rischio di comportamenti scorretti, che un'area geografica con certe caratteristiche strutturali sia vulnerabile a specifiche forme di corruzione. Si tratta del tipo di contributo epistemicamente più originale – e al tempo stesso del più problematico dal punto di vista giuridico e istituzionale.

Il sistema Forest Foresight, sviluppato dall'organizzazione WWF-Paesi Bassi, predice con sei mesi di anticipo e 80% di accuratezza dove avverrà disboscamento illegale su aree pilota in Gabon e nel Borneo. In Ungheria, il modello ML per la previsione delle offerte singole stima la probabilità di manipolazione prima dell'aggiudicazione, consentendo all'autorità di controllo di intervenire quando il costo dell'intervento è minimo e l'effetto massimo. In Colombia, un sistema di early warning basato su algoritmi di LASSO e gradient boosting assegna a ciascun contratto pubblico un punteggio di rischio prima che l'esecuzione inizi, permettendo di concentrare le risorse ispettive sulle situazioni più vulnerabili¹⁴.

Il problema epistemico e giuridico centrale è che la conoscenza anticipatoria opera su probabilità, non su evidenze. Un sistema che assegna a una gara un punteggio di rischio del 90% non afferma che quella gara è corrotta: stima che gare con caratteristiche simili lo siano state nel 90% dei casi passati. L'uso di questa informazione per prendere decisioni che incidono su soggetti specifici – intensificare i controlli, sospendere un'aggiudicazione, avviare un'indagine – pone questioni delicate su quale garanzia procedurale si applica al soggetto trattato diversamente sulla base di una stima probabilistica, e come si gestisce il rischio

12. Sulla capacità dell'analisi delle reti di far emergere la topologia dei fenomeni corruttivi, cfr. GERLI 2026; OECD 2025-A; RUSINOV 2025. Per ContÁgil e la riduzione da una settimana a un'ora nel mapping delle reti corruttive, cfr. ODILLA 2023; OECD 2025-B.

13. TELLO ARISTA–FAZEKAS–VOLKOTRUB 2026, dove si documenta il matching di 8 milioni di contratti pubblici con 11 milioni di record di beneficial ownership in sei paesi europei.

14. Per il sistema Forest Foresight (80% di accuratezza a sei mesi, aree pilota in Gabon e nel Borneo), cfr. WWF NETHERLANDS 2022; FAO 2024. Per il modello colombiano di early warning basato su LASSO e gradient boosting, cfr. GALLEGO–RIVERO–MARTÍNEZ 2021; cfr. anche RESIMIĆ 2025.

strutturale di self-fulfilling prophecy, per cui l'alert porta a più controlli, i controlli trovano più irregolarità, e le irregolarità trovate confermano l'accuratezza dell'alert, producendo un circolo che tende ad amplificare le asimmetrie di enforcement già esistenti¹⁵.

1.6. La percezione sensoriale estesa

Il sesto tipo di contributo può essere definito in termini di percezione sensoriale estesa: l'AI come organo di senso artificiale per monitorare realtà fisiche inaccessibili o troppo vaste per l'osservazione diretta. Non si tratta di amplificare il giudizio umano né di mettere in connessione archivi esistenti: si tratta di percepire ciò che l'umano non può fisicamente vedere, sia per ragioni geografiche (aree remote), sia per ragioni di scala (estensioni territoriali enormi), sia per ragioni tecniche (bande spettrali invisibili all'occhio umano). Computer vision e remote sensing applicati alla governance delle risorse naturali rappresentano il caso più maturo di questo tipo di contributo. Il sistema Global Fishing Watch – che monitora il comportamento delle imbarcazioni industriali attraverso i segnali AIS e l'analisi di immagini satellitari radar – ha documentato come il 72-76% delle imbarcazioni sfugga al monitoraggio pubblico attraverso la disattivazione deliberata dei transponder: dati invisibili a qualsiasi sistema di controllo tradizionale¹⁶.

Il limite strutturale di questo tipo di contributo è diverso dagli altri: la percezione estesa genera alert su eventi fisici, ma la traduzione di questi alert in azione anticorruzione richiede capacità di risposta sul campo – personale, mezzi, coordinamento istituzionale, volontà politica – che in molti dei contesti più vulnerabili alla corruzione nella governance delle risorse naturali semplicemente non esistono. Il divario tra capacità di rilevamento

e capacità di risposta rischia di trasformare gli alert in documenti di monitoraggio senza conseguenze operative.

1.7. La democratizzazione dell'accesso all'analisi anticorruzione

Il settimo tipo di contributo è epistemicamente diverso dagli altri: non si tratta di produrre conoscenza nuova per esperti istituzionali, ma di rendere accessibile la conoscenza esistente a soggetti che non avrebbero altrimenti la capacità cognitiva o tecnica di elaborarla – cittadini, giornalisti, organizzazioni della società civile, ricercatori, piccole e medie imprese. Il sistema Rosie in Brasile non solo elabora le note spese parlamentari, ma pubblica gli alert in formato comprensibile ai cittadini, permettendo un monitoraggio diffuso che l'architettura istituzionale tradizionale non avrebbe mai consentito. DOZORRO in Ucraina trasforma i dati grezzi della piattaforma Prozorro in alert leggibili dalla società civile e dai media, costruendo un secondo livello di controllo che integra e in certi casi supplisce alle carenze del primo¹⁷.

Il tratto epistemico specifico di questa tipologia è la riduzione delle asimmetrie informative tra chi detiene il potere e chi ne è governato. La corruzione prospera nell'opacità; la trasparenza è una delle sue principali contromisure. Ma la trasparenza formale – la pubblicazione di dati in formato PDF su siti istituzionali – produce informazione che resta largamente inaccessibile a chi non dispone di competenze tecniche per elaborarla. L'AI che trasforma questa informazione in segnali comprensibili e azionabili da attori non specializzati realizza una forma di empowerment cognitivo con effetti anticorruzione strutturali: non perché l'AI scopra la corruzione, ma perché aiuta gli umani a scoprirla, redistribuendo la

15. La self-fulfilling prophecy come rischio strutturale dei sistemi di predictive analytics anticorruzione è analizzata in GALLEGO-RIVERO-MARTÍNEZ 2021; cfr. anche RESIMIĆ 2025, che parla di “feedback loops that can reinforce existing enforcement biases”.

16. Per Global Fishing Watch e il dato che il 72-76% delle imbarcazioni industriali sfugge al monitoraggio pubblico attraverso la disattivazione deliberata dei transponder AIS, cfr. PAOLO-KROODSMA-RAYNOR et al. 2024; GLOBAL FISHING WATCH 2022. Per una panoramica dei sistemi di remote sensing applicati alla governance ambientale, cfr. APEC 2025.

17. Sul potenziale delle applicazioni AI per la democratizzazione del controllo civico e la riduzione delle asimmetrie informative, cfr. ODILLA-MATTONI 2023; ODILLA 2025; ZINNBAUER 2025. Per l'esperienza italiana si rinvia ai progetti Monithon (OpenCoesione), IrpiMedia e Openpolis, con le relative documentazioni istituzionali.

capacità cognitiva anziché concentrarla ulteriormente negli organi di controllo istituzionale¹⁸.

2. Le applicazioni mature: settori e casi

La distinzione tra applicazioni mature e sperimentali va intesa come gradiente, e non come una soglia netta. Si propone di qualificare come “mature” le applicazioni che dispongono di sistemi operativi in contesti reali, di risultati misurabili pubblicati e verificabili, e di un numero sufficiente di casi indipendenti da consentire comparazioni significative. La maturità non implica assenza di problemi: anche le applicazioni più avanzate presentano vulnerabilità strutturali che si analizzeranno a seguire. Significa, però, che vi è sufficiente evidenza empirica per valutarne l'efficacia, identificarne i limiti ricorrenti e trarne indicazioni per le politiche pubbliche¹⁹.

2.1. I contratti pubblici

I contratti pubblici costituiscono il settore più avanzato nell'applicazione dell'AI anticorruzione, con il maggior numero di implementazioni reali, i dati di impatto più verificabili e i modelli più trasferibili. La ragione strutturale di questa maturità è duplice: per un verso, le procedure di affidamento producono dati strutturati in formato digitale – bandi, offerte, aggiudicazioni, prezzi – che si prestano naturalmente all'analisi algoritmica; per altro verso, la corruzione negli appalti è sistematicamente documentata come tra le più pervasive e costose, il che ha concentrato su questo settore l'attenzione istituzionale e le risorse di ricerca in via prioritaria. Le applicazioni operative si articolano su tre livelli distinti.

Al primo livello si collocano i sistemi di monitoraggio in tempo reale, che analizzano le procedure durante il loro svolgimento, prima

dell'aggiudicazione. Il caso più documentato è Alice (Achados e Licitações), sviluppato dalla Controladoria-Geral da União brasiliana: applica algoritmi di ML alle gare nell'istante in cui vengono pubblicate, producendo alert che possono portare alla sospensione della procedura prima che il contratto sia stipulato. Tra il 2019 e il 2022, Alice ha portato alla sospensione o alla cancellazione di procedure per un valore complessivo superiore a 9,7 miliardi di reais brasiliani, mantenendo la stessa efficacia di rilevamento a fronte di una riduzione del 28% del personale della CGU impegnato nei controlli preventivi. In Cile, il sistema VigIA della Contraloría General de la República utilizza modelli di ML per calcolare indici di rischio sulle procedure in corso, generando red flag automatiche in presenza di tempi di sottomissione anormalmente brevi, requisiti tecnici eccessivamente restrittivi o criteri di selezione insoliti²⁰.

Al secondo livello si collocano i sistemi di risk scoring pre-aggiudicazione, che assegnano a ciascuna gara un punteggio di rischio prima dell'aggiudicazione, consentendo alle autorità di controllo di concentrare le risorse ispettive sui casi statisticamente più vulnerabili. In Spagna, il sistema ML dell'Intervención General de la Administración del Estado (IGAE) applicato ai contributi pubblici ha identificato 42.152 casi ad alto rischio su 1,05 milioni di contratti analizzati, ottimizzando l'allocazione delle risorse ispettive in modo che non sarebbe stato possibile con metodi tradizionali. In Ungheria, modelli ML hanno raggiunto un'accuratezza dell'82% nella previsione delle offerte singole. In Colombia, il sistema di early warning integra variabili sulla stazione appaltante, il settore merceologico e il contesto territoriale per produrre stime di rischio che guidano l'allocazione delle ispezioni²².

18. L'AI si configura, in questo modo, come un mediatore della trasparenza; cfr. PONTI 2019-A.

19. Per la distinzione tra applicazioni mature e sperimentali nell'AI anticorruzione, cfr. RESIMIC 2025; ZINNBAUER 2025; APEC 2025, che adotta il framework tripartito “prevention, detection, sanction” come griglia di classificazione.

20. Sul sistema Alice (Achados e Licitações) della Controladoria-Geral da União e i risultati documentati nel periodo 2019-2022, cfr. CONTROLADORIA-GERAL DA UNIÃO 2022; ODILLA 2023.

21. Per il sistema VigIA (Contraloría General de la República de Chile) e la sua metodologia di risk scoring basata su ML, cfr. APEC 2025; RESIMIC 2025.

22. Per il sistema ML dell'IGAE spagnola applicato ai contributi pubblici e il dato di 42.152 casi ad alto rischio su 1,05 milioni di contratti analizzati, cfr. GERLI 2026, come uno dei benchmark europei più avanzati; KATONA-FAZEKAS 2024.

Al terzo livello si collocano i sistemi di audit post-aggiudicazione, che analizzano la documentazione dei contratti già conclusi per identificare irregolarità nell'esecuzione. Il Tribunal de Contas portoghese ha sviluppato, con il supporto dell'OCSE e della NOVA University Lisbon, un modello di risk assessment basato su ML e 37 indicatori per rafforzare il controllo degli appalti pubblici, migliorando l'efficienza dell'analisi e l'individuazione precoce di irregolarità²³.

Gli indicatori di rischio più utilizzati nei sistemi ML per i contratti pubblici – sistematizzati dalla guida Open Contracting Partnership del 2024 – comprendono: single bidding (procedure con un solo offerente, indicatore di mercati ristretti o accordi collusivi); winner rotation (alternanza regolare tra vincitori, indicativa di accordi orizzontali tra imprese); pricing anomalies (prezzi unitari che si discostano significativamente dai prezzi di mercato di riferimento); vendor concentration (elevata concentrazione delle aggiudicazioni su un numero ristretto di imprese); timeline compression (tempi di pubblicazione e aggiudicazione anormalmente compressi, che impediscono una competizione effettiva). La ricerca più avanzata non usa questi indicatori singolarmente ma in combinazione, sfruttando la capacità degli algoritmi ML di rilevare pattern complessi che coinvolgono più variabili simultaneamente²⁴.

Nel contesto italiano, il sistema di monitoraggio degli appalti è tra i più articolati per architettura normativa: il d.lgs. 31 marzo 2023, n. 36 ha disegnato un ciclo di vita interamente digitale dei contratti pubblici, la Banca Dati Nazionale dei Contratti Pubblici (BDNCP) gestita da ANAC costituisce uno degli archivi di dati sugli appalti più ricchi d'Europa per ampiezza della copertura, e la delibera ANAC n. 148 dell'aprile 2026 e il Bando Tipo n. 2/2026 hanno introdotto per la prima volta l'obbligo per gli operatori economici di dichiarare

l'eventuale utilizzo di sistemi di intelligenza artificiale nella predisposizione delle offerte e nell'esecuzione dei contratti, in attuazione dell'art. 13 della l. 132/2025 e del Regolamento (UE) 2024/1689. Il passaggio a sistemi ML automatizzati di risk scoring è tuttavia ancora in fase sperimentale, e il confronto con i sistemi spagnolo e portoghese – entrambi costruiti su basi normative e istituzionali comparabili – suggerisce che il gap da colmare è più organizzativo che tecnologico²⁵.

2.2. L'antiriciclaggio e l'intelligence finanziaria

L'antiriciclaggio e l'intelligence finanziaria costituiscono il secondo settore per maturità nell'applicazione dell'AI anticorruzione, con una storia di adozione algoritmica che precede cronologicamente quella degli appalti. Le unità di intelligence finanziaria (UIF) e le istituzioni bancarie sono state tra i primi ad adottare sistemi di machine learning per la detection di operazioni anomale, spinte da una combinazione di incentivi che non ha equivalenti in altri settori: obblighi normativi sempre più stringenti in materia di antiriciclaggio; risorse private consistenti e forte orientamento all'innovazione nel settore bancario; disponibilità di dataset strutturati e completi – le transazioni finanziarie – che si prestano naturalmente all'analisi algoritmica.

Il sistema Inspector AI, sviluppato dall'Unità di Intelligence Finanziaria peruviana con il supporto della GIZ, utilizza NLP e reti neurali per elaborare le SARs ricevute dalle istituzioni finanziarie, classificandole automaticamente per livello di rischio e producendo report strutturati per i revisori umani: a parità di personale, il numero di casi trasmessi alle procure si è più che raddoppiato, non perché il sistema abbia abbassato le soglie di segnalazione, ma perché ha liberato i revisori dall'onere di analisi preliminare. Nel settore bancario privato, il caso più citato è quello della partnership tra HSBC e Google: l'adozione di algoritmi ML per il rilevamento di operazioni sospette ha prodotto una riduzione del

23. Per il Tribunal de Contas portoghese e il modello di risk assessment basato su ML e 37 indicatori, cfr. OECD 2024-A; OECD 2025-B; cfr. anche LONGOBUCCO-FERWERDA 2025.

24. OPEN CONTRACTING PARTNERSHIP 2024. Gli indicatori sistematizzati dalla guida comprendono: single bidding, winner rotation, pricing anomalies, vendor concentration, timeline compression.

25. Il d.lgs. 31 marzo 2023, n. 36 ha disegnato un ciclo di vita interamente digitale dei contratti pubblici. Per un'analisi del "paradigma digitale dell'evidenza pubblica", cfr. MANCINI PALAMONI 2024.

75% nei falsi positivi, con un risparmio significativo in termini di costi di analisi manuale²⁶.

Nel contesto italiano, l'UIF della Banca d'Italia ha registrato nel 2025 il record storico di 162.058 segnalazioni di operazioni sospette, con un incremento dell'11,5% rispetto all'anno precedente, in una dinamica di crescita strutturale che ha reso non più differibile il ricorso a strumenti automatizzati di triage e classificazione. L'infrastruttura applicativa integrata RADAR incorpora un modello di risk scoring composto da tre componenti algoritmiche distinte: il ranking finanziario (valutazione automatica del peso di ciascun soggetto in proporzione ai volumi dell'operatività segnalata); il link rating (mapping attraverso algoritmi di analisi dei grafi dei collegamenti latenti tra SARs diverse sulla base di soggetti comuni e flussi finanziari incrociati); la classificazione automatica dei soggetti neutri, realizzata con modelli NLP. Si tratta di un'architettura che integra simultaneamente tre dei contributi epistemici identificati nella sezione precedente – rilevamento di anomalie statistiche, analisi topologica delle reti e sintesi di conoscenza eterogenea – in un sistema operativo unitario²⁷.

2.3. Le dichiarazioni patrimoniali e i conflitti di interesse

Le dichiarazioni patrimoniali dei funzionari pubblici e la verifica dei conflitti di interesse costituiscono un settore relativamente maturo, con implementazioni operative in diversi contesti nazionali, ma ancora lontano dalla piena maturità osservabile negli appalti. Le applicazioni ML in questo settore si articolano su due modalità distinte. La prima è quella del cross-referencing automatico: il sistema verifica sistematicamente la coerenza tra quanto dichiarato e i dati in possesso di altre amministrazioni – catasto, registro delle imprese, dati fiscali, anagrafi degli eletti – rilevando incongruenze che l'analisi manuale lascerebbe

invisibili, sia per ragioni di volume sia per ragioni di frammentazione istituzionale delle banche dati. La seconda modalità è quella del rilevamento di pattern temporali: il sistema analizza l'evoluzione nel tempo delle dichiarazioni, identificando variazioni patrimoniali anomale rispetto al profilo del dichiarante o strutture di detenzione di beni insolite per la categoria professionale di appartenenza.

Il sistema armeno di verifica automatica delle dichiarazioni patrimoniali integra i dati dichiarati dai funzionari con i dati del catasto, del registro delle imprese e dell'amministrazione fiscale, producendo alert automatici sulle incongruenze rilevate. Il progetto DATACROS applica algoritmi di ML e NLP alle strutture proprietarie di 56 milioni di imprese europee, individuando catene anomale riconducibili a soggetti politicamente esposti. Sistemi di verifica automatica sono altresì operativi in diversi paesi dell'Europa centrale e orientale – Romania, Georgia, Moldavia – dove le riforme anticorruzione degli ultimi anni hanno prodotto investimenti significativi in questo settore²⁸.

Nel contesto italiano, il sistema delle dichiarazioni patrimoniali è frammentato tra diversi regimi normativi e i formati di raccolta non sono standardizzati, con pubblicazione spesso in formati non machine-readable che rende l'analisi algoritmica sistematica tecnicamente impraticabile senza un intervento preliminare di normalizzazione. Il sistema ARACHNE della Commissione europea – parzialmente utilizzato in Italia per il monitoraggio dei beneficiari dei fondi strutturali e del PNRR – rappresenta il modello più vicino a un sistema di cross-referencing automatizzato già operativo nel nostro ordinamento. Più di recente, il progetto ACOI – Assessing Conflict of Interest, finanziato con fondi PNRR e condotto da Transcrime-Università Cattolica in collaborazione con l'Università di Perugia, ha testato uno strumento sperimentale per lo screening

26. Per il caso HSBC/Google (riduzione del 75% nei falsi positivi con l'adozione di algoritmi ML per il rilevamento di operazioni sospette), cfr. RESIMIC 2025; GIZ 2024.

27. Per il sistema RADAR (UIF) e le sue tre componenti algoritmiche (ranking finanziario, link rating, classificazione dei soggetti neutri mediante NLP), cfr. BANCA D'ITALIA 2025; BANCA D'ITALIA 2026. Dati 2025: 162.058 segnalazioni di operazioni sospette ricevute, con incremento dell'11,5% rispetto all'anno precedente.

28. Il progetto DATACROSS è documentato in *Report on AI-driven service*, nel sito transcrime.it. Sull'impiego di ML per il monitoraggio delle strutture societarie opache e per l'identificazione dei beneficiari effettivi di contratti pubblici, cfr. PARVANOV 2025; OECD 2019. Per le applicazioni in Romania, Georgia e Moldavia, cfr. RESIMIC 2025; APEC 2025.

automatizzato del rischio di conflitto di interessi, che costituisce lo studio di caso analizzato nella terza parte del presente saggio²⁹.

2.4. Il monitoraggio della spesa pubblica

Il monitoraggio della spesa pubblica discrezionale – rimborsi, indennità, contributi, agevolazioni – costituisce un settore in cui le applicazioni ML mostrano risultati misurabili ma anche, in alcuni casi documentati, effetti collaterali gravi che richiedono attenzione specifica. I casi di fallimento più noti – il sistema SyRi nei Paesi Bassi, annullato dalla Corte distrettuale dell'Aia nel 2020 come violazione della CEDU per l'impossibilità dei soggetti interessati di comprendere e contestare le ragioni del profilo di rischio; il sistema automatizzato del Michigan per l'assicurazione contro la disoccupazione, che ha prodotto circa 40.000 false accuse di frode; lo scandalo olandese del childcare benefit, che ha colpito decine di migliaia di famiglie innocenti portando alle dimissioni del governo Rutte nel 2021 – condividono tre caratteristiche: opacità algoritmica; assenza di supervisione umana effettiva; concentrazione degli errori sui soggetti più vulnerabili³⁰.

Questi casi dimostrano che il rischio di un'applicazione ML nel monitoraggio della spesa pubblica non è simmetrico: i danni da falsi positivi ricadono sistematicamente sulle fasce più deboli della popolazione. Si tratta del retroterra casistico da cui si è poi attivata l'esigenza di regolazione che ha trovato concretizzazione – nel contesto europeo – nell'adozione dell'AI Act.

2.5. L'amministrazione fiscale

L'amministrazione fiscale è il settore dove i sistemi ML hanno la storia più lunga e i risultati più robusti. Il confine tra evasione fiscale e corruzione amministrativa è mobile e spesso incerto: la collusione tra

funzionari fiscali e contribuenti – che permette a questi ultimi di ridurre arbitrariamente il proprio carico tributario in cambio di compensi illegali – è una forma di corruzione amministrativa con impatti enormi sul gettito pubblico e sulla fiducia istituzionale. Le applicazioni più mature riguardano tre aree: il risk scoring delle dichiarazioni fiscali; il rilevamento delle frodi carosello IVA, in cui sistemi che incrociano i dati del sistema VIES con quelli delle dichiarazioni fiscali nazionali identificano le catene di imprese utilizzate per generare crediti IVA inesistenti; e il monitoring of the monitors, ossia l'analisi comportamentale degli ispettori fiscali per rilevare pattern anomali nelle loro decisioni.

In Italia, l'obbligo di fatturazione elettronica, introdotto per tutte le partite IVA a partire dal 2019, ha prodotto un dataset di straordinaria ricchezza per l'analisi ML delle frodi IVA e delle incongruenze tra flussi economici dichiarati e reali. L'Agenzia delle Entrate gestisce il sistema VeRa (Verifica dei Rapporti Finanziari), che incrocia i dati dell'Anagrafe tributaria, dell'Archivio dei rapporti finanziari comunicato dagli operatori bancari e dei flussi dei pagamenti digitali, producendo liste di contribuenti a rischio per orientare l'attività di controllo. Il recupero complessivo dell'evasione ha raggiunto 18,1 miliardi di euro nel 2023, con l'Atto di indirizzo per la politica fiscale del febbraio 2026 che ha fissato la traiettoria evolutiva verso l'impiego di “nuovi strumenti di analisi avanzata dei dati, favoriti dall'applicazione di tecniche di intelligenza artificiale, quali il machine learning, il text mining e il network analysis”, utilizzando i dati “in chiave predittiva”³¹.

3. Le applicazioni sperimentali: promesse e limiti

Le applicazioni qualificate come sperimentali non lo sono necessariamente per ragioni tecniche: alcune tecnologie in questa categoria sono mature

29. CALDERONI-POLICINO-PONTI-VALLE 2026.

30. Sul sistema SyRi (Paesi Bassi) e il suo annullamento da parte della Corte distrettuale dell'Aia nel 2020 per violazione della CEDU, cfr. Rechtbank Den Haag, 5 febbraio 2020; APPELMAN-Ó FATHAIGH-VAN HOBOKEN 2021; RACHOVITSA-JOHANN 2022. Per lo scandalo olandese del childcare benefit e le dimissioni del governo Rutte nel 2021, cfr. RESIMIĆ 2025; APEC 2025.

31. Per il sistema VeRa (Verifica dei Rapporti Finanziari, Agenzia delle Entrate) e i risultati del recupero dell'evasione (18,1 miliardi di euro nel 2023), cfr. OECD 2026; OECD 2025-A. L'Atto di indirizzo per la politica fiscale del febbraio 2026 ha fissato l'obiettivo di impiegare “nuovi strumenti di analisi avanzata dei dati, favoriti dall'applicazione di tecniche di intelligenza artificiale, quali il machine learning, il text mining e il network analysis”, utilizzando i dati “in chiave predittiva”.

sul piano computazionale ma non lo sono sul piano istituzionale, giuridico o della governance. La distinzione rilevante non è dunque tra ciò che funziona e ciò che non funziona in laboratorio, ma tra ciò che ha maturato un'evidenza empirica sufficiente in contesti istituzionali reali e ciò che non ha ancora raggiunto questo stadio di sviluppo. In alcuni casi l'assenza di maturità si spiega con la novità della tecnologia; in altri con la complessità dei requisiti istituzionali necessari per la sua implementazione; in altri ancora con il fatto che i fallimenti documentati hanno raffreddato l'entusiasmo e rallentato la diffusione.

3.1. L'AI nelle indagini giudiziarie sulla corruzione

Le indagini giudiziarie anticorruzione costituiscono il fronte meno sviluppato della catena del valore, paradossalmente il più strategico in termini di deterrenza. La deterrenza dipende dalla probabilità percepita di sanzione, non solo dalla qualità della prevenzione; e la probabilità percepita di sanzione dipende, in larga misura, dalla capacità investigativa. Il caso ContÁgil costituisce l'esempio più citato: la capacità di mappare reti di intermediari corruttori in un'ora anziché in una settimana ha effettivamente modificato le strategie investigative dell'Operação Lava Jato. Va però detto che lo stesso sistema ha prodotto anche problemi significativi: un numero elevato di alert – a fronte di una capacità di risposta investigativa limitata – ha generato un effetto di alert overflow; la presenza di falsi positivi in una fase così delicata del procedimento penale ha esposto l'indagine a contestazioni sulla correttezza del metodo; e la scarsa adattabilità del sistema a tipologie di rete diverse da quelle su cui era stato addestrato ne ha limitato la trasferibilità ad altri contesti investigativi³².

Il caso del Serious Fraud Office britannico è ancora più istruttivo. Il sistema Axcelerate, utilizzato in decine di casi compreso quello contro Rolls-Royce, ha omissso documenti rilevanti dal corpus analizzato per problemi di codifica dei file – un tipo di errore tecnico ordinario, gestibile nell'analisi documentale commerciale, ma con conseguenze potenzialmente molto rilevanti nella fase di disclosure probatoria del processo penale. Il caso ha aperto contestazioni su condanne già definitive e ha costretto lo SFO a riconsiderare le proprie procedure di gestione dei sistemi AI nelle indagini penali. Questi episodi mostrano che i requisiti di qualità e tracciabilità necessari per l'uso dell'AI in un contesto giuridicamente rilevante sono significativamente più elevati rispetto a quelli sufficienti per l'uso in contesti di analisi gestionale³³.

3.2. La governance delle risorse naturali

Le applicazioni di computer vision e remote sensing alla governance delle risorse naturali rappresentano il caso più avanzato di percezione sensoriale estesa applicata all'anticorruzione. Il sistema Forest Foresight prevede con sei mesi di anticipo e 80% di accuratezza dove avverrà disboscamento illegale su aree pilota; il sistema Global Fishing Watch ha documentato come il 72-76% delle imbarcazioni industriali sfugga al monitoraggio pubblico attraverso la disattivazione deliberata dei transponder AIS. La ragione del carattere ancora sperimentale di queste applicazioni non sta nella tecnologia di rilevamento – che è matura – ma nella difficoltà di tradurre le evidenze visive in azione istituzionale efficace. In molti dei contesti più vulnerabili alla corruzione nella governance ambientale, la capacità di risposta sul campo è insufficiente per trasformare gli alert in interventi³⁴.

32. Sul caso ContÁgil nella fase investigativa dell'Operação Lava Jato e sui suoi limiti (alert overflow, falsi positivi, scarsa trasferibilità), cfr. la documentazione sul sistema disponibile nel sito istituzionale della Controladoria-Geral da União e ODILLA 2023. Per l'inquadramento metodologico della network analysis nelle indagini anticorruzione, cfr. OECD 2025-a.

33. Per il sistema Axcelerate (SFO britannico) e le contestazioni processuali derivanti dall'omissione di documenti per problemi di codifica, cfr. OPENTEXT 2018; BBC NEWS 2018; GOV.UK 2025; RESIMIC 2025. Il caso ha aperto la questione dei "quality and traceability requirements" necessari per l'uso dell'AI in contesti giuridicamente rilevanti.

34. Per Forest Foresight (previsione del disboscamento illegale con 80% di accuratezza a sei mesi) cfr. WWF NETHERLANDS 2022; FAO 2024. Per Global Fishing Watch (rilevamento del 72-76% di imbarcazioni non monitorate), cfr. PAOLO-KROODSMA-RAYNOR et al. 2024; APEC 2025.

3.3. L'AI generativa e i Large Language Models

L'applicazione di Large Language Models (LLM) all'anticorruzione rappresenta la frontiera tecnologicamente più avanzata e al tempo stesso la più controversa. I LLM aprono prospettive significative: analisi semantica di contratti, delibere, relazioni di audit, dichiarazioni patrimoniali per rilevare incongruenze linguistiche indicative di manipolazione; sintesi di corpus documentali vastissimi in tempi incompatibili con l'analisi umana; supporto alla redazione di quesiti investigativi complessi. Al tempo stesso, i limiti specifici dei LLM nell'ambito giuridico-investigativo sono di natura diversa rispetto ai sistemi ML tradizionali: le allucinazioni (generazione di informazioni plausibili ma false) introducono rischi di evidenza fabbricata; l'assenza di un audit trail verificabile rende difficile la tracciabilità del ragionamento; la latenza e i costi computazionali dei modelli più capaci ne limitano ancora l'utilizzo su larga scala³⁵.

Il profilo più critico, sul piano della governance, è quello della protezione dei dati personali: i LLM richiedono che i dati vengano elaborati dal modello, il che pone questioni rilevanti in ordine alla base di liceità del trattamento, alla compatibilità con la finalità originaria di raccolta dei dati e, soprattutto, alle garanzie da assicurare qualora il modello venga utilizzato in modalità cloud (API verso provider esterni) anziché in-house. Questo profilo – di particolare rilevanza per il caso ACOI analizzato nella Parte terza – sarà esaminato nel quadro delle norme applicabili.

3.4. Il riconoscimento facciale, la biometria e i droni

Il riconoscimento facciale, le tecnologie biometriche e i droni rappresentano la categoria più controversa delle applicazioni sperimentali, per ragioni che attengono alla loro natura strutturalmente *dual-use*: sono strumenti potenti di rilevamento dell'identità e di monitoraggio fisico, ma

presentano rischi specifici di discriminazione algoritmica, normalizzazione della sorveglianza e potenziale utilizzo come strumenti di controllo politico. Il Regolamento (UE) 2024/1689 (AI Act) ne vieta, in generale, l'uso per la sorveglianza biometrica di massa negli spazi pubblici, con eccezioni tassativamente elencate per le forze dell'ordine in presenza di specifiche condizioni³⁶.

Le applicazioni anticorruzione più promettenti sono quelle che utilizzano i droni per il monitoraggio di infrastrutture (verifica della reale esecuzione di opere finanziate con fondi pubblici) e quelle che impiegano tecnologie biometriche per rafforzare i sistemi di identificazione dei funzionari pubblici e ridurre i fenomeni di "funzionario fantasma". Il carattere sperimentale di queste applicazioni non è tecnico ma normativo: i vincoli imposti dall'AI Act e, nel contesto italiano, dalla legge 132/2025 ne limitano significativamente il perimetro di utilizzo legittimo nell'ambito dell'azione pubblica.

È opportuno richiamare, a chiusura di questa parte ricognitiva, tre limiti strutturali che attraversano trasversalmente tutte le categorie applicative e che condizionano la praticabilità di qualsiasi sistema AI anticorruzione, indipendentemente dal settore di intervento e dal grado di maturità tecnologica: il *selective labelling problem* – il fatto che i sistemi addestrati su casi di corruzione già accertati replicano e amplificano i bias dell'enforcement precedente, imparando a riconoscere le forme di corruzione già identificate e non quelle ancora invisibili; l'opacità algoritmica – il *deficit di interpretabilità* che accompagna, in misura inversamente proporzionale alla loro accuratezza, tutti i sistemi ML; e il *rischio di cattura algoritmica* – la possibilità che attori corrotti imparino a manipolare i parametri dei sistemi di alert, o che i sistemi stessi vengano strumentalizzati per finalità di controllo politico anziché di prevenzione della corruzione.

35. Per le potenzialità degli LLM nell'analisi documentale anticorruzione e i loro limiti specifici (allucinazioni, mancanza di audit trail, latenza), cfr. OECD 2024-B; RESIMIĆ 2025; GERLI 2026. La letteratura sottolinea la necessità di distinguere tra LLM "in-house" e LLM tramite API a provider esterni sotto il profilo della protezione dei dati.

36. APEC 2025, sul riconoscimento facciale come "dual-use technology" con rischi specifici di discriminazione e normalizzazione della sorveglianza. Cfr. anche *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, che ha per la prima volta sottoposto a vaglio giudiziario l'uso del riconoscimento facciale da parte di autorità di polizia nel contesto europeo.

Parte seconda - La governance dei dati in Italia: forze e debolezze

4. I vincoli della tutela dei dati personali

La tutela dei dati personali costituisce, nell'ordinamento italiano ed europeo, il quadro normativo che più direttamente condiziona la praticabilità dei sistemi AI anticorruzione. Questa constatazione, tuttavia, non deve essere letta nel senso che la tutela dei dati personali sia un ostacolo alla prevenzione della corruzione: il quadro giuridico europeo – correttamente inteso – offre, accanto ai vincoli, anche le condizioni positive per un impiego legittimo e proporzionato dei dati personali a fini anticorruzione. La questione non è se il trattamento è possibile, ma a quali condizioni, con quali architetture e con quali garanzie. Chiarire questo punto è premessa indispensabile per una valutazione realistica del *gap* italiano.

4.1. Il GDPR come doppio binario: tutela e circolazione

Il Regolamento (UE) 2016/679 (GDPR) è comunemente percepito come strumento di tutela dei diritti fondamentali e, in quanto tale, come un vincolo alla circolazione dei dati. Questa percezione è corretta ma incompleta. Il GDPR opera, in realtà, su un doppio binario: da un lato, esso costituisce e garantisce il diritto fondamentale alla protezione dei dati personali, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea; dall'altro, esso abilita – attraverso la clausola di necessità e il sistema delle basi di liceità – la circolazione dei dati personali ogniquale volta essa sia giustificata da un interesse pubblico sufficientemente determinato, proporzionato e garantito. La tensione tra i due binari non è patologica ma strutturale: è la modalità con cui il Regolamento persegue il suo duplice obiettivo, esplicitato nell'art. 1: la protezione delle

persone fisiche con riguardo al trattamento dei dati personali “e” la libera circolazione di tali dati³⁷.

La Corte di giustizia ha precisato, con giurisprudenza costante, che il diritto alla protezione dei dati personali non è assoluto: deve essere “considerato alla luce della sua funzione nella società e bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità”. Il bilanciamento non è discrezionale: deve rispettare il test di proporzionalità sancito dall'art. 52(1) della Carta, che richiede che qualsiasi limitazione del diritto sia prevista dalla legge, rispetti il contenuto essenziale del diritto e sia necessaria e rispondente a finalità di interesse generale riconosciute dall'Unione. La prevenzione della corruzione – che attiene al corretto funzionamento delle istituzioni democratiche, all'efficienza dell'uso delle risorse pubbliche e all'uguaglianza dei cittadini di fronte alla legge – rappresenta un obiettivo di interesse generale pienamente riconosciuto dall'ordinamento europeo³⁸.

4.2. Lo *strict legality standard* e l'evoluzione verso la legalità funzionale

Uno dei nodi più rilevanti per la praticabilità dei sistemi AI anticorruzione nel contesto italiano è rappresentato dall'evoluzione dello standard di legalità applicabile ai trattamenti di dati personali da parte delle pubbliche amministrazioni. La letteratura ha distinto, a questo riguardo, tra uno “standard di legalità formale” e uno “standard di legalità funzionale”. Il primo richiede una norma di legge che autorizzi espressamente e tipicamente il singolo trattamento, con un grado di determinatezza analogo a quello richiesto per le limitazioni dei diritti fondamentali nel modello di Stato di diritto formale. Il secondo – quello adottato dal GDPR e, a partire dalla riforma del 2021, dall'ordinamento italiano – richiede che il trattamento sia necessario, proporzionato e pertinente alla finalità pubblica perseguita, ma non

37. PONTI 2025. L'Autore ricostruisce il GDPR come “strumento a doppio binario” che opera simultaneamente come tutela dei diritti fondamentali e come abilitatore della circolazione dei dati, ove la clausola di necessità (art. 6(1)(e)) “permea trasversalmente tutto il sistema, abilitando il trattamento ogniquale volta esso sia giustificato dall'interesse pubblico cui il trattamento è funzionale”.

38. Sul “diritto alla protezione dei dati personali” come diritto fondamentale a struttura non assoluta e soggetto a bilanciamento (art. 8 Carta dei diritti fondamentali UE; art. 52(1) Carta), cfr. Corte giust. UE (GC), 1° agosto 2022, causa C-184/20, *OT c. Vyriausioji tarnybinės etikos komisija*, §§ 63-70, dove la Corte sottolinea che “la protezione di tale diritto fondamentale non è tuttavia assoluta, ma deve essere considerata alla luce della sua funzione nella società e bilanciata con altri diritti fondamentali, conformemente al principio di proporzionalità”.

che sia nominativamente previsto da una norma che ne definisca tutti i dettagli operativi³⁹.

La riforma del Codice in materia di protezione dei dati personali (d.lgs. 196/2003), operata dal d.lgs. 10 agosto 2018, n. 101 in attuazione del GDPR, ha segnato il passaggio definitivo dalla legalità stretta alla legalità funzionale per i trattamenti di dati pubblici. L'art. 2-ter del Codice consente il trattamento per finalità di interesse pubblico in presenza di una norma che specifichi le finalità perseguite, i tipi di dati trattabili, le operazioni eseguibili e il titolare del trattamento – una norma di abilitazione parametrica, non un'autorizzazione puntuale per ciascun trattamento. Questo passaggio ha conseguenze dirette per i sistemi AI anticorruzione: significa che la prevenzione della corruzione, in quanto finalità di rilevante interesse pubblico già definita dalla legge 190/2012 e dai suoi decreti attuativi, può costituire la base normativa per trattamenti di dati personali funzionali a tale finalità, senza che sia necessaria una norma ad hoc per ciascun sistema applicativo, purché il trattamento sia necessario e proporzionato rispetto all'obiettivo perseguito⁴⁰.

4.3. La base di liceità “compito di interesse pubblico”

Per i sistemi AI anticorruzione operati da soggetti pubblici, la base di liceità principale è quella prevista dall'art. 6(1)(e) GDPR: il trattamento è lecito se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. La norma richiede che la finalità del

trattamento sia specificata – il “compito di interesse pubblico” deve avere un fondamento giuridico esplicito – ma non impone che la specifica operazione di trattamento sia nominativamente prevista, né che il sistema tecnologico utilizzato sia dettagliatamente descritto dalla norma abilitante. Il fondamento normativo del “compito di interesse pubblico” nei sistemi AI anticorruzione è, nell'ordinamento italiano, costituito dall'insieme delle norme della legge 190/2012, dei decreti attuativi (d.lgs. 33/2013, d.lgs. 39/2013), degli atti di ANAC (Piano Nazionale Anticorruzione) e, per i contratti pubblici, del d.lgs. 36/2023⁴¹.

Tuttavia, il ricorso a tool epistemici basati su AI comporta ulteriori profili di tensione con il GDPR, che hanno ricadute dirette proprio in termini di assetto e architettura della governance pubblica dei dati. In particolare, vengono in questione i profili relativi al principio della limitazione della finalità del trattamento (art. 5, par. 1, lett. b) del GDPR) e della minimizzazione dei dati (art. 5, par. 1, lett. c) del GDPR).

4.3.1. Limitazione della finalità del trattamento e uso secondario a fini di prevenzione della corruzione

Il principio di limitazione della finalità (*purpose limitation*) impone che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e che i trattamenti successivi alla raccolta siano compatibili con tali finalità originarie. L'uso di dati raccolti da pubbliche amministrazioni per finalità operative, gestionali, di trasparenza – appalti

39. PONTI 2025, dove si distingue tra “standard di legalità formale” (richiede una norma di legge che autorizzi espressamente il singolo trattamento, con tassatività e tipicità delle basi di liceità) e “legalità funzionale” (il trattamento è legittimo se è funzionale al perseguimento della finalità pubblica).

40. È questo l'effetto delle modifiche all'art. 2-ter del Codice privacy apportate dal d.l. 139/2021 convertito in legge 205/2021. In particolare – mentre il comma 1 apre alla possibilità che la base giuridica che giustifichi il trattamento dei dati personali per l'esercizio di compito di interesse pubblico o di un potere pubblico possa essere costituita, oltre che dalla legge o dal regolamento, anche da atti amministrativi generali – è il nuovo comma 1-bis a chiarire che “il trattamento dei dati personali da parte di un'amministrazione pubblica [...] è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti”, ciò che segna il passaggio alla piena vigenza della *necessary clause*; per la articolazione della clausola di stretta legalità e di quella della clausola di necessità, cfr., *amplius*, PONTI 2023-A.

41. Regolamento (UE) 2016/679, art. 6(1)(e): il trattamento è lecito “se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento”. PONTI 2025 analizza il rapporto tra la base di liceità pubblica (art. 6(1)(e)) e il principio di necessità come “meta-principio” che permea l'intero sistema: “la clausola di necessità non è un requisito aggiuntivo rispetto alla base di liceità, ma la condizione costitutiva della sua applicabilità”.

pubblici, dichiarazioni patrimoniali, registri delle imprese, dati fiscali – come base di addestramento di un sistema AI per la prevenzione della corruzione costituisce un trattamento ulteriore rispetto alla finalità originaria di raccolta, e come tale deve superare un positivo giudizio di compatibilità secondo i criteri dell'art. 6, par. 4 del GDPR⁴².

La sfida è in realtà doppiamente articolata. Il ciclo di vita di un sistema AI per la prevenzione della corruzione implica due distinte traslazioni di finalità: una prima traslazione dalla finalità originaria di raccolta alla finalità di addestramento del modello; una seconda traslazione dall'addestramento (o da quella originaria) alla finalità applicativa, ossia all'effettivo utilizzo del sistema AI a fini di prevenzione. Ciascuno dei due passaggi deve essere autonomamente valutato sotto il profilo della compatibilità con la finalità che precede, il che significa che la catena causale che conduce dalla raccolta originaria al deployment applicativo deve essere giustificata in ogni suo anello. L'eventuale compatibilità della finalità di addestramento con quella originaria non esaurisce il problema: occorre altresì valutare se la finalità applicativa – profilare il rischio corruttivo in procedure di appalto o in soggetti specifici – sia a propria volta compatibile con la finalità di addestramento.

Tra i criteri individuati dall'art. 6, par. 4 del GDPR per la valutazione di compatibilità assume rilievo centrale quello delle “ragionevoli aspettative degli interessati” al momento della raccolta

originaria. Ad esempio, la Corte di giustizia ha affermato, nel caso *Meta Platforms* (C-252/21), che la compatibilità tra finalità deve essere valutata anche in funzione di ciò che gli interessati potevano ragionevolmente attendersi al momento in cui i loro dati sono stati raccolti⁴³. Nel contesto che ci occupa, il parametro delle ragionevoli aspettative è particolarmente problematico. Un funzionario pubblico che dichiara i propri dati patrimoniali ai fini della trasparenza anticorruzione o un operatore economico che partecipa a una procedura di gara fornendo documentazione imprenditoriale e finanziaria può ragionevolmente attendersi che tali dati vengano impiegati per addestrare un sistema di machine learning finalizzato alla profilazione del rischio corruttivo individuale? La raccolta era funzionale a scopi specifici e definiti; l'uso dell'AI introduce una dimensione diversa per natura, impatto e logica elaborativa. Sotto questo profilo, il contesto normativo di riferimento, anche rispetto alla definizione dell'architettura di governance, potrebbe incidere sulla definizione e la consistenza di queste aspettative⁴⁴.

L'EDPB ha affrontato questo punto nel Parere (Opinion) 28/2024, con riferimento ai dati disponibili pubblicamente. Al par. 94, il Board afferma che “the fact that personal data are publicly available cannot be considered per se sufficient for the legitimate interests pursued by AI developers or deployers to override those of the data subjects”⁴⁵. Tuttavia, tale ragionamento non appare

42. La valutazione di compatibilità tra finalità originaria e finalità ulteriore del trattamento è regolata dall'art. 6, par. 4 del GDPR, che individua i criteri rilevanti: (a) il nesso tra le finalità; (b) il contesto in cui i dati sono stati raccolti e le ragionevoli aspettative degli interessati in merito all'ulteriore utilizzo; (c) la natura dei dati, con riguardo particolare alla sensibilità delle categorie di cui all'art. 9; (d) le possibili conseguenze dell'ulteriore trattamento per gli interessati; (e) l'esistenza di garanzie adeguate. Cfr. WP29 2013.

43. CGUE, sentenza del 4 luglio 2023, *Meta Platforms e a. c. Bundeskartellamt*, C-252/21, in particolare punti 112-124. La Corte ha chiarito che la compatibilità della finalità ulteriore con quella originaria deve essere valutata tenendo conto delle “ragionevoli aspettative” degli interessati al momento della raccolta dei dati: il mero fatto che l'interessato abbia accettato le condizioni generali di servizio non è sufficiente a fondare il consenso a trattamenti ulteriori radicalmente diversi per natura e impatto. Il ragionamento non è direttamente trasponibile al caso dei dati raccolti da pubbliche amministrazioni per scopi gestionali-amministrativi e successivamente utilizzati per addestrare sistemi AI, ma fornisce certamente elementi di cui tenere conto.

44. Il WP29 2013 aveva già individuato, tra i criteri per il giudizio di compatibilità, la considerazione delle “ragionevoli aspettative degli interessati” come elemento autonomo rispetto ai criteri oggettivi della natura dei dati e delle possibili conseguenze. Cfr. anche CGUE, sentenza del 1° agosto 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, punti 76-85, sulla tensione tra obblighi di trasparenza e protezione dei dati personali.

45. EDPB 2024. Il punto centrale dell'argomentazione è al par. 94: “the fact that personal data are publicly available cannot be considered per se sufficient for the legitimate interests pursued by AI developers or deployers to

direttamente trasponibile al caso dei dati pubblici raccolti in forza di obblighi normativi: la pubblica accessibilità dei dati o la disponibilità di tali informazioni in una banca dati pubblica, sebbene non costituisca l'equipollente di un consenso degli interessati al relativo utilizzo per finalità AI, non si pone allo stesso modo relativamente al giudizio di compatibilità con la finalità originaria. Pertanto, non è da escludersi che esista uno spazio (ancora da esplorare) per la costruzione di un'architettura normativa di governance dei dati pubblici che possa agevolare (a determinate condizioni) l'uso dei dati pubblici a fini di addestramento e poi di deployment di soluzioni di AI da destinare (anche) a fini di prevenzione della corruzione.

La soluzione più solida, per sciogliere questo – e al tempo stesso la più significativa per le implicazioni di governance – è quella di una destinazione legislativa esplicita. Ad esempio, se una norma di legge qualificasse determinate basi di dati come fonti autorizzate per i sistemi AI anticorruzione, e identificasse l'anticorruzione come finalità autonoma del trattamento, il problema della compatibilità con le finalità originarie finirebbe per attenuarsi in modo significativo: il trattamento troverebbe la propria base di liceità direttamente nella legge (art. 6, par. 1, lett. c) del GDPR – obbligo legale – o nella

ridefinizione normativa del compito di interesse pubblico ai sensi della lett. e)), senza necessità di un giudizio comparativo con finalità antecedenti⁴⁶. La designazione legislativa opera, in altri termini, come una clausola normativa di autorizzazione che incorpora e risolve a monte il problema della compatibilità delle finalità.

Questa prospettiva non è meramente teorica, ma trova riscontro in soluzioni normative già adottate nell'ordinamento italiano e in quello europeo. Il modello delle Basi di Dati di Interesse Nazionale (BDIN) nell'ambito della Piattaforma Digitale Nazionale dei Dati (PDND)⁴⁷ appare coerente con questo modello: la designazione legislativa di determinate basi di dati come BDIN, con conseguente priorità nell'interoperabilità, costituisce un atto normativo che definisce il perimetro dei flussi dati autorizzati tra amministrazioni, al di là delle finalità originarie delle singole raccolte. In tale schema, la Banca Dati Nazionale dei Contratti Pubblici – che raccoglie dati sull'intera filiera degli appalti pubblici italiani – potrebbe essere designata per legge come fonte primaria autorizzata per i sistemi AI anticorruzione gestiti dall'ANAC o da altra autorità competente⁴⁸. La designazione costituirebbe la base giuridica del trattamento secondario, rendendolo non più un uso “compatibile” della

override those of the data subjects”. Il ragionamento è speculare a quello della CGUE in C-252/21: la pubblica accessibilità dei dati non equivale ad aspettativa degli interessati che tali dati siano utilizzati per qualsiasi finalità, e in particolare per l'addestramento di sistemi AI destinati a profilare il rischio corruttivo.

46. La proposta di ricondurre l'autorizzazione all'uso di determinati dati pubblici per finalità AI a una designazione legislativa esplicita – che costituisce una base giuridica autonoma ai sensi dell'art. 6, par. 1, lett. c) o e) del GDPR – è sviluppata sistematicamente in PONTI 2025, in part. § 3 e § 5. L'Autore evidenzia come la designazione normativa costituisca lo strumento attraverso il quale l'ordinamento risolve a monte il problema della compatibilità delle finalità, incorporandola nella base di liceità.
47. L'art. 50-ter del codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82), come modificato dall'art. 47 del d.l. 31 maggio 2021, n. 77, convertito con modificazioni dalla l. 29 luglio 2021, n. 108, istituisce la Piattaforma Digitale Nazionale dei Dati (PDND) e prevede al comma 2 che le Basi di Dati di Interesse Nazionale (BDIN) costituiscano la priorità della prima fase di attuazione dell'interoperabilità. Le BDIN includono, tra le principali, il Registro delle imprese, l'Anagrafe Nazionale della Popolazione Residente, la Banca Dati Nazionale dei Contratti Pubblici (BDNCP), il Casellario delle imprese. Cfr. PONTI 2025.
48. La Banca Dati Nazionale dei Contratti Pubblici (BDNCP), gestita dall'ANAC ai sensi dell'art. 222 del d.lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici), costituisce l'esempio più rilevante ai fini del presente discorso. La sua designazione come BDIN implica che i dati in essa contenuti sono resi disponibili, sulla piattaforma PDND, a tutte le amministrazioni pubbliche che li richiedano per l'esercizio delle loro funzioni istituzionali. Una designazione legislativa esplicita della BDNCP (e di altre basi di dati rilevanti per la prevenzione della corruzione) come fonti autorizzate per i sistemi AI anticorruzione costituirebbe una base giuridica ai sensi dell'art. 6, par. 1, lett. c) del GDPR (obbligo legale), eliminando la necessità del giudizio di compatibilità con la finalità originaria della raccolta.

finalità originaria (con tutto il margine di incertezza che ne consegue), ma un uso direttamente autorizzato da norma primaria.

Un modello ancora più articolato è offerto dal regolamento EHDS (Regolamento (UE) 2025/327), che ho definito un caso di “uso strategico” delle basi di liceità del GDPR⁴⁹. L'EHDS predispone un'architettura normativa a doppio livello: il primo utilizza l'art. 6, par. 1, lett. c) e l'art. 9, par. 2, lett. i) e j) per fondare gli obblighi di condivisione dei dati sanitari imposti ai detentori; il secondo utilizza l'art. 6, par. 1, lett. e) e l'art. 9, par. 2, lett. g)-j) per qualificare come compito di interesse pubblico la funzione degli organismi di accesso ai dati sanitari. In entrambi i casi, la norma regolamentare definisce direttamente le finalità dei trattamenti secondari – ricerca, politiche sanitarie, innovazione – senza lasciare margine a un giudizio discrezionale di compatibilità caso per caso. La finalità dell'uso secondario è incorporata nella base di liceità stessa, che la autorizza e al contempo la delimita⁵⁰.

La traduzione di questa logica al settore dell'anticorruzione ha implicazioni immediate per l'architettura di governance. Se la designazione legislativa è la soluzione che consente di superare il vincolo della compatibilità delle finalità, allora la condizione necessaria per la piena legittimità dei sistemi AI anticorruzione è un intervento legislativo specifico che: (a) identifichi nominativamente le basi di dati pubbliche autorizzate ad alimentare

i sistemi AI (BDNCP, registri titolari effettivi, dichiarazioni patrimoniali dei pubblici funzionari, dati fiscali rilevanti, ecc.); (b) qualifichi la prevenzione della corruzione mediante AI come finalità autonoma di trattamento, costituente base di liceità ai sensi dell'art. 6, par. 1, lett. c) o e) del GDPR; (c) individui il soggetto istituzionale responsabile del trattamento e dell'accesso ai dati; (d) stabilisca le garanzie appropriate, proporzionate alla sensibilità dell'operazione, in termini di minimizzazione, controlli di accesso, tracciabilità, supervisione umana e revisione periodica⁵¹. In assenza di tale intervento, i sistemi AI anticorruzione opererebbero in una zona di incertezza normativa che li espone a contestazioni e potenziali declaratorie di illiceità del trattamento.

4.3.2. Il principio di minimizzazione e le architetture compatibili

Il principio di minimizzazione dei dati si trova in tensione strutturale con la logica di funzionamento dei sistemi AI. I modelli di machine learning – e a maggior ragione i modelli di tipo foundation o large language model – tendono a migliorare le proprie prestazioni predittive all'aumentare della quantità e varietà dei dati di addestramento. Questa tendenza crea un incentivo intrinseco all'espansione, non alla riduzione, dei dataset utilizzati. Il principio di minimizzazione opera invece in senso contrario: i dati devono essere “adeguati, pertinenti

49. Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio del 5 febbraio 2025 che istituisce lo Spazio europeo dei dati sanitari (EHDS), 5 marzo 2025. Il regolamento adotta un'architettura di basi giuridiche stratificata che, come evidenziato da Ponti 2025, costituisce un uso “strategico” delle basi di liceità del GDPR: l'art. 6, par. 1, lett. c) e l'art. 9, par. 2, lett. i) e j) fondano gli obblighi di condivisione imposti ai detentori di dati sanitari; l'art. 6, par. 1, lett. e) e l'art. 9, par. 2, lett. g)-j) fondano il compito di interesse pubblico degli organismi di accesso ai dati sanitari. In entrambi i casi, la designazione regolamentare risolve a monte il problema della compatibilità delle finalità, rendendo direttamente autorizzato l'uso secondario dei dati per ricerca, politiche sanitarie e innovazione.

50. Sull'“uso strategico” delle basi giuridiche del GDPR come strumento di governance della circolazione dei dati pubblici, cfr. Ponti 2025, che osserva come l'EHDS abbia costruito un sistema in cui la finalità del trattamento secondario è direttamente definita dalla norma, senza lasciare spazio a un giudizio discrezionale di compatibilità caso per caso. La stessa logica si riscontra nel modello BDIN/PDND, dove la priorità dell'interoperabilità delle basi di dati di interesse nazionale viene imposta per legge come finalità autonoma di circolazione dei dati, distinta dalle finalità originarie di raccolta.

51. Sulla necessità di un intervento legislativo specifico come presupposto per la legittimità dei sistemi AI applicati all'esercizio di funzioni pubbliche, cfr. PONTI 2025, in cui l'Autore argomenta che, in assenza di una base normativa che identifichi con sufficiente precisione le finalità, le categorie di dati e i soggetti destinatari, il trattamento fondato sul compito di interesse pubblico (art. 6, par. 1, lett. e) rimane esposto all'incertezza circa la proporzionalità e necessità dell'intervento. La logica funzionale della base di liceità e) deve essere “completata” da una cornice normativa che espliciti i tratti essenziali del trattamento.

e limitati a quanto necessario rispetto alle finalità per le quali sono trattati”. La distanza tra le due logiche – massimizzazione dei dati per ottimizzazione del modello vs. minimizzazione dei dati per tutela degli interessati – è la fonte della tensione.

Questa tensione non è ignorata dalla prassi delle autorità di controllo. L’EDPB, nell’Opinion 28/2024, ha elaborato un framework strutturato per la valutazione della minimizzazione nei sistemi AI, articolando il test di necessità in due componenti distinte⁵². La prima componente è di natura qualitativa: riguarda le categorie di dati utilizzate (quali tipologie di dati sono necessarie per la finalità dichiarata?). La seconda componente è di natura quantitativa: riguarda il volume dei dati (quanti dati sono necessari?). Con riferimento alla componente quantitativa, il Board afferma esplicitamente che il volume dei dati di addestramento deve essere valutato rispetto alla possibilità di ricorrere ad “alternative meno invasive”. Questo trasforma la valutazione di minimizzazione da accertamento binario sulla non-superfluità dei dati in un confronto sistematico con le opzioni tecnologiche alternative disponibili – un confronto che deve essere documentato e giustificato dal titolare del trattamento.

Un presupposto essenziale perché questa valutazione possa essere condotta è che la finalità del trattamento sia chiaramente e specificamente

identificata fin dalla fase di sviluppo del modello. L’EDPB precisa al par. 64 dell’Opinion 28/2024 che anche nella fase di addestramento – quando ancora il sistema non è stato applicato ad uno specifico compito – la finalità deve essere “clearly and specifically identified”⁵³. Questo requisito ha conseguenze concrete per i sistemi AI anticorruzione: la generica indicazione “prevenzione della corruzione” come finalità è insufficiente. Occorre invece identificare con precisione la funzione specifica perseguita – rilevazione di anomalie nei contratti pubblici; profilazione del rischio di conflitto di interessi nei procedimenti autorizzativi; identificazione di pattern di collusione nelle gare d’appalto; detection di operazioni sospette di riciclaggio in transazioni pubbliche – perché ciascuna funzione richiede categorie e volumi di dati diversi, e la valutazione di minimizzazione deve essere condotta separatamente per ciascuna di esse.

Una specificità particolarmente rilevante riguarda la questione dell’anonimizzazione dei modelli addestrati. L’intuizione comune secondo cui un modello AI – in quanto aggregazione di parametri matematici – non “contiene” dati personali è smentita dall’Opinion 28/2024. Il Board chiarisce ai parr. 41-42 che i modelli AI non devono essere considerati automaticamente anonimi per il solo fatto che da essi non è possibile estrarre direttamente record personali⁵⁴. La condizione

52. EDPB 2024. Il test di necessità è articolato in due componenti distinte: (i) la necessità tipologica, relativa alle categorie di dati utilizzate (quali dati sono necessari per la finalità?); (ii) la necessità volumetrica, relativa alla quantità di dati (quanti dati sono necessari?). Con riferimento alla seconda componente, il Board afferma esplicitamente che “the volume of data used for training should be assessed against the possibility of using less intrusive alternatives”, configurando così la valutazione di minimizzazione come un confronto sistematico con tecniche alternative meno invasive, e non come mero accertamento della non-superfluità dei dati.

53. EDPB 2024: “the purpose of the processing [during development] must be clearly and specifically identified”. Il Board chiarisce che la finalità dello sviluppo di un modello AI non può essere descritta in termini generici (es. “sistema anticorruzione”): deve essere articolata con sufficiente precisione da consentire la valutazione della necessità dei dati. Nella pratica, ciò significa che sistemi destinati alla rilevazione di frodi negli appalti pubblici, alla profilazione del rischio di conflitto di interessi, al riconoscimento di pattern di corruzione nei procedimenti amministrativi, richiedono ciascuno una distinta valutazione della minimizzazione, con dataset potenzialmente diversi per natura e volume.

54. Cfr. EDPB 2024. Il Board esclude che i modelli AI debbano essere considerati automaticamente anonimi per il solo fatto che da essi non è possibile estrarre direttamente dati personali individuali. Le due condizioni cumulative che devono essere entrambe soddisfatte sono: (i) che l’estrazione di dati personali dal modello sia impossibile; (ii) che da nessun output del modello, anche attraverso attacchi di tipo inversione o di membership inference, sia possibile ricavare dati personali. Se anche una sola di tali condizioni non è verificata, il modello addestrato rimane assoggettato al GDPR come trattamento di dati personali. La conseguenza pratica è significativa: l’obbligo di minimizzazione non si esaurisce con la fase di training, ma si estende al modello addestrato come tale.

di anonimità è soddisfatta solo se (i) l'estrazione di dati personali dal modello è impossibile e (ii) nessun output del modello – inclusi quelli ottenibili mediante attacchi di inversione (*inversion attacks*) o di membership inference – consente di ricavare informazioni personali identificative. Finché entrambe le condizioni non sono verificate, il modello addestrato rimane assoggettato al GDPR come trattamento di dati personali, con tutte le conseguenti obbligazioni. Ciò significa che l'obbligo di minimizzazione non si esaurisce con la fase di raccolta e addestramento, ma si estende al modello stesso come prodotto del trattamento: un modello “denso” di dati personali incorporati in forma trasformata è, a tutti gli effetti, un trattamento in corso finché rimane in uso.

La valutazione del volume dei dati in rapporto alle alternative meno invasive – imposta dall'EDPB come elemento del test di minimizzazione – richiede che il titolare del trattamento consideri concretamente le principali tecniche di privacy by design applicabili allo sviluppo AI⁵⁵. Il federated learning consente di addestrare il modello localmente sui dati di ciascun titolare, scambiando solo parametri aggregati del modello e non i dati grezzi: in un sistema anticorruzione distribuito su più amministrazioni, questa architettura ridurrebbe significativamente il rischio di centralizzazione di grandi volumi di dati personali. La *differential privacy* aggiunge rumore statistico calibrato ai dati o ai parametri, rendendo statisticamente impossibile l'inferenza di informazioni individuali pur

preservando le proprietà aggregate. I dati sintetici, generati algoritmicamente in modo da replicare le proprietà distributive dei dati reali senza contenere dati personali effettivi, possono in alcuni casi sostituire i dati reali nelle prime fasi di sviluppo o per il testing del modello. Il titolare del trattamento deve documentare per quale ragione queste alternative non sono state adottate, o non sono adottabili nella misura necessaria, per ogni componente del dataset.

Sulla base dell'analisi appena svolta – i.e., quali condizioni operative la legalità vigente in materia di tutela dei dati personali sembra imporre allo sviluppo e all'impiego di sistemi AI per la prevenzione della corruzione – emerge un quadro di requisiti di praticabilità stringenti ma anche definiti. La finalità dell'AI anticorruzione deve essere articolata in termini specifici, funzione per funzione, prima dell'avvio della raccolta dei dati di addestramento. Deve essere condotta – e documentata nella valutazione d'impatto (DPIA) prevista dall'art. 35 del GDPR – un'analisi delle alternative *tecnologiche* (cioè, *diverse* dell'AI) che, a parità di efficacia, risultino meno invasive⁵⁶. Il volume dei dati di addestramento deve essere limitato al minimo statisticamente dimostrato come necessario per le prestazioni richieste, con monitoraggio continuo al procedere dell'addestramento per verificare se la stessa performance possa essere raggiunta con dataset più ridotti. Le scelte architetturali del sistema – federated learning, differential privacy, dati sintetici – devono essere considerate come opzioni primarie e documentate come insufficienti prima

55. Le principali tecniche di privacy by design rilevanti per lo sviluppo di sistemi AI sono: (a) il federated learning, in cui il modello è addestrato localmente su dati distribuiti presso ciascun titolare senza che i dati stessi vengano centralizzati; vengono condivisi solo i parametri del modello (c.d. gradient updates), che possono comunque presentare rischi di re-identificazione ma in misura drasticamente ridotta rispetto alla centralizzazione dei dati grezzi; (b) la differential privacy, che consiste nell'aggiunta di rumore statistico calibrato ai dati o ai parametri del modello in modo da rendere statisticamente impossibile l'inferenza di informazioni individuali, pur preservando le proprietà aggregate; (c) i dati sintetici, ossia dataset generati artificialmente che preservano le proprietà statistiche e distributive dei dati reali senza contenere dati personali effettivi. Su questi approcci nel contesto AI cfr. EDPB 2024; WP29 2014.

56. L'art. 35 del GDPR impone al titolare del trattamento di effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) quando il trattamento “può presentare un rischio elevato per i diritti e le libertà delle persone fisiche”, e in particolare nei casi di “trattamento sistematico su larga scala di categorie particolari di dati” e di “trattamento che implica la valutazione sistematica e globale di aspetti personali relativi a persone fisiche”. Lo sviluppo e l'impiego di sistemi AI per la profilazione del rischio corruttivo ricade in almeno due delle ipotesi elencate nell'art. 35, par. 3, e nei criteri enunciati nella guida EDPB: cfr. EDPB 2024. La DPIA è pertanto obbligatoria e deve includere la documentazione dell'intera valutazione di minimizzazione, compreso il confronto con le alternative tecnologiche meno invasive.

di procedere alla centralizzazione di dati personali reali. L'anonimizzazione del modello addestrato deve essere verificata empiricamente, non presupposta. Solo un percorso di sviluppo che soddisfi queste condizioni cumulative può ritenersi conforme al principio di minimizzazione e, dunque, al quadro complessivo del GDPR.

Tenendo insieme le acquisizioni dei due sottoparagrafi che precedono, emerge una indicazione di fondo per la governance pubblica dei dati nell'ambito dell'anticorruzione. I profili di tensione con il GDPR non sono risolvibili dalla sola virtù tecnica dei sistemi AI, né dalla sola buona prassi amministrativa dei titolari del trattamento: sembrano richiedere entrambi – quello relativo alla limitazione della finalità e quello relativo alla minimizzazione – una risposta normativa strutturata⁵⁷. Per il primo, la risposta è una designazione legislativa che attribuisca direttamente base giuridica all'uso dei dati per finalità AI anticorruzione, sul modello BDIN/EHDS. Per il secondo, la risposta è un quadro di obblighi procedurali – DPIA, valutazione comparativa delle alternative, verifica empirica dell'anonimizzazione del modello – che devono essere incorporati nella base giuridica di trattamento. In questa prospettiva, la questione della governance dei dati per l'AI anticorruzione non è separabile dalla questione di una architettura giuridica funzionale allo scopo⁵⁸.

5. La Piattaforma Digitale Nazionale dei Dati e il PNRR

La Piattaforma Digitale Nazionale dei Dati (PDND), disciplinata dall'art. 50-ter del Codice

dell'amministrazione digitale (d.lgs. 82/2005), nella formulazione risultante dalle successive modifiche, rappresenta l'infrastruttura tecnico-giuridica più rilevante per i sistemi AI anticorruzione che operano sulla sintesi di conoscenza eterogenea. La sua comprensione richiede di distinguere tra la PDND come infrastruttura tecnologica e la PDND come istituzione normativa: sono due piani distinti, e la praticabilità dei sistemi AI anticorruzione dipende dalla coerenza tra i due.

5.1. L'architettura della PDND

L'architettura della PDND costituisce la risposta al problema della "interoperabilità predicata", ossia l'interoperabilità formalmente proclamata nei testi normativi fin dall'(ormai) lontano 2005⁵⁹, ma non effettivamente praticata per l'eterogeneità degli standard tecnici adottati dalle diverse amministrazioni. Il modello della PDND è quello di un hub centralizzato che funge da intermediario tra amministrazioni "erogatrici" di dati e amministrazioni "fruitrici", attraverso un sistema di API standardizzate e di Accordi di Accessibilità che definiscono le condizioni giuridiche dello scambio. Il vantaggio è la standardizzazione tecnica e normativa; il limite è che l'architettura a hub presuppone che le amministrazioni erogatrici abbiano già digitalizzato i propri dataset in formati compatibili con le API della piattaforma, il che non è ancora vero per molte delle banche dati rilevanti per la prevenzione della corruzione.

La PDND integra, come nodi prioritari, le Basi di Dati di Interesse Nazionale (BDIN) previste dall'art. 60 CAD, tra cui: l'Anagrafe Nazionale

57. EDPB-EDPS 2021: il Board e il Supervisor evidenziano che la proposta di certificazione (CE marking) del sistema AI non è strutturata in modo da garantire la conformità al principio di minimizzazione dei dati, dal momento che "the proposed AIA does not address the relationship between the certification/conformity assessment and data protection law and the data minimisation principle in particular". Il rischio segnalato è che la conformità tecnica ai requisiti dell'AI Act possa essere percepita – erroneamente – come sostitutiva della conformità al GDPR.

58. EDPB 2018. Le Linee guida chiariscono che anche le decisioni semi-automatizzate (in cui l'output del sistema AI è sottoposto a revisione umana prima di produrre effetti giuridici) rimangono soggette alle garanzie dell'art. 22 del GDPR laddove il contributo umano sia meramente formale. Nel contesto anticorruzione, i sistemi di risk scoring che assegnano punteggi di rischio corruttivo alle singole procedure o ai singoli soggetti rientrano nella categoria della "profilazione" ai sensi dell'art. 4, n. 4, del GDPR, con tutte le conseguenti garanzie.

59. Il testo del d.lgs. 42/2005, istitutivo del Sistema pubblico di connettività (testo in seguito assorbito nel Codice dell'amministrazione digitale), prevedeva già i servizi per la "interoperabilità evoluta" (i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini); e per la "cooperazione applicativa", finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione delle informazioni e dei procedimenti amministrativi.

della Popolazione Residente (ANPR); il Registro delle Imprese; l'Anagrafe Nazionale degli Studenti; il Casellario delle prestazioni sociali; la Banca Dati dei Contratti Pubblici (BDNCP) gestita da ANAC; il Catasto (Agenzia delle Entrate); il Fascicolo del Lavoratore. Queste banche dati coprono, in modo non ancora completo ma tendenzialmente sistematico, le principali fonti informative necessarie per sistemi di cross-referencing automatico a fini di anticorruzione. Il collegamento tra queste basi di dati attraverso la PDND – che richiede la stipulazione di Accordi di Accessibilità tra le amministrazioni interessate – è la preconditione tecnico-giuridica per qualsiasi sistema AI di sintesi di conoscenza eterogenea applicato alla prevenzione della corruzione.

5.2. Potenziale e limiti per i sistemi AI anticorruzione

Il PNRR ha stanziato risorse significative per il rafforzamento della PDND e per il completamento delle infrastrutture di interoperabilità. Le risorse della Missione 1, Componente 1 sono orientate sia all'estensione della copertura delle BDIN sia al potenziamento delle API della piattaforma, sia al supporto tecnico e organizzativo alle amministrazioni erogatrici per l'adeguamento dei propri sistemi informativi. Ponti ha tuttavia avvertito, sin dall'analisi della fase di avvio del PNRR, che la digitalizzazione accelerata imposta dai ritmi di attuazione del Piano presenta tensioni rispetto alle garanzie procedurali che il diritto fondamentale alla buona amministrazione impone nei confronti dei soggetti coinvolti nei processi amministrativi⁶⁰.

Per i sistemi AI anticorruzione, la PDND offre un potenziale significativo ma ancora parzialmente

teorico. Sul versante del potenziale: la disponibilità di API standardizzate riduce il costo tecnico dell'integrazione di dataset diversi; il sistema degli Accordi di Accessibilità fornisce il quadro giuridico per disciplinare le condizioni dello scambio; la progressiva inclusione di nuove banche dati amplia la copertura informativa disponibile per l'analisi algoritmica. Sul versante dei limiti: la qualità dei dati nelle banche dati erogatrici è ancora disomogenea, con problemi di completezza, aggiornamento e standardizzazione dei formati che limitano l'affidabilità dell'analisi ML; il sistema dei Requisiti di Accessibilità non definisce in modo generalizzato le condizioni per i trattamenti finalizzati alla prevenzione della corruzione, richiedendo negoziazioni bilaterali caso per caso; la struttura pluralistica dell'amministrazione italiana, con migliaia di enti locali e centinaia di amministrazioni centrali, rende molto eterogeneo il grado di adesione effettiva alla piattaforma^{61,62}.

Sul piano normativo, il quadro dei Requisiti di Accessibilità potrebbe essere rafforzato da un intervento di rango primario o regolamentare che definisca, in modo generalizzato e vincolante, le condizioni alle quali le banche dati della PDND possono essere utilizzate per sistemi AI anticorruzione: un atto normativo che specifichi le finalità di prevenzione della corruzione come ragione sufficiente per l'accesso, i tipi di dati accessibili, le garanzie tecniche e organizzative richieste, le modalità di supervisione e audit. Questo intervento – che potrebbe collocarsi a livello di decreto ministeriale o di regolamento ANAC – scioglierebbe molte delle incertezze interpretative che oggi rendono i sistemi AI anticorruzione basati sulla sintesi di dati eterogenei giuridicamente instabili, esponendoli al

60. Il Piano Nazionale di Ripresa e Resilienza (PNRR), nella Missione 1 (Digitalizzazione, innovazione, competitività, cultura e turismo), Componente 1, ha stanziato risorse significative per il rafforzamento della PDND e per il completamento delle infrastrutture di interoperabilità. PONTI 2022 evidenzia le tensioni tra l'obiettivo di accelerazione delle riforme digitali e le garanzie procedurali imposte dal diritto fondamentale alla buona amministrazione.

61. Sul meccanismo dei "requisiti di accessibilità" come sistema che regola l'adesione (doverosa) delle amministrazioni ai servizi di fruibilità abilitati dalla PNND, cfr. PONTI 2023-B. I requisiti di accessibilità regolano le condizioni alle quali un'amministrazione "erogante" mette a disposizione di un'amministrazione "fruitrice" i propri dataset attraverso le API della PDND, definendo finalità, frequenza di accesso, standard tecnici e garanzie di sicurezza.

62. Cfr. LONGOBUCCO-FERWERDA 2025, dove gli Autori analizzano la disponibilità dei dataset di procurement nei 27 Stati membri e concludono che "Italy has one of the most comprehensive procurement databases in Europe (BDNCP), but the lack of standardized data formats and the fragmentation of access rights between ANAC and other authorities significantly limit its utility for AI-based analytics".

rischio di contestazioni *ex post* da parte del Garante per la protezione dei dati personali.

6. L'AI Act e la legge 9 luglio 2025, n. 132

Il quadro normativo relativo ai sistemi di intelligenza artificiale ha subito, negli ultimi due anni, una trasformazione radicale sia a livello europeo sia a livello nazionale. L'entrata in vigore del Regolamento (UE) 2024/1689 (AI Act) e l'adozione della legge 9 luglio 2025, n. 132 (legge italiana sull'intelligenza artificiale) hanno introdotto, rispettivamente, un sistema di classificazione dei sistemi AI per livello di rischio e un regime di accountability applicabile ai soggetti pubblici che li utilizzano. La disciplina è rilevante per i sistemi AI anticorruzione sia come fonte di requisiti che tali sistemi devono soddisfare, sia come fonte di rischi istituzionali se implementati senza adeguata consapevolezza del quadro applicabile.

6.1. I sistemi AI ad alto rischio nella pubblica amministrazione

L'AI Act classifica i sistemi AI in quattro livelli di rischio: inaccettabile (vietati); alto rischio (ammessi con requisiti stringenti); specifici rischi di trasparenza (soggetti a obblighi di informazione); rischio minimo (non regolati). I sistemi AI di rilevanza per la prevenzione della corruzione che possono ricadere nella categoria ad alto rischio sono, in particolare, quelli destinati "a essere usati dalle autorità competenti ai fini di valutazione dei rischi relativi a persone fisiche al fine di individuare il rischio di un soggetto di commettere reati o di reiterare un reato" (Allegato III, punto 8). Rientrano in questa categoria i sistemi di predictive risk scoring dei contratti pubblici quando

producono profili di rischio associati a soggetti specifici (imprenditori, funzionari), i sistemi di screening del conflitto di interessi, i sistemi di analisi delle dichiarazioni patrimoniali⁶³.

I requisiti per i sistemi ad alto rischio sono significativi: adozione di un sistema di gestione del rischio AI documentato; requisiti di qualità dei dati di addestramento e test; documentazione tecnica e obblighi di conservazione dei log; trasparenza verso gli utenti e obbligo di informativa; supervisione umana significativa; accuratezza, robustezza e cybersecurity; registrazione nel database EU. L'inadempienza espone il titolare del trattamento a sanzioni fino a 30 milioni di euro o al 6% del fatturato mondiale totale annuo, con un regime di enforcement che per le autorità pubbliche prevede la segnalazione all'autorità di vigilanza nazionale⁶⁴.

Il requisito più rilevante per il funzionamento pratico dei sistemi AI anticorruzione è quello della supervisione umana. L'art. 14 dell'AI Act richiede che i sistemi ad alto rischio siano "dotati di misure tecniche adeguate per consentire agli operatori di supervisionare in modo efficace il loro funzionamento durante il periodo in cui vengono utilizzati" e che gli operatori umani abbiano la "capacità di comprendere le caratteristiche e i limiti pertinenti del sistema AI ad alto rischio e di supervisionare il suo funzionamento in modo efficace". Questo requisito esclude il modello di automazione piena (fully automated decision-making) in cui il sistema AI produce direttamente un atto o una decisione vincolante senza revisione umana, ma non esclude il modello del sistema AI come strumento di supporto alla decisione umana (human-in-the-loop), a condizione che la supervisione umana sia genuina e non meramente formale⁶⁵.

63. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act). L'art. 6 e l'Allegato III individuano i sistemi AI ad alto rischio; il punto 8 dell'Allegato III include, tra questi, i "sistemi AI destinati ad essere usati dalle autorità competenti ai fini di valutazione dei rischi relativi a persone fisiche al fine di individuare il rischio di un soggetto di commettere reati o di reiterare un reato". Per una prima analisi, cfr. in dottrina la letteratura già vasta sul tema, sintetizzata, per i profili di rilievo per il presente studio, in RESIMIC 2025.

64. Per l'obbligo di registrazione nel database EU dell'Unione europea (art. 71 AI Act) e l'obbligo di adempimenti tecnici pre-mercato (artt. 8-15 AI Act, inclusi: gestione del rischio, qualità dei dati, tracciabilità, trasparenza, supervisione umana, accuratezza e robustezza), cfr. Regolamento (UE) 2024/1689, Capo III, Sezione 2.

65. Sul principio di supervisione umana significativa ("meaningful human oversight") come condizione di legittimità dei sistemi AI ad alto rischio nell'azione pubblica, cfr. AI Act, art. 14; GERLI 2026, dove si analizza il rischio che la supervisione umana si riduca a una "firma di approvazione formale" sul risultato algoritmico, senza reale capacità di comprensione e contestazione – fenomeno che la letteratura anglosassone denomina "automation bias".

6.2. La disciplina italiana della legge 132/2025

La legge 9 luglio 2025, n. 132 ha introdotto nell'ordinamento italiano una disciplina organica dell'intelligenza artificiale che integra il quadro europeo dell'AI Act con disposizioni specifiche per il contesto nazionale. Per i profili rilevanti in questa sede, tre aspetti meritano particolare attenzione. In primo luogo, l'istituzione della Commissione nazionale per l'intelligenza artificiale (art. 3), organo di coordinamento e indirizzo in materia di AI per le pubbliche amministrazioni, con funzioni anche di promozione di standard e linee guida per i sistemi AI nella pubblica amministrazione. In secondo luogo, le disposizioni sull'accountability dei sistemi AI nella pubblica amministrazione (artt. 7-9), che richiedono la designazione di un responsabile AI per ciascuna amministrazione e la predisposizione di un registro dei sistemi AI utilizzati, con indicazione della categoria di rischio e delle misure di governance adottate. In terzo luogo, la disciplina applicativa per i contratti pubblici (art. 13), che in attuazione dell'AI Act e del d.lgs. 36/2023 richiede agli operatori economici di dichiarare l'utilizzo di sistemi AI nella predisposizione delle offerte⁶⁶.

La legge 132/2025 non affronta tuttavia il tema più rilevante della governance per i sistemi AI anticorruzione: quello della definizione delle condizioni alle quali tali sistemi possono operare in modo sistematico, con accesso strutturato ai patrimoni informativi pubblici, in un quadro di regole chiare sulla base di liceità, sulle garanzie per i soggetti interessati e sulle modalità di supervisione. Su questi profili, la legge delega alle amministrazioni competenti la definizione delle regole operative, senza fornire criteri vincolanti uniformi. Questa lacuna – che si somma all'assenza di un atto normativo che regolamenti in modo organico il sistema di governance dei dati per la prevenzione della corruzione – costituisce un limite oggettivo che le

analisi di gap della Parte terza del presente saggio intendono identificare e analizzare.

Parte terza - Il gap da colmare: il tool ACOI come studio di caso

7. Il divario su piano generale: confronto internazionale e focus sui contratti pubblici

La ricognizione comparata svolta nella Parte prima consente di misurare, con un qualche grado di precisione, il divario tra il sistema italiano di prevenzione della corruzione e i più avanzati sistemi internazionali nel campo dell'applicazione dell'AI. Questo divario, su un piano generale, si articola in tre dimensioni distinte che meritano di essere analizzate separatamente, perché rispondono a cause diverse e richiedono rimedi diversi⁶⁷.

La prima dimensione è quella della maturità dei sistemi operativi. L'Italia dispone di sistemi ML operativi in campo fiscale (VeRa, Agenzia delle Entrate) e in campo antiriciclaggio (RADAR, UIF), che rappresentano applicazioni mature e di buon livello. Il confronto diventa sfavorevole nel campo dei contratti pubblici, dove la Spagna (IGAE), il Portogallo (Tribunal de Contas), l'Ucraina (DOZORRO/Prozorro) e il Cile (VigIA) dispongono di sistemi ML integrati nelle procedure di affidamento in tempo reale, mentre l'Italia non ha ancora un sistema equivalente operativo su scala nazionale. Il dato è significativo: la BDNCP gestita da ANAC è, per ampiezza di copertura e per ricchezza informativa, una delle banche dati sugli appalti più complete d'Europa; il mancato sfruttamento di questo patrimonio a fini di analisi ML non si spiega con carenze tecnologiche ma con carenze di governance normativa e organizzativa.

La seconda dimensione è quella della qualità e dell'accessibilità dei dati. La letteratura internazionale ha identificato nell'Italia un caso emblematico

66. Legge 9 luglio 2025, n. 132, Disposizioni in materia di intelligenza artificiale. L'art. 3 istituisce la Commissione nazionale per l'intelligenza artificiale; l'art. 13 contiene la disciplina applicativa per i contratti pubblici. Per i profili di accountability e supervisione umana nella pubblica amministrazione, cfr. artt. 7-9.

67. GERLI 2026, dove si propone una graduatoria della maturità dei sistemi AI anticorruzione negli appalti europei: Spagna (massimo livello di integrazione istituzionale), Portogallo, Ucraina, Estonia, seguiti da un gruppo di paesi con implementazioni parziali o sperimentali. L'Italia è classificata in quest'ultimo gruppo, con il riconoscimento che la BDNCP "ha un potenziale di eccellenza per l'analisi ML" ma che "mancano sia le garanzie di qualità del dato sia i modelli di governance per l'utilizzo sistematico a fini anticorruzione".

di “procurement data gap” strutturale: la ricchezza teorica della BDNCP non si traduce in idoneità pratica per l’analisi ML a causa di problemi di completezza (non tutte le stazioni appaltanti alimentano sistematicamente la banca dati), di standardizzazione (i formati dei documenti di gara non sono uniformi) e di accessibilità (l’accesso alla BDNCP per finalità di ricerca e analisi esterna è soggetto a procedure burocraticamente complesse). Analogamente, il collegamento tra BDNCP e registri societari – preconditione per il rilevamento automatico dei conflitti di interesse nel ciclo degli appalti – non avviene in modo sistematico attraverso la PDND ma richiede integrazioni ad hoc *case by case*⁶⁸.

La terza dimensione è quella dell’integrazione dei dati di beneficial ownership. Lo studio di Tello Arista, Fazekas e Volkotrub ha dimostrato che il collegamento tra dati di appalto e dati di beneficial ownership aumenta del 23-31% la capacità di rilevamento delle situazioni a rischio rispetto all’utilizzo dei soli dati di aggiudicazione. L’Italia non figura tra i sei paesi europei analizzati nel campione principale dello studio, per problemi di qualità e completezza dei dati di beneficial ownership disponibili: il Registro dei Titolari Effettivi, istituito dal d.lgs. 90/2017 in attuazione della IV Direttiva antiriciclaggio e successivamente riformato, ha avuto una storia applicativa travagliata, con significativi ritardi di implementazione e problemi di completezza delle dichiarazioni. La risoluzione di questi problemi è condizione necessaria per

l’integrazione dei dati di beneficial ownership nei sistemi ML di analisi del rischio negli appalti⁶⁹.

Una valutazione realistica del gap deve altresì considerare il sistema ARACHNE della Commissione europea, che costituisce l’unico strumento di risk scoring per gli appalti parzialmente operativo nel contesto italiano, limitatamente però ai contratti finanziati con fondi strutturali e PNRR. ARACHNE incrocia dati di appalto con informazioni su beneficiari, subappaltatori e persone fisiche associate, producendo alert su situazioni di potenziale conflitto di interesse e frode. La sua limitazione ai fondi europei, la sua architettura centralizzata a livello di Commissione e il suo accesso limitato alle stazioni appaltanti nazionali ne fanno uno strumento utile ma insufficiente rispetto alle esigenze di un sistema di monitoring nazionale sistematico⁷⁰.

8. Lo studio di caso: il progetto ACOI

Il progetto ACOI (Assessing Conflicts of Interest), condotto da un team di ricerca che includeva ricercatori dell’Università degli studi di Perugia e il centro di ricerca Transcrime – Università Cattolica del Sacro Cuore, è un caso di studio che permette di apprezzare, in termini concreti e sistematici, le condizioni giuridiche per l’implementazione di un sistema AI anticorruzione nell’ordinamento italiano. Il progetto ha verificato empiricamente la praticabilità tecnica di uno strumento di screening automatizzato del rischio di conflitto di interessi su un campione reale di dirigenti pubblici, documentando la metodologia,

68. LONGOBUCCO–FERWERDA 2025, dove gli Autori definiscono il “procurement data gap” come la distanza tra la ricchezza teorica delle banche dati disponibili e l’effettiva idoneità dei dati per l’analisi ML, tenuto conto di: completezza della copertura; struttura e standardizzazione dei formati; qualità e coerenza delle informazioni; accessibilità effettiva per soggetti esterni alle amministrazioni titolari. Per l’Italia, il gap più significativo è identificato nella mancanza di collegamento sistematico tra BDNCP e registri societari (Registro delle Imprese), che rende difficile la verifica automatica del conflitto di interessi nel ciclo degli appalti.

69. TELLO ARISTA–FAZEKAS–VOLKOTRUB 2026, dove si documenta che, nella maggior parte dei sei paesi europei analizzati (tra cui non figura l’Italia per problemi di qualità del dato sui beneficial owner), il collegamento tra contratti pubblici e dati di beneficial ownership aumenta in modo significativo la capacità di rilevamento di situazioni a rischio di conflitto di interessi rispetto all’utilizzo dei soli dati di aggiudicazione: “matching procurement with BO data reveals an additional 23-31% of high-risk awards that would have gone undetected using procurement data alone”.

70. Sul sistema ARACHNE della Commissione europea come strumento di gestione del rischio per i fondi strutturali, cfr. COMMISSIONE EUROPEA 2023. Il sistema è stato oggetto di pareri del EDPS, che ne hanno validato la compatibilità con il GDPR a condizione del rispetto di specifici standard di qualità dei dati e di trasparenza verso i beneficiari.

i risultati e i nodi giuridici aperti per il passaggio dalla sperimentazione all'operatività sistematica.

8.1. La metodologia ACOI

La metodologia ACOI si articola in due fasi sequenziali: una fase di screening automatizzato, in cui algoritmi di cross-referencing incrociano i dati dei dirigenti dell'amministrazione partner con le fonti informative disponibili; e una fase di validazione qualitativa, in cui un LLM dovrebbe elaborare i profili dei casi flaggati dallo screening automatizzato producendo una valutazione in linguaggio naturale che integra il risk score quantitativo con elementi di contesto che arricchiscono, precisano e confermano (o smentiscono) l'analisi automatizzata del conflitto d'interessi. Il modello ha sviluppato un tool sperimentale per l'esecuzione della fase di screening automatizzato, mentre il sistema basato su LLM per l'assistenza alla fase di analisi qualitativa è ancora in fase di sviluppo. Le fonti informative utilizzate nella fase automatizzata sono: l'Anagrafe Nazionale della Popolazione Residente (ANPR), per la verifica dell'identità e dei dati anagrafici del dirigente e dei familiari conviventi; il Registro delle Imprese (Camera di Commercio), per la verifica delle partecipazioni societarie e degli incarichi in organi societari; il Catasto (Agenzia delle Entrate), per la verifica della titolarità di diritti reali su immobili; Orbis (Bureau van Dijk/Moody's Analytics), per i dati sulle partecipazioni societarie internazionali (e la validazione di quelle nazionali).

La fase di screening automatizzato si articola nella ricostruzione della rete di interessi che fa capo al soggetto interessato (dalla verifica del conflitto d'interessi), compiuta mediante l'articolazione della rete familiare più prossima (dati ANPR) e dall'individuazione degli interessi imprenditoriali, societari ed economici di ciascuno dei componenti di tale rete (Registro delle imprese, Catasto, Orbis). Gli interessi così identificati sono posti a confronto con l'interesse pubblico rilevante al caso (la competenza esercitata dall'organo, le funzioni assegnate all'amministrazione di appartenenza). La classe di interessi è codificata e normalizzata in accordo al nomenclatore "NACE". Il calcolo del conflitto è

effettuato sulla base di un criterio di somiglianza: se l'interesse pubblico è identico (o affine) ad uno degli interessi che ricadono nella rete dell'interessato, il tool segnala un potenziale rischio di conflitto. Tale fase è utile a "scremare" le posizioni da sottoporre a verifica, così da concentrare la fase di analisi qualitativa solo sul sotto-insieme così selezionato⁷¹.

Il campione analizzato ha riguardato 485 dirigenti di amministrazioni locali, provinciali, regionali e statali. Di questi, 111 sono risultati collegati a imprese attraverso uno o più legami (titolarità di partecipazioni, cariche societarie, rapporti familiari con i soggetti titolari). Dallo screening automatizzato sono emersi 51 casi flaggati come potenzialmente a rischio (il 46% dei 111 collegati ad interessi economico-finanziari). Su questi 51 casi è stata avviata la validazione qualitativa; di questi, 21 hanno confermato un rischio concreto (il 41% dei flaggati). L'architettura tecnica ha garantito la pseudonimizzazione dei record individuali durante tutto il processo di analisi, secondo le indicazioni formulate in accordo con il Garante privacy.

Tale sperimentazione dimostra che la fase di screening automatizzato è idonea a indirizzare le risorse per la valutazione qualitativa ad un sottoinsieme che corrisponde a circa il 10% del campione (51 su 485), un contributo significativo in termini di efficienza ed efficacia operativa. Il futuro sviluppo dell'analisi qualitativa assistita mediante LLM potrà contribuire ad incrementare ulteriormente la capacità epistemica del sistema.

8.2. La base giuridica nella ricerca

La fase sperimentale del progetto ACOI ha adottato, come base di liceità per il trattamento dei dati personali, la combinazione tra l'art. 6(1)(e) GDPR (esecuzione di un compito di interesse pubblico, nella forma della ricerca scientifica di rilevante interesse pubblico⁷²) e il combinato disposto tra l'art. 5 e l'art. 89 del GDPR, che consente deroghe ad alcune garanzie previste dal Regolamento quando il trattamento è effettuato a fini di ricerca scientifica, accompagnate da garanzie adeguate. Il regime applicato ha previsto: la pseudonimizzazione dei record individuali fin dalla fase di raccolta

71. Per una descrizione completa dell'approccio metodologico, cfr. CALDERONI-POLICINO-PONTI-VALLE 2026, *passim*.

72. Infatti, la sperimentazione del tool ACOI è stato realizzato nel quadro di un progetto di ricerca di rilevante interesse nazionale-PRIN 2022, finanziato su fondi PNRR.

dei dati; la limitazione dell'accesso al team di ricerca; il coinvolgimento del DPO dell'Università e la stipulazione di un Data Processing Agreement con l'amministrazione partner; la distruzione dei dati identificativi alla conclusione della fase di ricerca⁷³. Inoltre, occorre considerare che, poiché il trattamento dei dati era funzionale all'esecuzione di un'attività di ricerca, la valutazione di compatibilità della finalità del trattamento rispetto a quella originaria è data per presupposta, sulla base di quanto disposto dall'art. 5 del GDPR⁷⁴.

La scelta della base di ricerca scientifica è utile per la fase sperimentale, ma il Rapporto ACOI tematizza esplicitamente il fatto che essa non è trasferibile all'operatività sistematica: un sistema istituzionale di screening del conflitto di interessi richiede, come detto, una base giuridica del tutto diversa (e ben più impegnativa).

8.3. Le condizioni abilitanti: piano normativo, giuridico e tecnico

Che la prevenzione del conflitto di interessi costituisca una finalità di interesse pubblico rilevante ai sensi dell'art. 6(1)(e) GDPR e dell'art. 2-ter del Codice privacy è già desumibile dall'assetto

normativo vigente: la legge 190/2012, il d.lgs. 39/2013 (artt. 6 e 7 sulla vigilanza ANAC in materia di inconferibilità e incompatibilità degli incarichi), e l'art. 222, co. 8-bis del Codice dei contratti pubblici fondano già compiti istituzionali di verifica che sono idonei ad attivare tale base di liceità⁷⁵. L'adozione di sistemi AI a supporto dell'esercizio di queste funzioni, tuttavia, richiede, come visto, condizioni abilitanti ulteriori che l'ordinamento non ha ancora pienamente previsto, sul piano normativo, giuridico e tecnico.

Sul piano dell'architettura normativa, occorre statuire in termini espliciti che l'esercizio di compiti funzionali alla prevenzione della corruzione integra un compito di interesse pubblico rilevante. Ciò può contribuire a modificare il contesto giuridico e istituzionale, incrementando le aspettative di un uso dei dati nella disponibilità del settore pubblico a tali fini. Inoltre, tale qualificazione agevolerebbe l'inclusione di alcune tipologie di dati personali particolari (a cominciare da quelli relativi alle cariche pubbliche e alle appartenenze politiche).

La seconda condizione è la designazione legislativa delle banche dati come fonti autorizzate per la finalità AI anticorruzione. Come evidenziato

73. CALDERONI-POLICINO-PONTI-VALLE 2026, dove si illustra la base giuridica adottata per la ricerca: art. 6(1)(e) GDPR ("esecuzione di un compito di interesse pubblico") per il trattamento dei dati anagrafici e patrimoniali; art. 89 GDPR e art. 110 del Codice privacy per il trattamento a fini di ricerca scientifica. La distinzione tra base ricerca e base a regime è espressamente tematizzata: "la presente ricerca utilizza la base di liceità della ricerca scientifica per la fase sperimentale; l'implementazione a regime richiederebbe una base giuridica diversa e più robusta, individuata nella prevenzione della corruzione come compito istituzionale delle autorità competenti".

74. Sul regime speciale per il trattamento a fini di ricerca scientifica, cfr. art. 89 GDPR e, nel diritto italiano, art. 110 d.lgs. 196/2003 (come modificato dall'art. 37 d.lgs. 101/2018) e il Codice di deontologia per il trattamento a fini di ricerca scientifica, Allegato 4 al d.lgs. 196/2003 (provvedimento Garante 5 giugno 2019, doc. web n. 9124510). Il regime speciale consente deroghe al principio di minimizzazione e al test di compatibilità della finalità, ma è vincolato ai principi di anonimizzazione o pseudonimizzazione dei dati, di limitazione dell'accesso al team di ricerca e di distruzione dei dati identificativi al termine della ricerca. Inoltre, poiché il trattamento dei dati era funzionale all'esecuzione di un'attività di ricerca, la valutazione di compatibilità della finalità del trattamento rispetto a quella originaria è data per presupposta; cfr. art. 5, par. 2, lett. b) del GDPR, ai sensi del quale "un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali".

75. La legge 6 novembre 2012, n. 190 impone a tutte le pubbliche amministrazioni di adottare misure organizzative per la prevenzione della corruzione. Il d.lgs. 8 aprile 2013, n. 39, agli artt. 6 e 7, attribuisce ad ANAC la vigilanza sul rispetto delle disposizioni in materia di inconferibilità e incompatibilità degli incarichi. L'art. 222, co. 8-bis del d.lgs. 31 marzo 2023, n. 36 (Codice dei contratti pubblici) attribuisce ad ANAC funzioni di monitoraggio con strumenti informatici avanzati sulla Banca Dati Nazionale dei Contratti Pubblici. La prevenzione del conflitto di interessi è pertanto già qualificata come finalità di interesse pubblico rilevante ai sensi dell'art. 6(1)(e) GDPR, e come tale idonea – in linea di principio – ad attivare tale base di liceità per il trattamento dei dati personali necessari alla verifica. Cfr. PONTI 2026.

nell'analisi del principio di limitazione della finalità (§4.3.1), le banche dati che ACOI utilizza – ANPR, Registro delle Imprese, Catasto, e la BDNCP per i contratti pubblici – sono state raccolte per finalità diverse da quelle dello screening AI. Il loro uso secondario richiede un positivo giudizio di compatibilità ai sensi dell'art. 6(4) GDPR, che è raggiungibile ma contestabile caso per caso. La soluzione strutturale è una designazione legislativa esplicita che qualifichi tali banche dati come fonti autorizzate per sistemi AI anticorruzione, sul modello di quanto sperimentato a livello Ue con il Regolamento EHDS. Una tale designazione costituirebbe una base giuridica autonoma che incorpora e risolve a monte il problema della compatibilità delle finalità⁷⁶.

Sul piano giuridico-infrastrutturale, l'accesso strutturato alle banche dati pubbliche attraverso la PDND – mediante Accordi di Accessibilità ai sensi dell'art. 50-ter CAD – deve essere formalizzato per il caso specifico della verifica istituzionale del

conflitto di interessi. Questa formalizzazione è tecnicamente possibile nell'ambito del quadro vigente, ma richiede che la finalità anticorruzione AI sia esplicitamente inclusa tra quelle legittimate dagli Accordi di Accessibilità, il che presuppone la designazione normativa di cui sopra⁷⁷. Un problema strutturale aggiuntivo riguarda i dati sulle partecipazioni societarie internazionali: il progetto ACOI ha risolto il punto ricorrendo ad Orbis, banca dati commerciale. Per un sistema istituzionale a regime, questa soluzione è tecnicamente e giuridicamente insostenibile – per ragioni di trasparenza metodologica, sostenibilità economica e qualità del dato –, e nessuna alternativa pienamente pubblica è attualmente disponibile a livello italiano o europeo⁷⁸.

Sul piano tecnico, la prima condizione è la conformità ai requisiti dell'AI Act per i sistemi ad alto rischio. Un sistema istituzionale di risk scoring del conflitto di interessi rientra nell'Allegato III, punto 8 del Regolamento (UE) 2024/1689, che qualifica

76. L'utilizzo delle banche dati ANPR, Registro delle Imprese e Catasto per la verifica del conflitto di interessi dei dirigenti pubblici costituisce un uso secondario rispetto alle rispettive finalità originarie di raccolta (gestione anagrafica, pubblicità legale degli atti societari, gestione tributaria della proprietà immobiliare). Tale uso secondario deve superare il test di compatibilità dell'art. 6(4) GDPR. La valutazione di compatibilità può essere positivamente condotta nell'ordinamento vigente – stante il forte legame strutturale tra la finalità anticorruzione e l'interesse pubblico sottostante alle finalità originarie – ma rimane esposta a contestazioni caso per caso. La soluzione più solida è la designazione legislativa esplicita di tali banche dati come fonti autorizzate per i sistemi AI anticorruzione, seguendo il modello delle Basi di Dati di Interesse Nazionale (BDIN) nell'ambito della PDND (art. 50-ter CAD, come modificato dall'art. 47 del d.l. 31 maggio 2021, n. 77) e il modello dello Spazio europeo dei dati sanitari (Reg. (UE) 2025/327, EHDS). Cfr. PONTI 2025.

77. L'accesso strutturato alle banche dati pubbliche attraverso la Piattaforma Digitale Nazionale dei Dati (PDND), ai sensi dell'art. 50-ter del d.lgs. 82/2005 (CAD) e del d.p.c.m. 14 ottobre 2021 recante le Linee guida sul punto, avviene mediante Accordi di Accessibilità stipulati tra il soggetto erogatore e il soggetto fruitore dei dati. La formalizzazione di tali accordi per ANAC – con accesso a ANPR, Registro delle Imprese, Catasto e BDNCP – costituisce una condizione tecnico-giuridica necessaria per l'operatività istituzionale del sistema di screening. Essa è possibile nell'ambito del quadro normativo vigente, ma richiede il completamento del percorso di onboarding sulla PDND da parte delle banche dati rilevanti e, in particolare, la designazione normativa della finalità anticorruzione come finalità legittima di accesso, che oggi non è esplicitamente contemplata per il caso dei sistemi AI.

78. L'utilizzo di Orbis (Bureau van Dijk/Moody's Analytics) come fonte per le partecipazioni societarie internazionali è stato il principale compromesso tecnico del progetto ACOI in fase sperimentale. La dipendenza da una banca dati commerciale pone tre ordini di problemi per un sistema istituzionale a regime: (i) sostenibilità economica (i costi di accesso ad Orbis sono significativi per utilizzi sistematici su larga scala); (ii) trasparenza metodologica (la qualità e la completezza dei dati non è verificabile dall'autorità pubblica); (iii) interoperabilità sovranazionale (l'assenza di un identificativo comune standardizzato per le persone giuridiche a livello europeo rende difficile il cross-referencing automatico cross-border senza affidarsi a provider commerciali). Il Business Registers Interconnection System (BRIS), istituito dalla direttiva (UE) 2017/1132 e pienamente operativo dal 2021, costituisce una parziale soluzione a livello europeo per i dati dei registri nazionali delle imprese, ma non copre le partecipazioni non registrate nei registri EU. Cfr. CALDERONI-POLICINO-PONTI-VALLE 2026.

come ad alto rischio i sistemi AI utilizzati da autorità pubbliche per la valutazione del rischio associato a persone fisiche in ambiti di ordine pubblico e prevenzione di illeciti. Ciò comporta obblighi di gestione del rischio, governance dei dati di addestramento e validazione, documentazione tecnica, registrazione degli eventi, trasparenza e – elemento cruciale – supervisione umana significativa⁷⁹. Questo ultimo requisito impone che l'alert prodotto dal sistema non possa mai essere l'atto finale che determina conseguenze per il soggetto interessato: deve essere input a una decisione umana motivata e revisionabile, con piena garanzia del contraddittorio⁸⁰.

La seconda condizione tecnica è l'architettura di pseudonimizzazione embedded nel flusso di trattamento. Il codice fiscale è la chiave di join tra le banche dati, ed è disponibile per questa funzione nell'ordinamento italiano; deve tuttavia essere pseudonimizzato immediatamente dopo il linking, con chiavi di de-pseudonimizzazione conservate separatamente e accessibili solo per i casi di rischio

confermato. Il progetto ACOI ha adottato questa architettura nella fase sperimentale: deve essere codificata come obbligatoria nella progettazione del sistema istituzionale. Analogamente, la validazione qualitativa mediante LLM deve avvenire in modalità in-house – senza trasmissione dei dati pseudonimizzati a provider terzi tramite API – per evitare le problematiche di data transfer verso responsabili del trattamento esterni (art. 28 GDPR) e per soddisfare il principio di minimizzazione quale inteso dall'EDPB nell'Opinion 28/2024⁸¹.

8.4. Un imperativo europeo non più differibile

Le condizioni normative, giuridiche e tecniche identificate, oltre che opzioni di policy discrezionalmente perseguibili, costituiscono nell'attuale scenario un tassello cruciale della strategia nazionale di prevenzione che la direttiva dell'Unione europea sulla prevenzione e il contrasto della corruzione impone a tutti gli Stati membri di adottare⁸². La

79. Il Regolamento (UE) 2024/1689 (AI Act), Allegato III, punto 8, classifica come sistemi AI ad alto rischio quelli utilizzati da autorità pubbliche “per valutare i rischi, tra cui il rischio di sicurezza o di recidiva, posti da una persona fisica, o per la valutazione della personalità e delle caratteristiche o delle condotte passate di persone fisiche o gruppi nel contesto di attività di contrasto”. Un sistema istituzionale di screening del conflitto di interessi che produce risk score su singoli dirigenti pubblici rientra nella medesima categoria. I requisiti dei sistemi ad alto rischio includono: sistema di gestione dei rischi (art. 9); governance dei dati di addestramento e validazione (art. 10); documentazione tecnica (art. 11); registrazione automatica degli eventi (art. 12); trasparenza verso i deployer (art. 13); supervisione umana significativa (art. 14); accuratezza, robustezza e cybersicurezza (art. 15). La supervisione umana significativa (art. 14) esclude che l'alert prodotto dal sistema possa essere l'atto finale che determina misure nei confronti del soggetto interessato: l'alert è input a una decisione umana motivata, con possibilità di contraddittorio.

80. Ai sensi dell'art. 22 del GDPR, le decisioni basate unicamente sul trattamento automatizzato che producono effetti giuridici o che incidono in modo analogo significativamente sulla persona fisica sono in linea di principio vietate, salvo eccezioni tassative. EDPB 2018 chiarisce che il requisito della supervisione umana deve essere “significativa” e non meramente formale: non è sufficiente che un essere umano “approvi” la decisione del sistema AI senza riesaminarla effettivamente. Il modello human-in-the-loop adottato nel progetto ACOI – in cui l'output del LLM è input alla revisione del team di ricerca, non atto finale – è conforme a questo requisito e deve essere mantenuto nel passaggio all'operatività istituzionale.

81. Sul modello di validazione qualitativa mediante LLM in-house nel progetto ACOI, cfr. CALDERONI-POLLICINO-PONTI-VALLE 2026, pp. 14-16. L'utilizzo di un LLM open-source in modalità in-house – senza trasmissione dei dati pseudonimizzati a provider terzi attraverso API – costituisce la scelta tecnica che minimizza il rischio di violazione del principio di minimizzazione (art. 5(1)(c) GDPR) e dell'obbligo di nomina del responsabile del trattamento esterno (art. 28 GDPR). Per un sistema istituzionale a regime, questa scelta deve essere resa obbligatoria dall'architettura tecnica: i dati pseudonimizzati dei dirigenti non devono mai uscire dal perimetro informatico dell'autorità titolare del trattamento. Cfr. EDPB 2024.

82. La direttiva UE sulla prevenzione e il contrasto della corruzione, accordo politico interistituzionale del 9 gennaio 2026 (in corso di adozione formale), all'art. 20 impone agli Stati membri di adottare misure nazionali di prevenzione della corruzione che includano meccanismi di verifica istituzionale affidati a organismi competenti

direttiva sembra optare per il modello della verifica istituzionale – la “trasparenza verticale”⁸³ affidata a organismi competenti dotati delle risorse necessarie – in coerenza con la giurisprudenza della Corte di giustizia (C-184/20) e anche quella della Corte costituzionale italiana (n. 20/2019) che sembrano precludere alla possibilità che la trasparenza diffusa possa rappresentare uno strumento proporzionato di (efficace) verifica del conflitto di interessi⁸⁴. Il progetto ACOI ha dimostrato empiricamente che questo modello è tecnicamente praticabile nell'ordinamento italiano. Le condizioni abilitanti identificate in questo paragrafo costituiscono l'insieme di interventi – normativi, giuridici e tecnici – senza i quali il risultato sperimentale rischia di rimanere un proof of concept non trasferibile all'operatività sistematica, con un gap che è al tempo stesso verso l'obbligo europeo e verso l'opportunità che la disponibilità tecnica della soluzione ha aperto.

9. Conclusioni: un'agenda non più rinviabile

L'analisi svolta nelle pagine precedenti permette di enunciare, in forma sintetica, le proposizioni principali che emergono dalla ricognizione comparata e dall'analisi dell'ordinamento italiano. Non sono

proposte come proposizioni meramente descrittive: sono le premesse di un'agenda normativa e organizzativa la cui urgenza è imposta sia dalle opportunità documentate dalla letteratura comparata sia dagli impegni derivanti dalla direttiva anticorruzione, impegni che occuperanno il legislatore nazionale nell'immediato futuro.

La prima proposizione è di ordine epistemologico: l'intelligenza artificiale non è uno strumento di indagine penale sulla corruzione, ma uno strumento di governance preventiva del rischio. Le sette tipologie di contributo epistemico analizzate nel presente saggio producono conoscenza preziosa e impossibile da generare altrimenti, ma nessuna di esse produce prove nel senso processuale del termine. Il valore dell'AI nell'anticorruzione è nella capacità di rilevare segnali deboli, di costruire mappe di rischio strutturali, di concentrare le risorse di controllo sui punti di maggiore vulnerabilità prima che il danno si produca. Confondere questa funzione con quella investigativa porta a errori sia giuridici sia organizzativi: all'eccesso di aspettative tecnologiche e alla delusione consequenziale; a requisiti di qualità del dato e di robustezza del sistema che si rivelano impossibili da soddisfare quando si tratti di produrre prove; e alla perdita

dotati di risorse adeguate. L'art. 20 sceglie il modello della “trasparenza verticale” – la verifica centralizzata da parte di autorità istituzionalmente competenti – in coerenza con la giurisprudenza della CGUE (sentenza C-184/20, *Vyriausioji tarnybinės etikos komisija*, del 1° agosto 2022) e con la sentenza della Corte costituzionale italiana n. 20/2019, che hanno entrambe escluso la trasparenza diffusa (pubblicazione in chiaro su Internet dei dati personali dei funzionari e dei loro familiari) come strumento proporzionato di prevenzione del conflitto di interessi. Cfr. PONTI 2026.

83. In effetti, mentre le disposizioni in materia di trasparenza “orizzontale” appaiono alquanto generiche (la direttiva inserisce tra le misure di prevenzione “un accesso adeguato ad informazioni di interesse pubblico”, art. 29, par. 3), quelle in materia di trasparenza “verticale” appaiono ben più strutturate. Tra le misure suggerite, infatti ci sono “norme sulle dichiarazioni della situazione patrimoniale e la verifica di tali dichiarazioni” (art. 29, par. 3, corsivo aggiunto); inoltre, tra i compiti degli “Organismi o unità organizzative anticorruzione”, organismi che l'art. 22 impone di istituire, figurano: “la valutazione delle dichiarazioni della situazione patrimoniale dei funzionari nazionali designati a norma del diritto nazionale” nonché “il monitoraggio della conformità alle disposizioni di legge e alle norme sui conflitti di interessi nel settore pubblico” (par. 1, lett. a) e c)).

84. Infatti, se da una parte la sentenza n. 19/2020 della Corte costituzionale italiana ha ridimensionato la praticabilità della prevenzione della corruzione amministrativa per mezzo della diffusione al pubblico di informazioni e dati personali dei funzionari pubblici, limitandola ai soli funzionari politici e ai funzionari di carriera con ruoli apicali (cfr. PONTI 2019-B) dall'altra la CGUE è giunta alla conclusione per cui una normativa che prevede la pubblicazione in rete della dichiarazione di interessi privati “in quanto, in particolare, tale pubblicazione riguardi dati nominativi, relativi al coniuge, convivente o partner nonché ai parenti o conoscenti del dichiarante che possono dar luogo a un conflitto di interessi”, non è compatibile con il quadro normativo posto a tutela dei dati personali (cfr. C-184/20, *Vyriausioji tarnybinės etikos komisija*, del 1° agosto 2022, in part. par. 116). Sul punto, cfr. PONTI 2026, nonché GERHOLD–LAUENSTEIN 2022, e JACQUES 2023.

del valore genuino degli strumenti AI, che è nella capacità preventiva, non in quella probatoria.

La seconda proposizione è di ordine comparato: il divario tra l'Italia e i sistemi più avanzati non è tecnologico ma normativo e organizzativo. La BDN-CP è una delle banche dati sugli appalti più ricche d'Europa; il codice fiscale consente cross-referencing sistematici che altri ordinamenti devono costruire ad hoc; la PDND offre l'infrastruttura per l'interoperabilità dei dataset pubblici; ANAC ha le competenze istituzionali per la funzione di verifica. Ciò che manca è l'architettura normativa di governance che renda questi strumenti utilizzabili sistematicamente a fini anticorruzione: regole chiare sulla base di liceità per il trattamento; Accordi di Accessibilità standardizzati sulla PDND per le finalità anticorruzione; garanzie procedurali per i soggetti interessati dagli alert; modelli di supervisione umana conformi all'AI Act. Il gap da colmare non richiede investimenti tecnologici di grande entità: richiede intelligenza normativa e coordinamento istituzionale.

La terza proposizione riguarda i canali della verifica del conflitto di interessi: la trasparenza diffusa come meccanismo generale di verifica è sostanzialmente preclusa dal quadro europeo-fondamentale; tale circostanza costituisce, ai fini del nostro discorso, una opportunità. La pubblicazione in chiaro su Internet dei dati patrimoniali e delle partecipazioni societarie dei funzionari pubblici e dei loro familiari, infatti, non è giudicata come proporzionata all'obiettivo di prevenzione del conflitto di interessi, secondo un approccio che è caratteristico della giurisprudenza dalla Corte di giustizia (C-184/2020), e che la Corte costituzionale italiana (n. 20/2019) sembra condividere negli esiti (anche se non nei percorsi argomentativi). La direttiva europea anticorruzione sembra

muoversi sulla medesima falsariga: il modello alternativo – la verifica istituzionale, affidata ad autorità competenti con accesso strutturato ai dati attraverso canali di trasparenza verticale, con adeguate garanzie procedurali per i soggetti interessati – non è una soluzione di ripiego ma il modello sistematicamente preferito dall'ordinamento europeo, e l'unico compatibile con il quadro dei diritti fondamentali. Il progetto ACOI ha dimostrato, in sede sperimentale, che questo modello è tecnicamente praticabile nell'ordinamento italiano. La questione ora aperta è se si vuole compiere il passaggio dalla sperimentazione all'operatività sistematica: e la risposta a questa domanda non è tecnica ma politica e normativa.

La quarta e ultima proposizione riguarda l'urgenza dell'agenda. L'art. 22 della direttiva UE anticorruzione impone agli Stati membri di istituire organismi competenti per la prevenzione dotati delle risorse umane, finanziarie e tecnologiche necessarie per adempiere effettivamente ai propri compiti⁸⁵. L'Italia ha già gli organismi (ANAC) e già le risorse informative (BDNCP, ANPR, Infocamere, catasto, banche dati tributarie, etc.). Quello che deve costruire, con urgenza, è l'architettura normativa che renda l'utilizzo di queste risorse sistematico, proporzionato e garantito: un intervento legislativo che specifichi le condizioni del trattamento dei dati per finalità anticorruzione; un sistema di Accordi di Accessibilità standardizzati sulla PDND; un quadro di garanzie procedurali per i soggetti interessati dagli alert; un modello di supervisione e audit dei sistemi AI conforme all'AI Act. Non si tratta di creare qualcosa di nuovo dal nulla: si tratta di connettere ciò che esiste in modo che funzioni nel modo in cui dovrebbe funzionare da tempo. È un'agenda non più rinviabile.

Riferimenti bibliografici

ANAC (2013), *Piano Nazionale Anticorruzione*, 2013

85. Uno dei tratti qualificanti della direttiva è rappresentato dall'esplicito vincolo agli Stati membri a che gli organismi o le unità organizzative "incaricati della prevenzione e della repressione della corruzione siano forniti personale qualificato in numero sufficiente e le risorse finanziarie, tecniche e tecnologiche necessarie per l'efficace esercizio delle funzioni connesse all'attuazione della presente direttiva" (cfr. art. 22): pertanto, nella misura in cui le applicazioni di AI si presentano come idonee ad incrementare non solo l'efficienza, ma pure l'efficacia dell'azione di prevenzione, esse (alla luce della direttiva) smettono di rappresentare una semplice opzione, ma si configurano come elemento necessario, ai fini del dispiegamento della strategia nazionale di contrasto della corruzione, e quindi non eludibile.

- APEC POLICY SUPPORT UNIT (2025), *Technologies for Preventing, Detecting, and Combating Corruption*, Issues Paper No. 15, 2025
- N. APPELMAN, R. Ó FATHAIGH, J. VAN HOBOKEN (2021), *Social Welfare, Risk Profiling and Fundamental Rights: The Case of SyRI in the Netherlands*, in “Journal of Intellectual Property, Information Technology and E-Commerce Law”, vol. 12, 2021, n. 4
- E. ASH, S. GALLETTA, T. GIOMMONI (2025), *A Machine Learning Approach to Analyze and Support Anti-corruption Policy*, in “American Economic Journal: Economic Policy”, vol. 17, 2025, n. 2
- BANCA D'ITALIA, UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA (2026), *Quaderno Statistiche – Segnalazioni di operazioni sospette (SOS)*, secondo semestre 2025, 2026
- BANCA D'ITALIA, UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA (2025), *Rapporto annuale per il 2024*, n. 17, 2025
- BBC NEWS (2018), *A digital game or a powerful weapon against boardroom crime?*, 3 settembre 2018
- F. CALDERONI, M.C. POLLICINO, B. PONTI, S. VALLE (2026), *Applicazione di un modello di screening automatico e validazione qualitativa del rischio potenziale di conflitto di interessi*, Studio condotto da Transcrime – Università Cattolica del Sacro Cuore nell'ambito del Progetto ACOI (Assessing conflicts of interest), Università Cattolica del Sacro Cuore, 2026
- COMMISSIONE EUROPEA (2023), *Nota metodologica Arachne*, versione 3.2, 2023
- CONTROLADORIA-GERAL DA UNIÃO (2022), *Alice: Desafios, resultados e perspectivas da ferramenta de auditoria contínua de compras públicas governamentais com uso de inteligência artificial*, in “Revista da CGU”, vol. 14, 2022, n. 26
- EDPB (2024), *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, 17 dicembre 2024
- EDPB (2018), *Guidelines 01/2018 on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (ex WP251rev.01)*, Version 2.0, 6 febbraio 2018
- EDPB-EDPS (2021), *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, 18 giugno 2021
- FAO (2024), *Global Forest Observations Initiative (GFOI), GFOI Forest Foresight – Predicting deforestation*, 2024
- J. GALLEGÓ, G. RIVERO, J. MARTÍNEZ (2021), *Preventing rather than punishing: An early warning model of malfeasance in public procurement*, in “International Journal of Forecasting”, vol. 37, 2021, n. 1
- M. GERHOLD, J. LAUENSTEIN (2022), *Litauens Ethikkommission als Datenschutzverletzerin: Nordische Transparenz und europarechtlicher Datenschutz*, in “Europarecht”, vol. 67, 2022, n. 6
- C. GERLI (2026), *Artificial Intelligence in Anti-Corruption. Comparative Insights from Public Procurement across the EU*, Tesi di dottorato, Università di Bologna, 2026
- GIZ (2024), *Inspector AI tackles money laundering*, 25 marzo 2024
- GLOBAL FISHING WATCH (2022), *Global analysis shows where fishing vessels' identification switched off*, 1 novembre 2022
- GOV.UK (2025), *Initial findings of our e-discovery review*, 2 febbraio 2025
- F. JACQUES (2023), *Protection des données à caractère personnel: la Cour de justice a-t-elle transformé le RGPD en un instrument d'une sensibilité extrême? Note d'observations sous CJUE (GC), 1er août 2022, C-184/20 (OT)*, in “Revue du Droit des Technologies de l'information”, vol. 91, 2023, n. 2

- E. KATONA, M. FAZEKAS (2024), *Hidden barriers to open competition: Using text mining to uncover corrupt restrictions to competition in Hungarian public procurement*, GTI Working Paper 2024:01, Government Transparency Institute, 2024
- N. KÖBIS, C. STARKE, I. RAHWAN (2022), *The promise and perils of using artificial intelligence to fight corruption*, in "Nature Machine Intelligence", vol. 4, 2022, n. 5
- A. LONGOBUCCO, J. FERWERDA (2025), *Fighting Corruption with Artificial Intelligence: Searching for Suitable Public Procurement Data in the EU*, BridgeGap Working Paper 25-01, 2025
- G. MANCINI PALAMONI (2024), *Il paradigma digitale dell'evidenza pubblica*, in "Ceridap", 2024, n. 2
- F. ODILLA (2025), *The Digitalisation of Anti-Corruption in Brazil: Scandals, Reforms, and Innovation*, Routledge, 2025
- F. ODILLA (2023), *Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology*, in "Crime, Law and Social Change", 2023
- F. ODILLA, A. MATTONI (2023), *Unveiling the layers of data activism: The organising of civic innovation to fight corruption in Brazil*, in "Big Data & Society", vol. 10, 2023
- OECD (2026), *Anti-Corruption and Integrity Outlook 2026*, OECD Publishing, 2026
- OECD (2025-A), *AI in fighting corruption and promoting public integrity*, in *Governing with Artificial Intelligence*, OECD Publishing, 2025
- OECD (2025-B), *Using digital technology to strengthen oversight of public procurement in Portugal: The use of data analytics and machine learning by the Tribunal de Contas*, OECD Publishing, 2025
- OECD (2024-A), *Strengthening Oversight of the Court of Auditors for Effective Public Procurement in Portugal: Digital Transformation and Data-Driven Risk Assessments*, OECD Publishing, 2024
- OECD (2024-B), *Generative AI for anti-corruption and integrity in government: Taking stock of promise, perils and practice*, OECD Publishing, 2024
- OECD (2019), *Analytics for Integrity: Data-Driven Approaches for Enhancing Corruption and Fraud Risk Assessments*, OECD Publishing, 2019
- OPEN CONTRACTING PARTNERSHIP (2024), *Red Flags in Public Procurement: A Guide to Using Data to Detect and Mitigate Risks*, 2024
- OPENTEXT (2018), *UK Serious Fraud Office Selects OpenText to Expedite Data Discovery and Investigations*, 10 aprile 2018
- F.S. PAOLO, D. KROODSMA, J. RAYNOR, T. HOCHBERG, P. DAVIS, J. CLEARY, L. MARSAGLIA, S. OROFINO, C. THOMAS, P. HALPIN (2024), *Satellite mapping reveals extensive industrial activity at sea*, in "Nature", vol. 625, 2024, n. 7993
- I. PARVANOV (2025), *The use of big data by anti-corruption authorities*, U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute, 2025
- B. PONTI (2026), *Verifica del conflitto di interessi e prevenzione della corruzione. Il nodo del trattamento dei dati personali*, in E. Carloni (a cura di), "Abuso di potere e pubblica amministrazione. Integrazione ed effettività dell'anticorruzione tra prevenzione e repressione", Il Mulino, 2026, in corso di pubblicazione
- B. PONTI (2025), *Trattamento dei dati personali e standard di legalità: elementi di preminenza delle esigenze di circolazione?*, in "Rivista italiana di informatica e diritto", 2025, n. 2
- B. PONTI (2023-A), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

- B. PONTI (2023-B), *Tre scenari di digitalizzazione amministrativa «complessa»: dalla interoperabilità predicata alla standardizzazione praticata*, in “Istituzioni del federalismo”, 2023, n. 3
- B. PONTI (2022), *Le diverse declinazioni della “Buona amministrazione” nel PNRR*, in “Istituzioni del federalismo”, 2022, n. 2
- B. PONTI (2019-A), *La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi*, in “Il diritto dell’informazione e dell’informatica”, 2019, n. 2
- B. PONTI (2019-B), *Il luogo adatto dove bilanciare. Il «posizionamento» del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019*, in “Istituzioni del federalismo”, 2019, n. 2
- A. RACHOVITSA, N. JOHANN (2022), *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case*, in “Human Rights Law Review”, vol. 22, 2022, n. 2
- M. RESIMIĆ (2025), *Harnessing artificial intelligence (AI) for anti-corruption. Benefits and challenges in prevention, detection and investigation*, U4 Helpdesk Answer 2025:24, U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute, 2025
- M. RUSINOV (2025), *The Use of Network Analysis for the Detection of Corruption in Public Procurement: The Bulgarian Case as a Testing Ground*, in “Public Policies.bg”, vol. 16, 2025, n. 2
- SOUTH CHINA MORNING POST (2019), *China’s corruption-busting AI system ‘Zero Trust’*, 4 febbraio 2019
- I. TELLO ARISTA, M. FAZEKAS, A. VOLKOTRUB (2026), *Using Beneficial Ownership Data for Systematic Risk Assessment in Public Procurement. The Example of 6 European Countries*, in “European Journal on Criminal Policy and Research”, 2026
- U4 ANTI-CORRUPTION RESOURCE CENTRE (2023), *Unlocking AI’s potential in anti-corruption: Hype vs. reality*, 2023
- WP29 – ARTICLE 29 DATA PROTECTION WORKING PARTY (2014), *Opinion 05/2014 on Anonymisation Techniques*, WP216, 0829/14/EN, 10 aprile 2014
- WP29 – ARTICLE 29 DATA PROTECTION WORKING PARTY (2013), *Opinion 03/2013 on purpose limitation*, WP 203, 2 aprile 2013
- WWF NETHERLANDS (2022), *Forest Foresight Prospectus*, 2022
- D. ZINNBAUER (2025), *Artificial intelligence in anti-corruption – a timely update on AI technology*, U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute, U4 Brief 2025:1, 2025



GIOVANNI COMANDÈ – CHIARA NASI

Oltre la Conformità: dalle scelte strategiche ISO e NIST 2.0 alla gestione proattiva del rischio

Il panorama digitale odierno richiede un approccio strategico alla sicurezza informatica. Questo studio presenta un modello operativo e pragmatico progettato per semplificare la complessa conformità normativa in un sistema di gestione aziendale facilmente applicabile. Il Modello si basa su un allineamento multilivello tra le misure di sicurezza operative e i due pilastri normativi internazionali: ISO/IEC 27001:2022 e NIST *Cybersecurity Framework* (CSF) 2.0. La metodologia utilizzata ha permesso di generare una mappatura innovativa che associa le misure operative ai controlli ISO e alle categorie NIST. L'utilità pratica del Modello è dimostrata come strumento di adattamento cruciale per le organizzazioni (note come "entità NIS") soggette agli obblighi della direttiva NIS2. Ciò consente l'implementazione operativa degli elementi essenziali di gestione del rischio richiesti dalla normativa. Il Modello è progettato per essere scalabile a qualsiasi quadro normativo, riducendo i costi di conformità e massimizzando l'efficacia operativa. In prospettiva, lo stesso mira ad evolversi in un sistema quantitativo di misurazione della sicurezza IT, fornendo alle organizzazioni un mezzo tangibile per dimostrare il proprio livello di sicurezza informatica.

Cybersicurezza – Conformità – Misure di sicurezza – ISO/IEC 27001:2022 – NIST CSF 2.0

Beyond Compliance: from ISO and NIST 2.0 strategic choices to proactive risk management

Today's digital landscape requires a strategic approach to cybersecurity. This study presents a model (hereinafter also "Smartlex Model"), an operational and pragmatic model designed to simplify complex regulatory compliance into an easily applicable business management system. The Model is based on a multi-level alignment between operational security measures and the two international regulatory pillars: ISO/IEC 27001:2022 and the NIST *Cybersecurity Framework* (CSF) 2.0. The methodology generates an innovative mapping that associates operational measures with ISO controls and NIST categories. The practical usefulness of the Model is demonstrated as a crucial adaptation tool for organisations (known as "NIS entities") subject to the obligations of the NIS2 Directive. This allows for the operational implementation of the essential risk management elements required by the regulation. The Model is designed to be scalable to any regulatory framework, reducing compliance costs and maximising operational effectiveness. Looking ahead, the Smartlex Model aims to evolve into a quantitative IT security measurement system, providing organizations with a tangible means of demonstrating their cybersecurity posture.

Cybersecurity – Compliance – Security Measures – ISO/IEC 27001:2022 – NIST CSF 2.0

G. Comandè è professore ordinario di Diritto privato comparato alla Scuola Superiore Sant'Anna e fondatore di Smartlex s.r.l. e di Inlesi s.r.l.

C. Nasi è esperta in regolamentazione e conformità dell'Unione europea presso Smartlex s.r.l.

This research is part of the PQ-NEXT project, funded by the European Union through the European Cybersecurity Competence Center under the Grant Agreement number 101225759

SOMMARIO: 1. Introduzione. – 2. ISO e NIST 2.0: due modelli a confronto. – 2.1. Lo standard ISO/IEC 27001. – 2.2. Il *Cybersecurity Framework (CSF) 2.0* di NIST. – 3. La classificazione delle misure di sicurezza: il metodo utilizzato. – 3.1. La mappatura multilivello delle misure di sicurezza. – 4. Gli obblighi di Cybersecurity per le organizzazioni pubbliche e private: una guida introduttiva all'applicazione del Modello. – 4.1. Gli obblighi a carico dei soggetti NIS: gli articoli 23 e 24 del Decreto NIS. – 5. Esempi di implementazione. – 6. Conclusioni e prossimi obiettivi.

1. Introduzione

L'attuale panorama digitale è caratterizzato da un'esposizione sempre più evidente a rischi per lo più di natura informatica inerenti alla divulgazione non autorizzata di dati personali e non. Di fronte a minacce in continua evoluzione¹, ogni organizzazione è chiamata, ormai, a considerare la cybersecurity non più come un'opzione, bensì come un imperativo strategico. È fondamentale, infatti, che ogni organizzazione si impegni ad adottare una gestione proattiva e strutturata della sicurezza delle informazioni in luogo di un approccio meramente reattivo. Benché auspicabile, tale finalità presenta rilevanti criticità operative: raggiungere questo obiettivo è infatti difficile senza una mappatura coerente dei processi e dei rischi, idealmente trasformabile in uno strumento pratico per la conformità legale e organizzativa.

Questo studio ha l'intento di iniziare a colmare questo gap. Esso si pone infatti l'obiettivo principale di tradurre le complesse direttive ed i

framework in materia di sicurezza in un modello operativo e facilmente applicabile da ogni realtà aziendale o pubblica, con lo scopo di soddisfarne le esigenze operative di compliance. Sebbene questo sia solo un primo piccolo passo, il potenziale di ulteriore sviluppo, sia pratico che teorico, è considerevole.

A tal fine, verrà illustrata un'opera di allineamento che associa le misure di sicurezza delle informazioni adottate quotidianamente nel contesto operativo aziendale e pubblico con due pilastri fondamentali della cybersecurity a livello internazionale:

- lo standard ISO/IEC 27001:2022, che fornisce un quadro per un Sistema di Gestione della Sicurezza delle Informazioni (ISMS) e
- il NIST *Cybersecurity Framework 2.0* (CSF)², che, invece, individua una serie di linee guida preordinate al miglioramento della gestione dei rischi di cybersicurezza in quelle che sono classificate come infrastrutture critiche³.

1. Per una panoramica delle più recenti minacce informatiche e delle relative strategie difensive, si veda OBI-AKAGHA-DAWODU et al. 2024.

2. V. National Institute of Standards and Technology (di seguito NIST), *The NIST Cybersecurity Framework (CSF) 2.0*, 2024.

3. Sul punto, si veda Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio. La direttiva si applica a undici settori considerati critici, e cioè: Energia; Trasporti; Settore bancario; Infrastrutture dei mercati finanziari; Salute; Acqua potabile; Acque reflue; Infrastrutture digitali; Enti della pubblica amministrazione; Spazio; Produzione, trasformazione e distribuzione di alimenti.

Il risultato di un simile allineamento ha permesso di strutturare un sistema che risulti, allo stesso tempo:

- conforme, in quanto aderisce allo standard ISO;
- orientato al rischio, attraverso i principi del CSF e
- pragmatico, in quanto adattato alle effettive esigenze operative dell'organizzazione.

L'integrazione di questi tre livelli – operativo, normativo (ISO) e strategico (CSF) – crea una sinergia che non solo consente di garantire la conformità, ma rafforza altresì l'intero sistema di sicurezza dell'organizzazione⁴. Ciò ancor più considerando l'introduzione – tanto per le strutture private quanto per la Pubblica Amministrazione – di recenti obblighi in materia di sicurezza delle reti e dei sistemi informativi introdotti ad opera della c.d. Direttiva NIS2 (Direttiva UE 2022/2555)⁵. L'Italia ha infatti recentemente introdotto significativi obblighi in materia di sicurezza delle reti e delle informazioni sia per gli enti privati che per la Pubblica Amministrazione ai sensi della Direttiva NIS2, recepita a livello nazionale con il decreto legislativo n. 138/2024⁶ ed ulteriormente collegata alla legge italiana n. 90 del 2024⁷ (anche nota come "Legge sulla Cybersecurity").

Introdotta nel dicembre 2022, la direttiva NIS2 ha ampliato il proprio ambito di applicazione a circa 100.000 organizzazioni, tra cui enti pubblici, infrastrutture critiche e fornitori di servizi digitali. Tra le altre cose, essa richiede la gestione dei rischi, una rigorosa segnalazione degli incidenti, la sicurezza della catena di approvvigionamento, la responsabilità dei dirigenti e sanzioni fino a 10

milioni di euro o al 2% del fatturato globale. In un simile scenario, la conformità non costituisce solo un obbligo burocratico, bensì una priorità assoluta per la protezione dell'organizzazione.

Come si avrà modo di illustrare, il lavoro presentato in questo articolo non costituisce un esercizio puramente teorico, ma mira a fornire uno strumento pratico che trasforma l'analisi concettuale in un quadro attuabile, per tradurre i requisiti di sicurezza in un sistema di protezione coerente e dimostrabile. Il principale contributo innovativo dello studio consiste, infatti, nel convertire questo allineamento in un quadro con implicazioni operative immediate, tangibili e scalabili. Progettata per adattarsi alle future architetture normative, la mappatura mira a ridurre i costi di conformità, migliorando al contempo l'efficacia delle misure implementate.

Inoltre, la metodologia sino a qui delineata pone le fondamenta per affrontare una delle sfide più complesse della cybersecurity: quella di garantire l'oggettività e la misurabilità delle azioni e dei rischi che esse sono preordinate a mitigare. Essa evidenzia l'impatto sistemico di questa mappatura sulla valutazione dei rischi e introduce un approccio più obiettivo al principio di proporzionalità, alla base della regolamentazione della sicurezza informatica. Sulla base di questi risultati, la ricerca futura si concentrerà sull'evoluzione del Modello in un sistema per la misurazione quantitativa delle prestazioni in materia di sicurezza delle informazioni.

In conclusione, verrà poi esposto un esempio pratico (tratto dal contesto giuridico italiano) dell'utilità e dei vantaggi concreti che le

4. L'integrazione tra ISO/IEC 27001:2022 e CSF è evidente, tanto che i due strumenti possono essere considerati complementari nella gestione dei rischi di cybersecurity: ciascuno dei controlli riportati nel celeberrimo standard sono infatti collocabili all'interno di una delle cinque funzioni di cui si compone – come sarà più avanti illustrato nel dettaglio – il c.d. *Core* del CSF. Tuttavia, recenti studi hanno dimostrato come, tra le cinque funzioni, la più "compatibile" con quasi tutti i controlli di cui alla normativa ISO sia quella nota come "Protect". Sul punto, si veda MALATJI 2023.

5. Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (Direttiva NIS2).

6. Decreto legislativo del 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

7. Legge 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cibersicurezza nazionale e di reati informatici.

organizzazioni possono ottenere grazie all'utilizzo della mappatura realizzata.

2. ISO e NIST 2.0: due modelli a confronto

Prima di illustrare come realizzare un sistema di misure di sicurezza conforme e frutto dell'allineamento tra "realtà" all'apparenza distanti⁸, si rende necessario approfondire e contestualizzare, seppur brevemente, i due parametri che verranno in seguito utilizzati per la classificazione: la normativa ISO/IEC 27001:2022 (di seguito, ISO) ed il NIST *Cybersecurity Framework 2.0* (di seguito, CSF o NIST 2.0). Detto approfondimento si rende quantomai opportuno considerando che la costruzione di un sistema di gestione del rischio risulta fortemente influenzata dagli standard e dalle linee su cui si basa.

2.1. Lo standard ISO/IEC 27001

La normativa ISO/IEC 27001:2022⁹ (Information security, cybersecurity and privacy protection – Information security management systems – Requirements) è uno standard europeo che, trattando di sicurezza informatica e di sistemi di gestione, individua i requisiti necessari a stabilire, implementare, mantenere e migliorare un

sistema di gestione della sicurezza delle informazioni all'interno di un'organizzazione. Si tratta di un documento fortemente incentrato sulla gestione del rischio e, ovviamente, sui relativi controlli necessari per contrastarlo, elencati nel suo Allegato A. Sebbene la versione attuale risalgia ad ottobre 2022, lo standard in esame vanta una storia ben più lunga: pubblicato per la prima volta nel 2005, è stato poi oggetto di un'ulteriore importante revisione, avvenuta nel 2013¹⁰.

Le modifiche apportate rispetto a questa versione sono tutt'altro che irrilevanti, e cioè: il nominativo dello standard ed il contenuto del relativo abstract; l'aggiunta di nuovi requisiti; la riorganizzazione dei controlli di cui all'Allegato A¹¹. Ciò che rileva maggiormente in questa sede sono, senza dubbio, le modifiche apportate nell'ambito dei controlli. Non solo, infatti, gli stessi sono stati ridotti da centoquattordici a novantatré, ma, originariamente suddivisi in quattordici sezioni¹², sono stati altresì riorganizzati (come sarà più avanti specificato) in sole quattro macro-aree. Al di là della ricollocazione, alcuni di essi sono stati rinominati e/o modificati¹³ e all'elenco preesistente ne sono stati aggiunti ben undici nuovi¹⁴. Sebbene molti di questi aggiornamenti siano principalmente

8. Il lavoro che segue ha l'obiettivo di allineare, sottolineandone le somiglianze, la normativa ISO/IEC e il CSF. Tuttavia, preme sottolineare come, al di là degli evidenti punti di contatto che saranno più avanti messi in risalto, sussistono altresì delle importanti differenze. Si pensi, ad esempio, ai costi, alla possibilità di ottenere una certificazione (nel caso di ISO) ed al grado di maturità del rischio. Sul punto, si veda ALSHAR'E 2023.

9. "ISO" è l'abbreviazione di *Organization for Standardization*, un'organizzazione internazionale indipendente e non governativa la cui missione consiste nella realizzazione di standard (come quello oggetto della presente analisi) che garantiscano coerenza ed uguaglianza in tutto il mondo. Sul punto, si veda il sito dell'organizzazione: [iso.org](https://www.iso.org).

10. Per la storia di questo e degli altri standard, si rimanda al sito dell'ISO.

11. Per un'esauritiva comparazione delle due versioni, si veda VAKHULA-KURII-OPIRSKYY-SUSUKAILO 2024.

12. Di seguito, l'elenco delle quattordici sezioni di cui alla versione del 2013 (in seguito riorganizzate, per esigenze di semplificazione, in sole quattro macro-aree): A.5 Politiche di sicurezza delle informazioni; A.6 Organizzazione della sicurezza delle informazioni; A.7 Sicurezza delle risorse umane; A.8 Gestione dei beni; A.9 Controllo degli accessi; A.10 Crittografia; A.11 Sicurezza fisica ed ambientale; A.12 Sicurezza delle operazioni; A.13 Sicurezza delle comunicazioni; A.14 Acquisizione, sviluppo e manutenzione del sistema; A.15 Relazioni con i fornitori; A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni; A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa; A.18 Conformità.

13. Per quanto concerne ciò che maggiormente rileva in questa sede, ovvero sia l'Allegato A, preme sottolineare come le modifiche apportate con la versione del 2022, lungi dal rappresentare modifiche di sostanza, sono intervenute, soprattutto, sulla forma: si pensi, ad esempio, alla ridenominazione di alcuni controlli (come il controllo A.6.2.1 Politica per i dispositivi portatili, poi modificato in A.8.1 *Endpoint* degli utenti).

14. Di seguito, gli undici controlli inseriti nella nuova versione nella normativa in esame: A.5.7 *Threat intelligence*; A.5.23 Sicurezza delle informazioni per l'utilizzo dei servizi *cloud*; A.5.30 Prontezza dell'ICT per la continuità

formali, essi hanno uno scopo importante: allineare la norma al panorama tecnologico in evoluzione e garantire la coerenza con il NIST 2.0 (per la sicurezza tecnologica) e con il GDPR (per gli obblighi di sicurezza delle informazioni) a livello europeo.

Dal punto di vista della sua architettura, la ISO 27001 risulta costruita su due pilastri principali:

- 1) le *Clausole 4-10*¹⁵, ovvero i requisiti obbligatori per istituire, attuare, mantenere e migliorare il Sistema di Gestione per la Sicurezza delle Informazioni (il come gestire la sicurezza), organizzati secondo il noto ciclo di miglioramento c.d. PDCA (Plan-Do-Check-Act);
- 2) l'*Allegato A*, da intendersi come catalogo non esclusivo di riferimento delle misure di sicurezza (i c.d. controlli) che le organizzazioni possono (e devono) adottare per mitigare i rischi eventualmente identificati.

Il collegamento tra detti pilastri è rappresentato dalla dichiarazione di applicabilità (c.d. SoA), un fondamentale documento preordinato a dimostrare la coerenza del Sistema di Gestione per la Sicurezza delle Informazioni, sia in termini di gestione dei rischi individuati che in termini di selezione dei controlli appropriati per la mitigazione di quest'ultimi.

Proprio in ragione di dette caratteristiche e, soprattutto, del suo scopo principale di fornire un sistema di organizzazione, implementazione e miglioramento delle misure di sicurezza all'interno di un'organizzazione, è innegabile il ruolo che

la normativa in esame svolge anche rispetto alla cybersecurity: quello di quadro di gestione fondamentale. Ciò ancor più considerando i frequenti rimandi effettuati dalla ISO 27001 alla cybersecurity, soprattutto nell'ambito dei controlli¹⁶.

In sintesi, nel Modello che verrà presentato, un sistema di gestione della sicurezza delle informazioni costruito in conformità con la norma ISO 27001 può essere efficacemente integrato con le funzioni di valutazione dei rischi del quadro NIST per raggiungere un obiettivo comune: garantire un elevato livello di sicurezza delle informazioni insieme a una gestione solida e adeguata dei rischi di sicurezza informatica.

2.2. Il Cybersecurity Framework (CSF) 2.0 di NIST

A prescindere dal settore o dalle dimensioni, il NIST Cybersecurity Framework (CSF) 2.0 rappresenta una risorsa essenziale per le organizzazioni che desiderano affrontare la gestione dei rischi di sicurezza informatica in modo metodico¹⁷. Si tratta, infatti, di una linea guida volontaria (pubblicata per la prima volta nel febbraio 2024) che, seppur realizzata dal *National Institute of Standards and Technology* (NIST)¹⁸ statunitense, gode di un'indiscussa reputazione anche a livello internazionale per la sua primaria utilità¹⁹: consentire alle organizzazioni di migliorare la propria "postura" di sicurezza informatica allineandosi, così, anche ad altre normative. Si pensi, ad esempio, alla Direttiva NIS2, sulla quale si tornerà in seguito.

operativa; A.7.4 Monitoraggio della sicurezza fisica; A.8.9 Gestione delle configurazioni; A.8.10 Cancellazione delle informazioni; A.8.11 Mascheramento dei dati; A.8.12 Prevenzione di *leakage* delle informazioni; A.8.16 Attività di monitoraggio; A.8.23 *Web filtering*; A.8.28 Sviluppo sicuro.

15. Di seguito l'elenco delle clausole: 4. Contesto dell'organizzazione; 5. Leadership; 6. Pianificazione; 7. Supporto; 8. Attività operative; 9. Valutazione delle prestazioni; 10. Miglioramento.
16. La cybersecurity è infatti un settore considerato dalla normativa ISO sin dal suo principio (ci si riferisce, in particolare, al suo titolo "*Information security, cybersecurity and privacy protection – Information security management systems – Requirements*"), ma non solo: si rinvengono riferimenti rilevanti anche nell'ambito dei controlli, dove sono ad esempio citati i servizi *cloud* (A.5.23), la *Threat Intelligence* (A.5.7), ecc.
17. Quello in esame non esaurisce, però, il novero dei framework in materia di cybersecurity: si pensi, ad esempio, all'Architettura Zero Trust (ZTA). Sul punto, si veda ROSE-BORCHERT-MITCHELL-CONNELLY 2020.
18. Per dettagli sul *National Institute of Standards and Technology* e sui suoi compiti, si rimanda al sito nist.gov.
19. Oltre che per la sua utilità, il CSF è noto altresì per la sua flessibilità, che ne permette non solo l'applicazione ad organizzazioni di diversa natura e dimensione, ma anche la compatibilità con standard di settore come ISO/IEC 27001:2022, altri framework (come il COBIT 5) e quadri normativi come il GDPR e il HIPAA. Sul punto, si veda LOKARE-BANKAR-MHASKE 2025.

A livello strutturale, il NIST *Cybersecurity Framework 2.0* si compone di tre elementi fondamentali:

- 1) il *Core*, che individua i risultati desiderati in ambito di cybersecurity, suddividendo gli stessi in Funzioni, Categorie e Sottocategorie;
- 2) i cc.dd. *Implementation Tiers*, ovvero quattro livelli di implementazione (*Partial, Risk Informed, Repeatable, Adaptive*) che fungono da parametri di riferimento affinché l'organizzazione valuti il suo approccio alla gestione dei rischi legati alla sicurezza informatica;
- 3) i cc.dd. *Profiles*, che permettono all'organizzazione di testare il proprio livello di allineamento tra gli obiettivi di business e i requisiti di cybersecurity e di pianificarne eventuali attività di miglioramento.

Ai fini della realizzazione del Modello, tra i tre l'elemento che preme approfondire è il primo e, in particolare, le sei funzioni pensate per offrire una panoramica dei protocolli di sicurezza delle *best practice* che lo compongono, ovvero²⁰:

- 1) Governo (*Govern*): stabilisce, comunica e monitora la strategia, le aspettative e la politica dell'organizzazione relative alla gestione del rischio di cybersecurity. In sintesi, questa funzione fornisce la direzione e le linee guida necessarie per dare priorità e realizzare gli obiettivi delle altre cinque funzioni del framework;
- 2) Identificazione (*Identify*): garantisce che i rischi attuali di cybersecurity dell'organizzazione siano pienamente compresi e individua le opportunità di miglioramento per le politiche, i piani, i processi e le procedure che supportano la gestione del rischio di cybersecurity. In tal modo, questa funzione fornisce gli spunti necessari per informare e indirizzare gli sforzi di tutte le sei funzioni del framework;
- 3) Protezione (*Protect*): attua ed utilizza misure di sicurezza per gestire attivamente i rischi di cybersecurity dell'organizzazione. L'obiettivo di questa funzione è duplice: prevenire o ridurre la probabilità e l'impatto degli eventi avversi di cybersecurity, e, contestualmente, aumentare la possibilità di cogliere opportunità positive;

- 4) Rilevamento (*Detect*): rileva ed analizza potenziali attacchi e compromissioni di cybersecurity, facilitando così le funzioni successive;
- 5) Risposta (*Respond*): contiene l'effetto degli incidenti di cybersecurity adottando adeguate risposte, minimizzando, così, il relativo danno;
- 6) Ripristino (*Recover*): recupera e ripristina gli asset colpiti da un incidente di cybersecurity.

3. La classificazione delle misure di sicurezza: il metodo utilizzato

Venendo ora al lato "pratico" del presente studio, si tratta di illustrare la metodologia per mezzo della quale si è giunti all'allineamento tra misure operative, ISO e NIST 2.0. Il risultato finale che verrà in seguito proposto è stato ottenuto in quattro fondamentali passaggi.

In una prima fase, sono state individuate una serie di misure di sicurezza delle informazioni che rispecchiassero accuratamente le pratiche organizzative tipiche sulla base dell'esperienza e che, dunque, garantissero (in combinazione tra di loro) un'adeguata protezione dei dati personali contenuti tanto su supporto digitale quanto su quello cartaceo.

Successivamente, per garantire un maggior ordine oltre che una migliore fruibilità pratica, le misure individuate sono state raggruppate in due macrocategorie – misure di sicurezza organizzative e misure di sicurezza tecniche –, seguendo la struttura del GDPR. Ciascuna categoria è stata ulteriormente suddivisa in sottocategorie (sensibilizzazione degli utenti, protezione dei locali e delle postazioni di lavoro, etc.).

Il risultato di questa prima fase di analisi è stato riassunto nella classificazione presentata in Tab. 1 e Tab. 2.

In una seconda fase, grazie all'esperienza sul campo, si è ritenuto di organizzare le misure operative in modo più corretto e rigoroso anche sul piano generale, utilizzando criteri ufficiali e riconosciuti. A tal fine, la classificazione è stata rivista sulla scorta delle indicazioni fornite da ENISA nel suo report pubblicato nel 2019, ove le misure di sicurezza risultavano distinte come in Fig. 1.

20. Per una descrizione completa delle funzioni, v. NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, cit., p. 3 ss.

a)	Misure di sicurezza organizzative
	Sensibilizzazione degli utenti
1.	Formazione del personale
2.	Istruzioni di sicurezza fisica e comportamentale dettagliate agli utenti
3.	Lucchetto con cavo di sicurezza per dispositivi mobili pc
4.	Manuale del trattamento dei dati
	Protezione dei locali e delle postazioni di lavoro
1.	Accesso non consentito al pubblico
2.	Allarme centralizzato
3.	Allarme locale
4.	Armadi ignifughi con serratura
5.	Cassetti o armadi chiusi
6.	Chiusura con serratura
7.	Controllo degli accessi
8.	Distruzione sicura dei supporti fisici
9.	Etichettatura dei dispositivi portatili
10.	Finestre con inferiate
11.	Misure antiallagamento
12.	Misure antincendio
13.	Misure antincendio automatiche
14.	Scaffalature
	Protezione delle sale server
1.	Armadi blindati
2.	Armadi ignifughi e stagni con serratura
3.	Armadi protetti
4.	Armadi senza serratura
5.	Cassaforte
6.	Controllo degli accessi
7.	Locali dotati di impianto di allarme antifurto collegato all'esterno
8.	Locali server dotati di sistema antincendio automatico
9.	Sensori ambientali nei locali server (temperatura, umidità, allagamento)
	Altre misure organizzative
1.	Accordi di riservatezza con i dipendenti ed i fornitori
2.	Adozione di un piano di continuità operativa
3.	Conservazione dei supporti comunque contenenti dati personali, in apposite custodie o contenitori
4.	Gestione e controllo delle esternalizzazioni
5.	Politiche BYOD (Bring Your Own Device)
6.	Politiche di manutenzione e di distruzione dei dati
7.	Procedure di data breach e gestione incidenti con ruoli chiari e simulazioni periodiche
8.	Procedure di on-boarding e off-boarding (es.: disattivazione account, restituzione dispositivi, etc.)
9.	Sicurezza degli scambi con altri organismi

TAB. 1 — *Classificazione iniziale delle misure di sicurezza organizzative*

b)	Misure di sicurezza tecniche
	Infrastruttura e Server
1.	Aggiornamento automatico del registro delle minacce
2.	Antivirus
3.	Backup cifrati e conservati off-site o in cloud sicuro
4.	Backup di sicurezza: continuo, settimanale, giornaliero
5.	Controllo degli accessi a livello di sistema operativo/server (RBAC)
6.	Controllo degli accessi discrezionale
7.	Controllo e filtraggio del traffico in ingresso/uscita
8.	Crittografia dei dati a riposo e in transito
9.	Disaster Recovery Plan testato periodicamente (se non già incluso nel piano di continuità operativa)
10.	Firewall di rete
11.	Gruppo di continuità o UPS
12.	Monitoraggio e logging degli accessi e delle attività
13.	NAT/PAT
14.	Protezione da malware ed exploit
15.	Ridondanza
16.	Segmentazione della rete
17.	Sistemi di rilevamento e prevenzione intrusione (IDS/IPS)
18.	Wireless sicuro
	Postazioni di lavoro (desktop e laptop)
1.	Aggiornamento automatico del registro minacce
2.	Antivirus
3.	Archiviazione sicura: livello protezione del cartaceo o tecniche di protezione dei dati tipo criptatura
4.	Autenticazione a più fattori (MFA)
5.	Autenticazione dell'accesso con password sicura
6.	Backup di sicurezza: continuo, settimanale, giornaliero
7.	Blocco della navigazione su siti non sicuri
8.	Crittografia del disco (es.: BitLocker, FileVault) su laptop e desktop
9.	Estensione dei controlli a dispositivi rimovibili connessi
10.	Firewall di rete
11.	Gestione centralizzata degli endpoint (MDM/EDR)
12.	Gruppo di continuità o UPS
13.	Politiche di timeout di sessione/inattività
14.	Predisposizione del ripristino con snapshot
15.	Profili di accesso unici
16.	Protezione da malware ed exploit
17.	Salvaschermo protetto con password sicura

TAB. 2 — Classificazione iniziale delle misure di sicurezza tecniche

Organizational Security Measures Categories	Technical Security Measures Categories
Security management	Access control and authentication
Security policy and procedures for the protection of personal data	Logging and monitoring
Roles and responsibilities	Security of data at rest
Access control policy	Server/Database security
Resource/asset management	Workstation security
Change management	Network/Communication security
Data processors	Back-ups
Incident response and business continuity	Mobile/Portable devices
Incidents handling / Personal data breaches	Application lifecycle security
Business continuity	Data deletion/disposal
Human resources	Physical security
Confidentiality of personnel	
Training	

FIG. 1 — Classificazione delle misure di sicurezza operata da ENISA (ENISA 2019, p. 14)

Il rapporto ENISA ha così fornito solide basi metodologiche per ricollocare le misure di sicurezza precedentemente individuate in categorie standardizzate. Nello specifico, il quadro ENISA 2019 classifica le misure in due ambiti generali: Organizzativo e Tecnico.

- Le *misure organizzative* comprendono azioni relative alla *governance*, quali lo sviluppo di politiche, i processi di gestione dei rischi e la formazione del personale, volte a integrare la sicurezza nella struttura organizzativa.
- Le *misure tecniche* si riferiscono alle misure di sicurezza tecnologiche, tra cui la crittografia, il controllo degli accessi e i meccanismi di sicurezza della rete, progettate per proteggere i sistemi informativi da accessi non autorizzati o compromissioni.

Adottando queste categorie, la classificazione iniziale è stata perfezionata per allinearla agli standard riconosciuti a livello internazionale, ottenendo la tassonomia aggiornata delle misure di sicurezza delle informazioni presentata in Tab. 3 e Tab. 4. Questo allineamento non solo migliora il rigore metodologico, ma anche la conformità, armonizzando le pratiche organizzative con le aspettative normative e rafforzando la gestione dei rischi attraverso una definizione più chiara delle priorità e delle responsabilità.

Sebbene coerente e accurata, tale organizzazione risultava però indubbiamente ispirata alla classificazione dei controlli così come riportata nell'Allegato A alla precedente versione dello standard ISO/IEC 27001 risalente, ormai, all'anno 2013.

Come già anticipato, infatti, nella precedente versione dello standard ISO/IEC 27001, i controlli risultavano organizzati nelle seguenti quattordici sezioni: politiche di sicurezza delle informazioni; organizzazione della sicurezza delle informazioni; sicurezza delle risorse umane; gestione degli asset; controllo degli accessi; crittografia; sicurezza fisica e ambientale; sicurezza operativa; sicurezza delle comunicazioni; acquisizione, sviluppo e manutenzione dei sistemi; rapporti con i fornitori; gestione degli incidenti di sicurezza delle informazioni; aspetti di sicurezza delle informazioni della gestione della continuità operativa; conformità. Tuttavia,

tale suddivisione non è stata riutilizzata nella nuova versione dello standard.

Pertanto, nel terzo (nonché penultimo) passaggio, si è preso atto delle “novità” introdotte in tema di controlli dall'ultima versione della normativa, risalente al 2022. Da ciò, ne è conseguita un'ulteriore rivisitazione della classificazione, necessaria affinché la stessa risultasse conforme alla suddivisione dei “nuovi” controlli così come operata nell'Allegato A dell'ultima versione dell'ISO 27001.

In occasione dell'aggiornamento della normativa, infatti, i novantatré controlli elencati sono stati suddivisi nelle seguenti quattro macrocategorie: controlli organizzativi, sul personale, fisici e tecnologici. Per tale motivo, le misure di sicurezza precedentemente identificate sono state quindi parzialmente riassegnate a queste nuove categorie, che sono state ulteriormente suddivise in sottocategorie tematiche per migliorare l'usabilità e garantire una maggiore chiarezza.

Infine, ogni misura di sicurezza è stata associata al relativo controllo corrispondente riportato nell'Allegato A alla ISO/IEC 27001:2022. I risultati ottenuti in questa fase (e, dunque, la classificazione definitiva delle misure di sicurezza dell'informazione), sono riportati nella Tab. 5.

Nella quarta ed ultima fase – considerata, da chi scrive, la più innovativa – sono stati apportati alla mappatura elaborata ulteriori perfezionamenti ottenuti grazie allo studio della *Cybersecurity Framework 2.0* di NIST.

Come già in parte menzionato, questo documento individua sei funzioni principali – Governo (GV), Identificazione (ID), Protezione (PR), Rilevazione (DE), Risposta (RS) e Recupero (RC) – preposte a garantire il massimo livello di sicurezza informatica dell'organizzazione (vedi Fig. 2). Il formato di codifica adottato è XX.YY, dove XX rappresenta la Funzione e YY la Categoria²¹. Questa integrazione garantisce la coerenza con una tassonomia riconosciuta a livello internazionale e facilita l'interoperabilità tra le pratiche organizzative e i quadri normativi²².

In sintesi, in questo ultimo passaggio, si è provveduto a collegare le categorie elaborate da NIST nella *Cybersecurity Framework 2.0* alle misure di

21. Si precisa che, ai fini del presente studio, non è stata presa in considerazione la sottocategoria. Nel CSF, infatti, ogni funzione (XX) si compone di una categoria (YY) e, altresì, di una sottocategoria (NN).

22. V. NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, cit., p. 15.

a)	Misure di sicurezza organizzative
	Gestione della sicurezza
1.	Accesso non consentito al pubblico
2.	Armadi blindati
3.	Armadi ignifughi con serratura
4.	Armadi ignifughi e stagni con serratura
5.	Armadi protetti
6.	Armadi senza serratura
7.	Cassetti o armadi chiusi
8.	Cassaforte
9.	Chiusura con serratura
10.	Conservazione dei supporti comunque contenenti dati personali, in apposite custodie o contenitori
11.	Controllo degli accessi
12.	Etichettatura dei dispositivi portatili
13.	Finestre con inferriate
14.	Gestione e controllo delle esternalizzazioni
15.	Istruzioni di sicurezza fisica e comportamentale dettagliate agli utenti
16.	Lucchetto con cavo di sicurezza per dispositivi mobili pc
17.	Manuale del trattamento dei dati
18.	Politiche BYOD (<i>Bring Your Own Device</i>)
19.	Scaffalature
20.	Sicurezza degli scambi con altri organismi
	Risposta agli incidenti e continuità operativa
1.	Adozione di un piano di continuità operativa
2.	Allarme centralizzato
3.	Allarme locale
4.	Locali dotati di impianto di allarme antifurto collegato all'esterno
5.	Locali server dotati di sistema antincendio automatico
6.	Misure antiallagamento
7.	Misure antincendio
8.	Misure antincendio automatiche
9.	Procedure di <i>data breach</i> e gestione incidenti con ruoli chiari e simulazioni periodiche
10.	Sensori ambientali nei locali server (temperatura, umidità, allagamento)
	Risorse umane
1.	Accordi di riservatezza con i dipendenti ed i fornitori
2.	Formazione del personale
3.	Procedure di <i>on-boarding</i> e <i>off-boarding</i> (es.: disattivazione account, restituzione dispositivi, etc.)

TAB. 3 — Classificazione delle misure di sicurezza organizzative basata sulle indicazioni fornite da ENISA

b)	Misure di sicurezza tecniche
	Controllo degli accessi e autenticazione
1.	Autenticazione a più fattori (MFA)
2.	Autenticazione dell'accesso con password sicura
3.	Controllo degli accessi a livello di sistema operativo/server (RBAC)
4.	Controllo degli accessi discrezionale
5.	Politiche di <i>timeout</i> di sessione/inattività
6.	Profili di accesso unici
7.	Salvaschermo protetto con password sicura
	Registrazione e monitoraggio
1.	Monitoraggio e <i>logging</i> degli accessi e delle attività
2.	Sistemi di rilevamento e prevenzione intrusione (IDS/IPS)
	Sicurezza dei dati a riposo
1.	Aggiornamento automatico del registro delle minacce
2.	Antivirus
3.	Archiviazione sicura - livello di protezione del cartaceo o tecniche di protezione dei dati tipo crittatura
4.	Crittografia dei dati a riposo e in transito
5.	Crittografia del disco (es.: <i>BitLocker</i> , <i>FileVault</i>) su laptop e desktop
6.	Protezione da <i>malware</i> ed <i>exploit</i>
	Sicurezza della rete/comunicazione
1.	Blocco della navigazione su siti non sicuri
2.	Controllo e filtraggio del traffico in ingresso/uscita
3.	<i>Firewall</i> di rete
4.	NAT/PAT
5.	Segmentazione della rete
6.	Wireless sicuro
	Backup
1.	Backup cifrati e conservati <i>off-site</i> o in <i>cloud</i> sicuro
2.	Backup di sicurezza: continuo, settimanale, giornaliero
3.	<i>Disaster Recovery Plan</i> testato periodicamente (se non già incluso nel piano di continuità operativa)
4.	Gruppo di continuità o UPS
5.	Predisposizione del ripristino con <i>snapshot</i>
6.	Ridondanza
	Dispositivi mobili/portatili
1.	Estensione dei controlli a dispositivi rimovibili connessi
2.	Gestione centralizzata degli endpoint (MDM/EDR)
	Sicurezza del ciclo di vita delle applicazioni
1.	Analisi statica e dinamica del codice (SAST/DAST)
2.	Modellazione delle minacce (Threat modeling)
3.	<i>Patch management</i> e aggiornamenti di sicurezza
4.	Test di penetrazione periodici (<i>Penetration testing</i>)
	Cancellazione/smaltimento dei dati
1.	Cancellazione sicura del software
2.	Distruzione sicura dei supporti e/o dei documenti cartacei
3.	Politiche di manutenzione, conservazione e distruzione dei dati

TAB. 4 — Classificazione delle misure di sicurezza tecniche basata sulle indicazioni fornite da ENISA

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

FIG. 2 — Le sei funzioni principali del CSF e i nomi delle categorie con i rispettivi identificatori

sicurezza delle informazioni precedentemente enucleate dalla realtà operativa ed associate ai controlli della normativa ISO. Questa integrazione ha dato vita a una struttura unificata che collega l'implementazione pratica con gli standard riconosciuti a livello internazionale, migliorando così la coerenza, la tracciabilità e la conformità normativa.

3.1. La mappatura multilivello delle misure di sicurezza

La mappatura multilivello finale ottenuta dal lavoro sopra descritto consiste, come già anticipato, nell'associazione tra la classificazione delle misure di sicurezza delle informazioni elaborata²³ da chi scrive e, da un lato, i controlli di cui alla ISO/IEC 27001:2022 (Allegato A) e, dall'altro, le categorie coniate dalla NIST 2.0 (riportate sotto forma di codici identificativi similmente alla Fig. 2). La mappatura effettuata è stata poi suffragata dalla UNI/PdR 174:2025²⁴.

23. Da qui in poi denominata “Modello Smartlex” o il “Modello, in quanto basato anche sull'esperienza pratica di Smartlex. Si veda il sito smartlex.eu.

24. Per l'associazione tra normativa ISO e NIST 2.0, si veda UNI – Ente Italiano di Normazione UNI/PdR 174:2025. *Sistema di gestione per la cybersicurezza e la sicurezza delle informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001 e al Framework NIST CSF 2.0 – Requisiti.*

Il Modello Smartlex	ISO/IEC 27001:2022 (numero controllo allegato A)	NIST 2.0
a) Misure di sicurezza organizzative		
Gestione della sicurezza		
Adozione di un piano di continuità operativa	5.24;5.29;5.30; 7.11	GV.SC;ID.IM;DE.AE; PR.IR;RS.MI;RC.RP
<i>Disaster Recovery Plan</i> testato periodicamente (se non già incluso nel piano di continuità operativa)	7.11	RC.RP;PR.IR
OMISSIS	OMISSIS	OMISSIS
<i>Threat Intelligence</i> (Intelligenza sulle Minacce)	5.7	ID.RA;GV.RM;GV.RR; GV.OV;DE;RS.CO
b) Misure di sicurezza sul personale		
Gestione delle risorse umane		
Accordi di riservatezza con i dipendenti ed i fornitori	6.6;8.30	GV.OC;GV.SC;GV.RR; ID.RA;PR.PS;PR.AA; DE.CM
Formazione del personale	6.3;7.7	GV.RR;PR.AT;PR.DS; ID.AM
OMISSIS	OMISSIS	OMISSIS
Screening e normazione dipendenti	6.1;6.2;6.3;6.4; 6.5;6.7	GV.OC;GV.RR; GV.PO;ID.AM;PR.AA;PR.AT; PR.DS;DE.CM
c) Misure di sicurezza fisiche		
Sicurezza dei locali e delle attrezzature fisiche	7.1;7.3;7.9	GV.OC;PR.AA; PR.IR;PR.DS;PR.PS; DE.CM;ID.AM
Accesso non consentito al pubblico	7.2;7.4	ID.AM;DE.AE
OMISSIS	OMISSIS	OMISSIS
Controllo degli accessi ai locali	5.17;7.2;7.4	ID.AM;DE.AE
Finestre con inferriate		
Locali dotati di impianto di allarme antifurto collegato all'esterno		
Videosorveglianza		
Protezione ambientale	7.3;7.4;7.5;7.7; 7.8; 7.9;7.12;7.13	GV.OC;GV.RM; GV.RR;ID.AM; PR.AA;PR.DS; PR.IR;PR.PS
OMISSIS	OMISSIS	OMISSIS
Gruppo di continuità o UPS	7.11	
Locali server dotati di sistema antincendio automatico		
Misure antiallagamento	7.12	
Misure antincendio	7.12	
Misure antincendio automatiche		

Sensori ambientali nei locali server
(temperatura, umidità, allagamento)

d) Misure di sicurezza tecnologiche		
Controllo degli accessi e dell'autenticazione		GV.OC;GV.RM; GV.RR;PR.AA;PR.DS; PR.PS;DE. CM;RS.MA
OMISSIS	OMISSIS	OMISSIS
Autenticazione a più fattori (MFA)	8.2;8.3;8.4;8.5	ID.RA
Autenticazione dell'accesso con password sicura	8.2;8.3;8.4	ID.RA
OMISSIS	OMISSIS	OMISSIS
Controllo degli accessi discrezionale	8.2;8.3	
OMISSIS	OMISSIS	OMISSIS
Profili di accesso unici	8.2;8.3;8.18	
OMISSIS	OMISSIS	OMISSIS
Protezione da minacce	5.1;8.1;8.2; 8.3;8.4;8.5;8.12	GV;ID;PR.AA; PR.DS;PR.PS; DE.CM
Aggiornamento automatico del registro delle minacce	8.8	ID.RA
Antivirus	8.7	RS.MI
OMISSIS	OMISSIS	OMISSIS
Test di penetrazione periodici (Penetration testing)		ID.RA
Sicurezza della rete/ comunicazione	8.98.12;8.17; 8.19; 8.20;8.21;8.24;8.27	GV.OC;GV.RM; GV.OV;ID;PR.PS; PR.DS;PR.IR;DE; RS.AN
OMISSIS	OMISSIS	OMISSIS
Controllo e filtraggio del traffico in ingresso/ uscita	8.23	
OMISSIS	OMISSIS	OMISSIS
Segregazione della rete	8.22	
Wireless sicuro	8.23;8.24	
Registrazione e monitoraggio	8.9;8.16;8.34	GV.OC;GV.OV; GV.RM;ID;PR;DE; RS.MA
Monitoraggio e logging degli accessi e delle attività	8.3;8.4;8.15	RS.AN
Sistemi di rilevamento e prevenzione intrusione (IDS/IPS)	8.3;8.4;8.8	ID.RA
Sicurezza del ciclo di vita delle applicazioni		GV.OC;GV.RM; GV.OV;PR.PS; PR.DS;ID.AM; DE.CM
Analisi statica e dinamica del codice (SAST/ DAST)	7.10;8.15;8.22; 8.25; 8.26	DE.AE;RS.AN;RS.MA;PR.IR;ID.RA
OMISSIS	OMISSIS	OMISSIS
Patch management e aggiornamenti di sicurezza	5.7;5.25;5.26	GV.SC;ID.RA; DE.AE;RS.CO;RS.MA; RS.MI;RC.RP
OMISSIS	OMISSIS	OMISSIS

Separazione degli ambienti di sviluppo, test e produzione	8.19;8.25;8.26; 8.27;8.29;8.30; 8.31	ID.RA
Crittografia	8.24;8.26	PR.DS;DE.CM;ID.RA
Crittografia dei dati a riposo e in transito		
Crittografia del disco (es.: <i>BitLocker</i> , <i>FileVault</i>) su laptop e desktop	6.7;7.9;7.13	PR.IR;PR.PS;ID.AM
Backups	8.13;8.34	PR.DS;PR.PS;RC.RP; RS.MA;DE.CM; ID.AM; ID.RA; GV.OC; GV.RM
Backup cifrati e conservati <i>off-site</i> o in <i>cloud</i> sicuro	5.20;5.23	GV.SC
Backup di sicurezza: Continuo, Settimanale, Giornaliero		
Predisposizione del ripristino con <i>snapshot</i>	5.33	PR.PS;DE.AE;RS.AN
Ridondanza	8.14	PR.PS;PR.IR
Dispositivi mobili/ portatili	5.11;6.2;6.7; 7.13;8.26	GV.OC;GV.RR; GV.RM;ID.AM;ID.RA; PR.DS;PR.IR; PR.PS;DE.CM;
OMISSIS	OMISSIS	OMISSIS
Gestione centralizzata degli endpoint (MDM/ EDR)	8.1	PR.PS
Lucchetto con cavo di sicurezza per dispositivi mobili pc	7.5;7.8;7.9	PR.IR;PR.PS
Cancellazione/smaltimento dei dati	5.11;7.10; 8.10	GV.OC; GV.RM; ID;PR.DS;PR.PS DE.CM
Cancellazione sicura del software	7.14	
OMISSIS	OMISSIS	OMISSIS
Politiche di manutenzione, conservazione e distruzione dei dati	7.13;8.14	PR.IR

TAB. 5 — Esempi di come le misure di sicurezza del Modello Smartlex possono essere associate ai controlli ISO/IEC 27001:2022 e alle categorie NIST 2.0

La Tabella 5²⁵ mostra alcuni esempi tratti dalla mappatura²⁶. Basandosi su questo quadro integrato, la sezione successiva ne illustra l'applicazione in un contesto giuridico e organizzativo concreto. Esaminando un caso tratto dal contesto normativo italiano, è dimostrabile, così, come la classificazione proposta funzioni nella pratica, evidenziandone la capacità di semplificare i processi di conformità,

ridurre la complessità di attuazione e rafforzare la responsabilità. L'esempio che segue ha lo scopo, infatti, di dimostrare l'utilità pratica del Modello e il suo potenziale di adattamento a diversi contesti organizzativi.

25. Alcune delle misure di sicurezza inserite all'interno della tabella e contenute nella categoria delle misure di sicurezza tecnologiche sono considerate come necessarie per la costituzione di un valevole "sistema immunitario digitale" in un'era, come quella in cui si scrive, caratterizzata da continue minacce di cybersecurity in evoluzione. Sul punto, si veda SHAJI GEORGE-HOVAN GEORGE-BASKAR 2023.

26. Il lavoro di mappatura completo è protetto da *copyright* di Smartlex s.r.l.

4. Gli obblighi di Cybersecurity per le organizzazioni pubbliche e private: una guida introduttiva all'applicazione del Modello

Come già anticipato, l'allineamento sopra descritto è stato precipuamente elaborato anche per fungere da Modello pratico per le organizzazioni che intendano conformarsi agli obblighi previsti a loro carico in materia di cybersicurezza²⁷. Tale esigenza è divenuta ancor più urgente in seguito all'adozione della Direttiva NIS2 (Direttiva UE 2022/2555), pietra miliare della più ampia strategia della Commissione europea in materia di sicurezza informatica²⁸. La direttiva impone requisiti rigorosi ad un'ampia gamma di soggetti in materia di attuazione delle misure di sicurezza e di notifica degli incidenti²⁹, con l'obiettivo di raggiungere un livello senza precedenti di sicurezza delle informazioni sia nel settore privato che nelle amministrazioni pubbliche.

In particolare, infatti, la direttiva si rivolge direttamente alle strutture pubbliche e private (di seguito, soggetti NIS) che operano in settori particolarmente critici come, ad esempio, il settore sanitario, quello delle infrastrutture digitali, ecc.³⁰ In Italia, tali obblighi sono stati recepiti con il decreto legislativo n. 138 del 4 settembre 2024 (di seguito, Decreto NIS)³¹, che ha introdotto requisiti di conformità significativi strettamente connessi alla mappatura precedentemente descritta. Ci si

riferisce, in particolare ed a titolo esemplificativo, a quanto stabilito negli articoli 23 e 24 del suddetto decreto: si tratta di disposizioni fondamentali che, come si avrà modo di approfondire più avanti, individuano specifici obblighi in materia di gestione del rischio per la sicurezza informatica e di notifiche degli incidenti. I suddetti requisiti legali costituiscono un banco di prova ideale per valutare l'utilità pratica del Modello proposto, in quanto richiedono non solo la conformità formale, ma anche pratiche di sicurezza dimostrabili ed efficaci.

Il recepimento italiano della direttiva NIS2 rappresenta un esempio perfetto di come il Modello qui illustrato possa fungere da strumento strategico per le organizzazioni che operano in contesti normativi complessi. Per dimostrarne la validità, è utile premettere un breve *excursus* sugli obblighi introdotti dalla legislazione italiana, concentrandosi principalmente sulla determinazione n. 164179 del 14 aprile 2025 emanata dall'Agenzia per la Cybersicurezza Nazionale (di seguito ACN). Tale provvedimento chiarisce le modalità di adempimento degli obblighi NIS2 e include quattro allegati che definiscono le specifiche di base, ovvero le misure minime di sicurezza richieste per i soggetti NIS essenziali e importanti ai sensi degli articoli 23 e 24 del Decreto NIS. Quest'ultimi descrivono inoltre in dettaglio le categorie di incidenti significativi che devono essere segnalati al CSIRT Italia in conformità con l'articolo 25.

27. Sono note, infatti, non solo le correlazioni tra NIST 2.0 e NIS2, ma anche tra quest'ultima direttiva e la normativa ISO/IEC. Ciò in quanto il recepimento della direttiva NIS2 può influire direttamente sulle politiche di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS). Sul punto (e seppur con riferimento alla Repubblica Ceca) si veda WANECKI-JASEK-DROFOVA 2023.

28. Ci si riferisce, in particolare, al *Cybersecurity Act* (Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013) ed al *Cyber Resilience Act* (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). In realtà, la Direttiva NIS2 costituisce la "naturale" evoluzione della c.d. Direttiva NIS (Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione). Per un *excursus* sulle ragioni che hanno determinato il passaggio dalla Direttiva NIS alla Direttiva NIS2, si veda CASAROSA-COMANDÈ 2025.

29. In tema di segnalazione degli incidenti (e per la comparazione sul punto tra direttiva NIS e direttiva NIS2) si veda SCHMITZ-BERNDT 2023.

30. Per l'elenco completo dei settori, si veda l'Allegato 1 alla Direttiva NIS2.

31. Per un'analisi dettagliata del decreto, si veda ACN 2025.

Il Modello illustrato integra questi requisiti nella sua struttura, garantendo alle organizzazioni la possibilità di mantenere un percorso di conformità aggiornato e mappato, che assicuri una sicurezza reale piuttosto che una mera adesione formale ai requisiti legali.

Per convalidare il quadro teorico e dimostrarne la rilevanza operativa, la sezione seguente presenta un'applicazione pratica nel contesto normativo italiano. Questo caso di studio illustra come il Modello proposto possa essere efficacemente integrato con gli obblighi nazionali in materia di sicurezza informatica, in particolare quelli introdotti dalla direttiva NIS2 e dalle sue misure di attuazione. Mappando i requisiti legali, quali i protocolli di gestione dei rischi e gli obblighi di notifica degli incidenti, sull'allineamento strutturato dei controlli ISO/IEC 27001 e delle categorie del quadro di riferimento per la sicurezza informatica del NIST, l'esempio evidenzia la capacità del Modello di trasformare la conformità da un esercizio formale a un sistema dimostrabile di governance della sicurezza. Questa illustrazione pratica funge da prova empirica dell'adattabilità e del valore strategico del Modello per le organizzazioni che operano in contesti normativi complessi.

4.1. Gli obblighi a carico dei soggetti NIS: gli articoli 23 e 24 del Decreto NIS

Prima di esaminare gli articoli 23 e 24 del Decreto NIS ed illustrare in che modo il Modello proposto sostenga le organizzazioni nell'adeguarsi agli obblighi in materia di cybersicurezza, è utile premettere che i cc.dd. soggetti NIS³² tenuti all'adempimento degli obblighi in materia di cybersicurezza sono distinti in due categorie: soggetti essenziali e soggetti importanti. La distinzione riflette principalmente la criticità dei settori in cui operano e il livello intrinseco di rischio informatico associato alle loro attività. Nonostante queste differenze, i requisiti di sicurezza imposti a entrambe le categorie convergono sostanzialmente, rendendo il Modello proposto ugualmente applicabile ad entrambe.

Stante questa premessa, è ora possibile analizzare brevemente gli articoli 23 e 24 del Decreto NIS per verificare come essi possano essere più

facilmente rispettati grazie all'ausilio della mappatura oggetto del presente lavoro.

L'articolo 23 definisce le responsabilità specifiche degli organi di amministrazione e degli organi direttivi dei soggetti essenziali e dei soggetti importanti in materia di sicurezza informatica, attribuendogli, tra l'altro, la funzione essenziale – in questa sede – di approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate dai soggetti NIS e di sovraintendere all'implementazione dei relativi obblighi. Sebbene sia previsto uno specifico obbligo formativo sul tema³³, è intuibile come gli organi di amministrazione non siano di norma composti da esperti del tema e abbisognino di strumenti agili per orientarsi e decidere. Ciò sottolinea l'importanza della mappatura proposta, non solo per i team tecnici responsabili dell'attuazione e del monitoraggio delle misure, ma anche, e forse soprattutto, per i decisori di alto livello, legalmente responsabili della governance della sicurezza.

L'articolo 24 del Decreto NIS delinea gli elementi essenziali che le organizzazioni devono necessariamente prendere in considerazione quando si trovino ad adottare misure di sicurezza informatica, rendendo così operativo il principio della gestione della sicurezza basata sul rischio. In particolare, la disposizione richiede alle entità di attuare misure proporzionate ai rischi identificati, tenendo conto di fattori quali la natura e la criticità dei servizi forniti, il potenziale impatto degli incidenti sulla continuità del servizio e il grado di esposizione alle minacce informatiche. La norma in esame sottolinea un approccio globale che integra misure di salvaguardia tecniche, organizzative e procedurali, garantendo la resilienza a tutti i livelli del sistema informativo. Inoltre, l'articolo 24 sottolinea la necessità di un monitoraggio continuo e di una rivalutazione periodica delle misure attuate, riflettendo la natura dinamica del rischio informatico. Questi requisiti sono strettamente in linea con la logica alla base del Modello proposto, che facilita la mappatura sistematica degli obblighi e supporta le organizzazioni nel dimostrare la conformità attraverso processi strutturati e verificabili.

In sintesi, l'articolo 24 identifica con precisione gli elementi essenziali che devono essere presi

32. Per l'elenco dei soggetti NIS, v. art. 6 del Decreto NIS.

33. V. art. 20, comma 2, NIS2 e 23 del Decreto NIS.

- a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete
- b) Gestione degli incidenti
- c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e la gestione delle crisi
- d) Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi
- e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità
- f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica
- g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica
- h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura
- i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset
- l) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno

TAB. 6 — *Elenco degli elementi essenziali che devono essere presi in considerazione ai sensi dell'art. 24 del Decreto NIS al momento dell'adozione delle misure di sicurezza*

in considerazione al momento dell'adozione delle misure di sicurezza, come indicati nella Tab. 6.

L'opera di allineamento effettuata da chi scrive ha permesso di associare una o più misure di sicurezza, derivate da pratiche organizzative reali, a ciascun requisito stabilito dall'articolo 24. Attraverso questo Modello, tali misure sono state sistematicamente collegate ai corrispondenti controlli ISO/IEC 27001 e alle linee guida del NIST *Cybersecurity Framework 2.0*, garantendo un'integrazione coerente e funzionale. Questo approccio strutturato non solo facilita la conformità, ma fornisce anche alle organizzazioni uno strumento pratico per mappare gli obblighi legali agli standard riconosciuti a livello internazionale, migliorando così sia l'efficienza operativa che la responsabilità. Nella Tab. 7 si riportano alcuni esempi³⁴.

Prima di proseguire con l'illustrazione del risultato finale del presente lavoro, si ritiene opportuno soffermarsi su alcuni degli esempi, così da comprendere al meglio il vantaggio della mappatura.

(a) *Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete*

Quest'obbligo è soddisfatto garantendo che la sicurezza non sia lasciata al caso, ma sia strutturata e basata su dati. Le politiche di sicurezza delle informazioni e il Manuale del trattamento dei dati

costituiscono, in tal caso, il pilastro della governance, nella misura in cui stabiliscono ruoli, obiettivi e regole di base. L'inclusione della *Threat Intelligence* assicura poi che il processo di analisi dei rischi non sia teorico, ma alimentato da informazioni aggiornate sulle minacce. Infine, l'implementazione di procedure di *data breach* dimostra che l'organizzazione ha definito la sua reazione in caso di materializzazione del rischio in piena conformità con la legislazione applicabile mappata all'interno del Modello. Sebbene il Modello non richieda alle organizzazioni di ottenere la certificazione ISO/IEC 27001, esso adotta una struttura di responsabilità comparabile per fornire prove verificabili della conformità legale.

Questo approccio strutturato migliora la governance e la preparazione agli audit, creando un sistema trasparente e tracciabile che collega ogni misura di sicurezza ai requisiti normativi e agli standard riconosciuti, consentendo così alle organizzazioni di dimostrare proporzionalità e *due diligence* nella loro postura in materia di sicurezza informatica. In questo modo, il Modello rende operativo il principio di proporzionalità incorporato nelle normative sulla sicurezza informatica: le misure non vengono applicate in modo uniforme, ma calibrate in base al livello di rischio, alla complessità organizzativa e alla criticità specifica del settore. Ciò garantisce che la conformità

34. Per un'esauritiva illustrazione della corrispondenza tra misure di sicurezza di base e gli elementi di cui all'art. 24, comma 2, del Decreto NIS, si veda ACN 2025, cit., p. 13. Il lavoro di mappatura completo è protetto da *copyright* di Smartlex s.r.l.

Decreto NIS, art. 24	Misure di sicurezza (Modello Smartlex)
a) Politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete	Procedure di data breach e gestione incidenti con ruoli chiari e simulazioni periodiche; Politiche di sicurezza delle informazioni; Manuale del trattamento dei dati; Threat Intelligence
b) Gestione degli incidenti	Procedure di data breach e gestione degli incidenti con ruoli chiari e simulazioni periodiche; Relazione con autorità e gruppi specialistici
c) Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e la gestione delle crisi	Adozione di un piano di continuità operativa; Disaster Recovery Plan testato periodicamente; Backup; Ridondanza
d) Sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi	Gestione e controllo delle esternalizzazioni; Sicurezza delle informazioni per l'uso dei servizi cloud; Accordi di riservatezza con i dipendenti ed i fornitori
e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità	Patch management e aggiornamenti di sicurezza; Analisi statica e dinamica del codice (SAST/DAST); Aggiornamento automatico del registro delle minacce; Segregazione della rete
f) Politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica	Politiche di sicurezza delle informazioni; Adozione di un piano di continuità operativa; Gestione e controllo delle esternalizzazioni; Procedure di data breach e gestione incidenti con ruoli chiari e simulazioni periodiche
g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica	Formazione del personale; Salvataggio protetto con password sicura; Screening e normazione dipendenti; Politiche BYOD (Bring Your Own Device); Procedure di on-boarding e off-boarding (es.: disattivazione account, restituzione dispositivi, etc.)
h) Politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura	Crittografia dei dati a riposo e in transito; Crittografia del disco (es.: BitLocker, FileVault) su laptop e desktop
i) Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset	Screening e normazione dei dipendenti; Procedure di on-boarding e off-boarding; Accordi di riservatezza con i dipendenti ed i fornitori; Controllo degli accessi a livello di sistema operativo/server (RBAC); Controllo degli accessi ai locali; Accesso non consentito al pubblico; Formazione del personale; Videosorveglianza
l) Uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno	Autenticazione a più fattori (MFA); Profili di accesso unici; Controllo degli accessi discrezionale; Autenticazione dell'accesso con password sicura

TAB. 7 — Esempi di come le misure di sicurezza del Modello Smartlex si rapportano ai requisiti di cui all'art. 24 del Decreto NIS

non sia meramente formale, ma sostanzialmente allineata alla natura dinamica delle minacce informatiche e alle aspettative legali di una gestione della sicurezza basata sul rischio.

(c) *Continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e la gestione delle crisi*

L'obiettivo principale di quest'obbligo è, senza dubbio, quello di garantire la resilienza dei sistemi e dei

servizi critici. L'adozione di un piano di continuità operativa e di un *Disaster Recovery Plan*, fornisce la struttura documentale per il ripristino dei servizi critici. Un requisito fondamentale per la conformità è il test periodico del *Disaster Recovery Plan*, fondamentale per convalidarne l'efficacia e l'affidabilità. A integrazione di questi piani, le misure di backup e ridondanza costituiscono la base tecnica per la continuità: i backup consentono il recupero dei dati,

mentre la ridondanza garantisce la disponibilità immediata dei sistemi critici. Insieme, queste misure rispondono in modo completo al mandato normativo in materia di continuità e ripristino dei servizi, traducendo i requisiti legali in resilienza operativa.

(e) Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità

Si tratta del requisito della *Security by Design/Default*. Il *Patch management* e gli aggiornamenti di sicurezza costituiscono la base della manutenzione sicura. L'analisi statica e dinamica del codice è invece essenziale per la sicurezza nello sviluppo e nell'acquisizione, in quanto garantisce che le applicazioni non introducano vulnerabilità sin dall'origine. L'aggiornamento automatico del registro delle minacce alimenta la gestione delle vulnerabilità. Infine, la segregazione della rete è una misura di protezione fisica e logica che garantisce che un'eventuale compromissione in un'area non si propaghi a sistemi critici. È fondamentale collegare queste misure al principio di proporzionalità e all'approccio basato sul rischio: la portata e la complessità delle strategie di continuità e di ripristino devono corrispondere al livello di rischio e alla criticità dei servizi forniti. Ciò consente un'allocazione efficiente delle risorse, evitando sia una protezione insufficiente che un investimento eccessivo e non necessario.

Il Modello proposto integra questi obblighi associando ogni requisito a specifici controlli ISO/IEC 27001 e a categorie del NIST *Cybersecurity Framework*, creando un percorso di conformità strutturato e verificabile. Questo allineamento consente alle organizzazioni di dimostrare che le misure di continuità e ripristino non siano solo implementate, ma anche proporzionate alla loro esposizione al rischio, soddisfacendo così sia gli obblighi giuridici che le aspettative di *governance*. In questo modo, il Modello trasforma principi normativi astratti in pratiche attuabili e basate su prove concrete che migliorano la resilienza e la preparazione agli *audit* e la accountability.

(g) Pratiche di igiene di base e di formazione in materia di sicurezza informatica

Quest'obbligo si concentra non solo sulla *Cyber Hygiene* ma anche sulla gestione del fattore umano, che può, senza dubbio, rappresentare l'anello più vulnerabile della catena di sicurezza. Per questo, il cuore dell'adempimento è rappresentato dalla formazione del personale (accompagnata dall'ulteriore misura di screening e normazione dei dipendenti), necessaria per elevare la cultura della sicurezza. Le altre misure costituiscono esempi pratici di "igiene di base": ad esempio, il salvaschermo protetto è un controllo di accesso fisico di primo livello; le politiche BYOD e le procedure di *on-boarding* e *off-boarding* garantiscono invece che la gestione sicura del dispositivo e degli accessi degli utenti sia standardizzata, applicando così l'igiene in ogni fase del rapporto lavorativo. Collettivamente, queste misure rendono operativi i principi di sicurezza incorporando meccanismi di igiene e di controllo in ogni fase dell'interazione organizzativa, riducendo così l'esposizione alle vulnerabilità connesse al fattore umano³⁵.

Queste misure sono direttamente mappate sui controlli ISO/IEC 27001, come A.6.3 (Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni) e A.5.17 (Informazioni di autenticazione), e sulle categorie del quadro di riferimento per la sicurezza informatica del NIST 2.0, tra cui PR.AT (Sensibilizzazione e formazione) e PR.AC (Controllo degli accessi). Questo doppio allineamento garantisce che gli obblighi relativi al fattore umano non siano trattati come pratiche isolate, ma integrati in un quadro di conformità strutturato. Il Modello proposto facilita questa integrazione fornendo una chiara mappatura tra requisiti normativi, misure operative e standard internazionali, consentendo così alle organizzazioni di dimostrare proporzionalità e responsabilità nel loro approccio alla gestione dei rischi legati al fattore umano.

35. Sul punto, si veda ENISA 2025. In questo report, l'ENISA ha condotto un'analisi dettagliata delle minacce informatiche che hanno colpito l'Unione europea tra luglio 2024 e giugno 2025. Tra le principali minacce figura il *phishing*, strettamente legato al fattore umano e responsabile del 60% degli attacchi iniziali. Altre minacce significative includono lo sfruttamento delle vulnerabilità (21,3% degli attacchi), seguito dai *botnets* (9,9%), dalle applicazioni dannose (8%) e dai rischi interni (0,8%).

(i) *Sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset*
Si tratta dell'obbligo più complesso in quanto impone una gestione olistica che non si focalizza solo sulla tecnologia, ma integra persone, processi e asset fisici. La sua natura multidimensionale sottolinea l'utilità della mappatura proposta, che consente un controllo strutturato in tutti i domini e garantisce la coerenza nell'implementazione.

- *Rischio derivante dal fattore umano*: misure quali accordi di riservatezza, screening e normazione dei dipendenti e procedure di *on-boarding* e *off-boarding* garantiscono una gestione coerente e documentata del rischio lungo tutta la durata del rapporto di lavoro.
- *A livello tecnologico*: il controllo degli accessi a livello di sistema operativo/server e la formazione del personale sono necessarie per definire un sistema di permessi robusto, che garantisca che gli utenti siano dotati solamente dell'accesso strettamente necessario per svolgere le loro mansioni.
- *Gestione dei beni*: la sicurezza fisica è rafforzata attraverso misure quali la videosorveglianza, il controllo degli accessi ai locali e le restrizioni all'ingresso del pubblico, salvaguardando così le infrastrutture critiche.

Queste misure sono sistematicamente mappate sui controlli ISO/IEC 27001 (ad esempio, A.6.3, A.9.1, A.11.1) e sulle categorie del NIST *Cybersecurity Framework* (ad esempio, PR.AC, PR.AT, PR.PT), garantendo che gli obblighi legali siano operativi all'interno di una struttura di conformità riconosciuta a livello internazionale. Il Modello facilita questa integrazione fornendo un quadro unificato che collega i requisiti normativi alle misure pratiche, consentendo alle organizzazioni di dimostrare proporzionalità, responsabilità e preparazione all'audit in tutti i settori della sicurezza.

Il processo di associazione si è basato sugli allegati 1 e 2³⁶ alla determinazione n. 164179/2025 dell'ACN³⁷, che sono stati concepiti per tradurre gli obblighi di legge in misure di sicurezza operative specifiche applicabili ai soggetti NIS. Dal punto

di vista contenutistico, i due allegati si distinguono (quasi) esclusivamente per i soggetti ai quali sono destinati: se l'allegato 1, infatti, è rivolto ai c.d. soggetti importanti, il secondo, invece, individua quelle che sono le misure di sicurezza di base che ogni soggetto c.d. essenziale dovrebbe implementare. Nonostante questa differenziazione, i requisiti di sicurezza sottostanti presentano una sostanziale convergenza, consentendo lo sviluppo di un approccio di mappatura unificato all'interno del Modello proposto. Il ruolo principale degli allegati 1 e 2 della determinazione n. 164179/2025 dell'ACN è quello di fungere da meccanismo di traduzione primario tra gli obblighi giuridici di alto livello della direttiva/quadro NIS (*Network and Information Systems*) e i requisiti di sicurezza operativa specifici e attuabili imposti ai soggetti regolamentati. Gli allegati definiscono le "specifiche di base" (o requisiti minimi di sicurezza) descrivendo in modo sistematico le misure organizzative e tecniche necessarie per raggiungere un livello sufficiente di sicurezza per le reti e i sistemi informativi.

L'allegato 2 riguarda le entità essenziali (EE), che in genere forniscono servizi critici la cui interruzione potrebbe avere un impatto sociale o economico significativo (ad esempio, energia, trasporti, sanità). Le specifiche qui riportate sono state concepite per essere rigorose ed esaurienti, riflettendo la natura ad alto rischio dei servizi forniti.

L'allegato 1 riguarda invece le entità importanti (IE), che sono soggette a requisiti meno rigorosi rispetto alle EE, ma devono comunque mantenere un solido livello di sicurezza. Sebbene i requisiti di sicurezza fondamentali (domini di sicurezza) spesso coincidano con quelli dell'allegato 2, i dettagli specifici di attuazione, le prove richieste o il livello di controllo possono essere adeguati in base al principio di proporzionalità. In sostanza, questi allegati suddividono gli obblighi giuridici generali (come "garantire la sicurezza") in domini di sicurezza specifici.

L'utilità del Modello proposto risiede nella sua capacità di tradurre i requisiti nazionali obbligatori in materia di sicurezza informatica, stabiliti

36. Per il testo completo di entrambi gli allegati, si rimanda a *Modalità e specifiche di base* – ACN.

37. ACN, determinazione n. 164179/2025 di cui all'articolo 31, commi 1 e 2, del decreto legislativo 4 settembre 2024, n. 138, adottata secondo le modalità di cui all'articolo 40, comma 5, lettera l), che, ai sensi dell'articolo 42, comma 1, lettera c), in fase di prima applicazione, stabilisce le modalità e le specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto medesimo.

dagli allegati 1 e 2 dell'ACN, in standard di sicurezza attuabili e riconosciuti a livello internazionale per gli enti NIS.

Questa funzione colma il divario tra l'obbligo giuridico prescrittivo e l'attuazione operativa pratica.

In altre parole, gli Allegati ACN (e, in particolare, la determinazione n. 164179/2025) costituiscono il quadro normativo autorevole che codifica i requisiti essenziali di sicurezza informatica previsti dalla legge italiana per gli enti che operano in settori critici e di grande rilevanza nazionale. Questi allegati stabiliscono la base minima delle misure di sicurezza operativa che gli Enti Essenziali e Importanti devono implementare per mitigare i rischi per la loro rete e i loro sistemi informativi. Essi adottano un approccio prescrittivo dall'alto verso il basso, definendo ciò che deve essere raggiunto (l'obiettivo normativo) senza necessariamente specificare il *come* operativo e granulare (il meccanismo tecnico).

L'utilità principale del Modello Smartlex è quella di facilitare l'operatività della conformità colmando il divario tra prescrizioni normative ed esecuzione pratica. Il Modello consente alle organizzazioni regolamentate di interpretare i requisiti generali stabiliti negli allegati dell'ACN e di tradurli in controlli di sicurezza specifici e dimostrabili che si allineano alla loro realtà operativa (c.d. traduzione in esecuzione). Il meccanismo centrale del Modello è il processo di mappatura incrociata (standardizzazione e allineamento). Questa mappatura allinea gli obblighi identificati dall'ACN con una serie di controlli derivati dai principali standard internazionali di sicurezza informatica (ISO/IEC 27001 e NIST *Cybersecurity Framework*). Questo allineamento garantisce che gli sforzi di conformità non solo siano giuridicamente validi, ma sfruttino anche le migliori pratiche del settore, affinando così la sicurezza complessiva al di là della semplice adesione alle normative. Il quadro di mappatura risultante può quindi essere popolato con requisiti legislativi specifici derivanti da varie normative nazionali e settoriali pertinenti,

fornendo un registro di conformità unificato e completo per il soggetto NIS³⁸.

La correlazione tra gli allegati ACN e il Modello può essere rappresentata come mostrato in Fig. 3.

Come illustrato nella Fig. 3:

- gli allegati dell'ACN stabiliscono ciò che la legge italiana richiede in materia di sicurezza informatica per gli enti che operano in settori altamente rilevanti, adottando un approccio prescrittivo;
- il Modello Smartlex consente alle organizzazioni interessate di comprendere come implementare i requisiti dell'ACN attraverso standard di sicurezza perfettamente aderenti alla realtà operativa.

In altre parole, la mappatura risultante da questo lavoro consente al soggetto NIS di implementare i requisiti identificati dall'ACN utilizzando misure di sicurezza specifiche e di allinearli ai due principali standard internazionali (ISO e NIST 2.0). Una volta eseguita la mappatura, è possibile inserirvi gli obblighi richiesti derivanti dalle normative pertinenti.

5. Esempi di implementazione

A conclusione del presente lavoro, vengono forniti in Tab. 8 alcuni esempi che illustrano come le misure di sicurezza del Modello possano essere utilizzate per implementare in maniera olistica e strategica i requisiti di cui agli allegati già menzionati.

Per comprendere sino in fondo i vantaggi apportati dal Modello Smartlex, segue un breve approfondimento di alcuni degli esempi riportati nella Tabella 8.

(a) *ID.RA-01 – Le vulnerabilità negli asset sono identificate, confermate e registrate*

Questo controllo impone un sistema in cui l'identificazione e il trattamento delle vulnerabilità costituiscano un'attività costante dell'organizzazione, lungi dall'esserne richiesta, invece, una semplicemente annuale. In tal senso, la fase di identificazione continua può essere soddisfatta, ad esempio, dall'utilizzo di test di penetrazione periodici: così l'organizzazione può dimostrare di aver adottato

38. Inoltre, occorre considerare due ulteriori aspetti: 1) l'integrazione tra il Modello Smartlex e gli allegati è estremamente semplice grazie all'utilizzo di un linguaggio comune, ovvero NIST 2.0; 2) il Decreto NIS impone un approccio basato sul rischio, che è preso in considerazione anche nel Modello Smartlex grazie all'associazione delle misure di sicurezza da adottare con lo standard ISO/IEC 27001:2022.

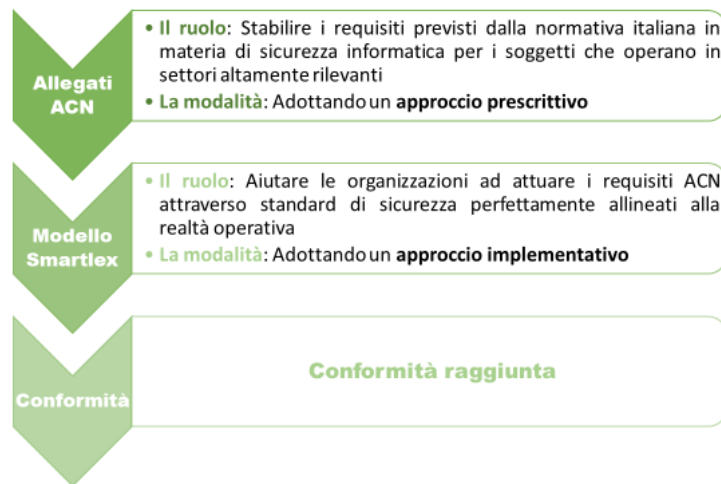


FIG. 3 — Percorso che le organizzazioni intraprendono per raggiungere la conformità, partendo dagli allegati ACN e passando, poi, dal Modello Smartlex

un approccio proattivo (in luogo di uno viceversa reattivo) non attendendo il verificarsi dell'incidente, ma ricercando attivamente gli eventuali punti deboli. La correttezza di una simile gestione è enfatizzata altresì dalla periodicità del test, che evidenzia come l'organizzazione riconosca la dinamicità dell'ambiente IT.

In tal modo, dunque, è possibile scoprire e registrare le vulnerabilità. Successivamente, grazie al *patch management* e agli aggiornamenti di sicurezza, le vulnerabilità possono essere mitigate. Le misure di sicurezza del Modello garantiscono, pertanto, un processo maturo e completo per la gestione delle vulnerabilità: l'organizzazione può infatti dimostrare non solo di aver definito il metodo per scoprire il rischio, ma anche il flusso di lavoro per gestirlo e risolverlo (l'intero "ciclo di vita della vulnerabilità").

(b) DE.CM-01 – Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi

Si tratta del controllo più considerevole della funzione di rilevamento e funge da ponte operativo tra la protezione passiva e la risposta attiva agli attacchi. Esso presuppone infatti un sistema che garantisca l'intercettazione tempestiva di eventuali eventi avversi. Tramite le misure di sicurezza di monitoraggio e *logging* degli accessi e delle attività, l'organizzazione può registrare dettagliatamente ogni accesso e attività sui sistemi informativi e di rete rilevanti: senza *log* completi e conservati, non sarebbe, infatti, possibile risalire alla causa radice di un incidente.

In più, grazie ad ulteriori misure, quali i sistemi di rilevamento e prevenzione dell'intrusione e l'aggiornamento automatico del registro delle minacce, è possibile elevare le capacità di rilevazione dell'organizzazione. La prima, infatti, è una "sentinella" che esamina i flussi di rete e i *log*, cercando *pattern* di attacco noti o comportamenti anomali (si pensi, ad esempio, ad un utente che accede a troppi file contemporaneamente). L'aggiornamento del registro delle minacce è anch'esso cruciale: assicura che questi sistemi operino con le *signature* di attacco più recenti, rendendo la rilevazione precisa e tempestiva. Infine, l'avviso di potenziali intrusioni viene immediatamente intercettato grazie alle procedure di *data breach* e di gestione degli incidenti. In conclusione, il Modello consente di dimostrare la completa integrazione del ciclo di vita della rilevazione e della risposta: grazie ad esso, infatti, gli eventi avversi possono essere identificati e successivamente gestiti in maniera efficace.

6. Conclusioni e prossimi obiettivi

Il lavoro presentato ha raggiunto con successo il suo obiettivo fondamentale: dimostrare la traducibilità di complessi quadri normativi e di sicurezza informatica in un Modello pragmatico e operativo applicabile dalle organizzazioni. Sebbene il Modello richieda ancora ricerca e perfezionamento, la sua utilità attuale è oggettivamente già significativa. Il Modello proposto offre un allineamento multilivello che integra sistematicamente le misure operative di sicurezza delle informazioni con gli standard

Allegati 1 e 2	Misure di sicurezza del Modello Smartlex	Utilità del Modello Smartlex
GV.SC-01: Sono stabiliti e accettati dagli stakeholder dell'organizzazione il programma, la strategia, gli obiettivi, le politiche e i processi di gestione del rischio di cybersecurity della catena di approvvigionamento.	Gestione e controllo delle esternalizzazioni; Sicurezza delle informazioni per l'uso dei servizi cloud.	L'adozione delle misure di sicurezza di cui alla mappatura permette di dimostrare l'esistenza di clausole contrattuali e di un processo di due diligence sui fornitori cloud, mitigando i rischi della supply chain come richiesto dall'ACN.
ID.RA-01: Le vulnerabilità negli asset sono identificate, confermate e registrate.	Patch management e aggiornamenti di sicurezza; Test di penetrazione periodici.	La mappatura presenta un allineamento tra ID.RA e la funzione di risposta (RS) che permette di adottare un approccio completo che soddisfi il requisito del ciclo di vita delle vulnerabilità degli asset.
PR.DS-11: I backup dei dati sono creati, protetti, mantenuti e verificati.	Backup cifrati e conservati off-site o in cloud sicuro; Backup di sicurezza: Continuo, Settimanale, Giornaliero; Predisposizione del ripristino con snapshot; Ridondanza.	L'adozione delle misure di sicurezza individuate nella mappatura consente all'organizzazione di disporre di dati in ripristino che siano non solo presenti, ma anche disponibili, integri e protetti, come richiesto dagli standard di governance più elevati.
DE.CM-01: Le reti e i servizi di rete sono monitorati per individuare eventi potenzialmente avversi.	Monitoraggio e logging degli accessi e delle attività; Sistemi di rilevamento e prevenzione intrusione (IDS/IPS); Procedure di data breach e gestione degli incidenti; Aggiornamento automatico del registro delle minacce.	La mappatura fornisce il meccanismo (logging), la tecnologia (IDS/IPS) e la procedura (gestione incidenti) che assicurano che gli eventi di sicurezza sui sistemi rilevanti vengano non solo registrati, ma anche analizzati e gestiti secondo i requisiti NIS2/ACN.
RS.CO-02: Gli stakeholder interni ed esterni sono informati degli incidenti.	Procedure di data breach e gestione degli incidenti con ruoli chiari e simulazioni periodiche; Relazione con autorità e gruppi specialistici.	La mappatura prevede strumenti di che includono l'interazione con soggetti esterni, soddisfacendo così l'obbligo di coordinamento e informazione in caso di incidenti.

TAB. 8 — *Esempi di come le misure di sicurezza del Modello Smartlex possono essere utilizzate per attuare i requisiti di cui agli allegati 1 e 2*

internazionali consolidati e gli obblighi normativi specifici. Esso si basa su solidi pilastri internazionali poiché associa le misure di sicurezza organizzative a due fondamentali quadri internazionali di riferimento per la sicurezza informatica (ISO/IEC 27001:2022 e NIST *Cybersecurity Framework (CSF) 2.0*).

L'allineamento multilivello ha il pregio di trasformare i principi astratti di sicurezza in misure attuabili, garantendo sia la coerenza strategica che la resilienza operativa. Il nostro Modello integrato, che combina i controlli ISO/IEC 27001 con le categorie del NIST *Cybersecurity Framework*, insieme alla serie di misure di sicurezza informatica da noi

individuate, offre vantaggi significativi: consente l'allineamento normativo, permettendo di armonizzare le pratiche organizzative con gli standard internazionali e i requisiti legali dell'Unione europea; fornisce un approccio strutturato per dare priorità e mitigare i rischi in modo efficace; in questo processo, contribuisce a ridurre i costi di conformità attraverso processi standardizzati e mappature chiare che migliorano l'efficienza operativa; infine, ma non meno importante, facilita una governance dimostrabile e la preparazione agli audit.

Inoltre, il Modello associa e traccia le misure adottate ai requisiti di conformità normativa

pertinenti. L'analisi degli obblighi imposti dalla legislazione italiana (Decreto Legislativo n. 138/2024, che recepisce la Direttiva NIS2) e la successiva determinazione dell'ACN sono servite come esempio definitivo per convalidare questa funzionalità.

Il contributo più significativo del Modello alle organizzazioni – in particolare, a quelle designate come soggetti NIS nell'esempio fornito – è la sua capacità di definire la metodologia concreta di implementazione dei requisiti prescrittivi dell'ACN. L'esempio illustra infatti come il Modello contribuisca a rendere operativi i requisiti: fornisce misure di sicurezza specifiche necessarie per soddisfare gli elementi essenziali della gestione del rischio previsti, ad esempio, dall'articolo 24 del Decreto NIS. Inoltre, detto quadro consente un monitoraggio semplice ed efficace dello stato di conformità, facilitando al contempo una dimostrabilità più agevole ed efficace della responsabilità e fornendo prove verificabili dell'attuazione dei controlli.

Nonostante i sostanziali risultati ottenuti, la mappatura realizzata deve considerarsi solo come un solido punto di partenza. Gli sviluppi futuri sono pianificati strategicamente per massimizzare la portata e l'utilità quantitativa del Modello. Essi dovrebbero sfruttare l'agnosticismo del quadro

normativo ampliando la portata dello strumento per comprendere tutti i quadri normativi pertinenti, consentendo una mappatura unica, funzionale e coordinata di obblighi disparati. Si prevede che questa capacità produrrà significativi risparmi sui costi per gli utenti, riducendo al minimo i costi di conformità e massimizzando l'efficacia operativa delle misure di sicurezza adottate.

Da un punto di vista teorico e operativo, la ricerca futura dovrebbe concentrarsi anche sullo sviluppo di un metodo in grado di assegnare un valore quantitativo misurabile al rischio per la sicurezza affrontato da ogni singola misura di sicurezza. Questo obiettivo si basa sull'analisi precedente, che ha dimostrato le potenziali implicazioni sistemiche del Modello per la valutazione del rischio e per fornire un approccio più oggettivo al criterio di proporzionalità, alla base della regolamentazione della sicurezza informatica.

Si prevede che l'evoluzione finale del Modello sarà un sistema quantitativo completo di misurazione della sicurezza informatica, che consentirà alle organizzazioni di misurare con precisione il proprio "livello di sicurezza" e di dimostrare in modo tangibile la conformità e la mitigazione dei rischi alle autorità di regolamentazione e alle parti interessate.

Riferimenti bibliografici

- ACN–AGENZIA PER LA CYBERSICUREZZA NAZIONALE (2025), *Linee guida NIS. Specifiche di base. Guida alla lettura*, in can.gov.it, 2025
- M. ALSHAR'E (2023), *Cyber security framework selection: comparision of nist and iso27001*, in "Applied computing Journal", vol. 3, 2023, n. 1
- F. CASAROSA, G. COMANDÈ (2025), *Il percorso di implementazione della Direttiva NIS 2: verso l'armonizzazione o una maggiore frammentazione?*, in "Annuario di Diritto Comparato", 2025, in corso di pubblicazione
- ENISA–EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (2025), *ENISA Threat Landscape 2025*, in enisa.europa.eu, 2025
- ENISA–EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (2019), *Reinforcing trust and security in the area of electronic communications and online services. Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing*, in enisa.europa.eu, 2019
- A. Lokare, S. Bankar, P. Mhaske (2025), *Integrating Cybersecurity Frameworks into IT Security: A Comprehensive Analysis of Threat Mitigation Strategies and Adaptive Technologies*, in Arxiv, arXiv:2502.00651, 2025
- M. MALATJI (2023), *Management of enterprise cyber security: A review of ISO/IEC 27001:2022*, in "International Conference On Cyber Management And Engineering (CyMaEn)" (Bangkok, 26-27 gennaio 2023), 2023

- A. OBI, O.V. AKAGHA, S.O. DAWODU, A.C. ANYANWU, S. ONWUSINKWUE, I.A. AHMAD (2024), *Comprehensive review on cybersecurity: Modern threats and advanced defense strategies*, in “Computer Science & IT Research Journal”, vol. 5, 2024, n. 2
- S. ROSE, O. BORCHERT, S. MITCHELL, S. CONNELLY (2020), *Zero Trust Architecture*, NIST Special Publications 800-207, 2020
- S. SCHMITZ-BERNDT (2023), *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive*, in “Journal of Cybersecurity”, vol. 9, 2023, n. 1
- A. SHAJI GEORGE, A.S. HOVAN GEORGE, T. BASKAR (2023), *Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats*, in “Partners Universal International Innovation Journal (PUIIJ)”, vol. 1, 2023, n. 4
- O. VAKHULA, Y. KURII, I. OPIRSKYI, V. SUSUKAILO (2024), *Security-as-Code Concept for Fulfilling ISO/IEC 27001:2022 Requirements*, in “Cybersecurity Providing in Information and Telecommunication Systems”, vol. 3654, 2024
- P. WANECKI, R. JASEK, I. DROFOVA (2023), *The Contribution of the European NIS2 Directive to the Design of the Cyber Security Model*, in “2023 International Conference on Information and Digital Technologies (IDT)” (Zilina, 20-22 giugno 2023), 2023



ARIANNA FIORENZA

I poteri privati digitali nell'era dell'IA: profili di concorrenza, protezione dei dati e tutela dei consumatori

Il contributo si concentra sull'intersezione tra diritto dei consumatori, protezione dei dati personali e diritto della concorrenza, promuovendo una lettura integrata e complementare di tali normative al fine di fronteggiare efficacemente i rischi connessi all'utilizzo dei sistemi di intelligenza artificiale e allo sfruttamento dei dati personali nella *data-driven economy*. Il rapido sviluppo tecnologico ha favorito, infatti, l'emersione di nuovi poteri privati, suscettibili di incidere profondamente non solo sulle dinamiche di mercato, ma anche sui diritti degli utenti. Particolare attenzione è dedicata alle nuove forme di pratiche commerciali scorrette che, attraverso meccanismi di consenso opachi e tecniche aggressive di profilazione sono suscettibili di comprimere la libertà di autodeterminazione del consumatore digitale, manipolando le sue scelte. L'analisi si sofferma, infine, sulle implicazioni concorrenziali, evidenziando come l'accesso privilegiato ai dati e alle tecnologie computazionali necessarie per elaborarli possa rafforzare le barriere all'ingresso e favorire condotte abusive non solo nel mercato digitale, ma anche nei mercati ad esso connessi, quale quello dell'intelligenza artificiale.

*Intelligenza artificiale – Economia digitale – Pratiche commerciali scorrette – Libertà di autodeterminazione
Concorrenza*

The digital private powers in the AI era: Competition, data protection and consumer law perspectives

The article focuses on the intersection between consumer law, data protection law and competition law, highlighting the need for an integrated and complementary interpretation of these regulatory frameworks in order to effectively address the risks associated with the use of artificial intelligence systems and the exploitation of personal data in the data-driven economy. Rapid technological development has, in fact, given rise to new forms of private power capable of profoundly affecting not only market dynamics but also consumers' rights. Particular attention is devoted to new forms of unfair commercial practices which, through opaque consent mechanisms and aggressive profiling techniques, may undermine the freedom of self-determination of the digital consumer by manipulating their choices. The analysis finally addresses the competition-law implications, highlighting how privileged access to data and to the computational technologies required to process them may strengthen barriers to entry and facilitate abusive conduct not only in digital markets, but also in related ones, including the AI market.

*Artificial intelligence – Digital economy – Unfair commercial practices – Right to self-determination
Competition*

SOMMARIO: 1. IA, *Big Data* e dominio tecnologico. – 2. Sfruttamento dei dati personali e AI: il complementare ruolo del *data protection law* e del diritto dei consumatori. – 3. Le dinamiche concorrenziali nell'era dei *Big Data* e dell'Intelligenza Artificiale. – 4. Riflessioni conclusive.

1. IA, *Big Data* e dominio tecnologico

L'intelligenza artificiale¹ si trova oggi al centro di una profonda rivoluzione tecnologica che sta ridefinendo molteplici aspetti della nostra società, contribuendo a ridelinearne regole ed equilibri. Lo sviluppo dei sistemi di IA sta riguardando diversi settori tra i quali la medicina, il lavoro, le neuroscienze, l'economia e, persino, il diritto e la giustizia². I vantaggi dell'automazione dei processi decisionali³, l'incredibile aumento della potenza di calcolo, la crescita esponenziale delle quantità di dati disponibili – resa possibile grazie all'espansione della rete Internet – sono tra le principali ragioni della rapida diffusione dei sistemi di IA.

In particolare, l'efficace funzionamento dell'IA non può prescindere dalla disponibilità di enormi volumi di dati, i quali ne costituiscono la linfa vitale. Com'è noto, essi sono essenziali, sia in fase di addestramento degli algoritmi che nella successiva fase di concreta operatività del sistema ai fini della produzione degli output.

Negli ultimi decenni, grazie all'avanzamento dell'ICT, si è assistito ad un profondo processo di datificazione⁴ della realtà, che ha portato a considerare i dati una risorsa imprescindibile per la conduzione delle più svariate attività, di interesse pubblico e privato. In tale contesto è nato il concetto di *Big Data*⁵, definiti quale carburante⁶ dell'intelligenza artificiale. Tra essi rientrano, certamente,

1. Com'è noto, la locuzione "intelligenza artificiale" comparve per la prima volta nella c.d. "proposta di Dartmouth" scritta da John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon ai fini della famosa conferenza di Dartmouth tenutasi nel 1956, evento che segna convenzionalmente l'inizio degli studi in materia di IA. L'espressione, nel tempo, è stata definita in vari modi. Un gruppo di ricercatori dell'Università di Stanford descrive l'IA come "una scienza e un insieme di tecniche computazionali che vengono ispirate – pur operando tipicamente in maniera diversa – dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire". Cfr. STONE–CALO–BROOKS et al. 2016, p. 5. Una più recente definizione è contenuta nel Reg. 2024/1689 secondo cui per sistema di IA si intende: "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".
2. BATTELLI 2024, p. 295 ss.
3. I sistemi automatizzati sollevano gli esseri umani dal compimento di molteplici attività più o meno complesse come il ragionare, riflettere, decidere.
4. Per datificazione si intende la trasformazione delle interazioni sociali in dati digitali suscettibili di acquisire valore anche economico. Tra i principali studiosi del fenomeno si ricordano: MAYER–SCHÖNBERGER–CUKIER 2013.
5. "Big Data usually refer to (1) the large dimension of datasets; and (2) the need to use large scale computing power and non-standard software and methods to extract value from the data in a reasonable amount of time", OECD 2016. Sul punto, v. anche DE MAURO–GRECO–GRIMALDI 2016.
6. PELUSO 2023.

anche i dati personali. Pur non essendoci univocità su cosa debba intendersi per Big Data, le loro caratteristiche sono tradizionalmente sintetizzate nelle “5 V”: volume, velocità, varietà, veridicità e valore⁷.

Più nello specifico, il *volume* fa riferimento all'enorme dimensione di dati raccolti, la *varietà* alla tipologia di dati disponibili, la *velocità* riguarda la capacità delle tecnologie di generare tali dati in modo continuativo. La *veridicità*, invece, si riferisce alla qualità dei dati raccolti, i quali se errati o incompleti possono causare errori nelle risposte degli algoritmi che si basano su di essi per fare previsioni.

Il *valore*, infine, identifica la capacità dei dati di produrre valore nel momento in cui sono analizzati ed elaborati dai soggetti che li raccolgono. In particolare, sono le tecniche di intelligenza artificiale – e, più precisamente, gli algoritmi di machine learning – che consentono di estrarre valore dai Big Data. Come spiegato in alcuni recenti studi⁸, dopo una preliminare fase di raccolta, interviene la vera e propria analisi dei dati la quale consente di far emergere dai dati grezzi non strutturati informazioni suscettibili di interpretazione e utilizzo pratico.

Per tale ragione riveste un ruolo centrale nell'intera “filiera dei Big Data” la fase della elaborazione, che comporta l'organizzazione dei dati grezzi non strutturati in informazioni suscettibili di essere utilizzate, ad esempio, per finalità economiche.

Ed è proprio il crescente valore acquisito – ed estratto – da tali dati che ha comportato l'emersione e l'espandersi del mercato digitale, governato

da pochi attori la cui posizione dominante, però, rischia di ostacolarne una leale concorrenza⁹. Come si chiarirà in seguito, tali soggetti privati – le c.d. *Bigh Tech* – sono detentori di grandi quantità di dati posti alla base dei nuovi modelli di business delle piattaforme digitali e utilizzati prevalentemente per offrire servizi personalizzati e pubblicità mirata agli utenti, oggetto, quest'ultimi, di un'intensa e costante attività di profilazione.

Dunque, Il valore economico del dato deriva non dalla mera fornitura da parte dell'interessato, bensì dal successivo trattamento di aggregazione ed analisi¹⁰, che si rivela essere particolarmente efficiente laddove condotto con algoritmi di auto-apprendimento¹¹. Ne consegue che sussiste un legame di corrispondenza biunivoca tra intelligenza artificiale e Big Data. Sebbene questi ultimi siano indispensabili per il training e il funzionamento dell'IA, allo stesso tempo la tecnologia si rivela essere uno strumento cruciale per estrarre ed attribuire, in fase di analisi, una funzione nonché un valore – anche economico – a tali dati.

Si osserva, sul punto, che lo sviluppo di nuove tecnologie per la raccolta, l'analisi e il trattamento delle informazioni sta conducendo al consolidamento della c.d. *data-driven economy*, un sistema economico basato sullo sfruttamento e la commercializzazione dei dati attraverso tecnologie automatizzate. Queste ultime consentono di creare accuratamente categorie e profili degli interessati da reimpiegare, ad esempio, nel settore della pubblicità online. Il risultato è “an economy based not on the creation of value through

7. AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2020, p. 8.

8. *Ivi*, p. 15.

9. PELUSO 2023, p. 41.

10. D'IPPOLITO 2022, p. 58.

11. Inoltre, è possibile osservare che gli algoritmi di *machine learning* consentono di estrarre nuova conoscenza da questi dati. Com'è noto il sistema di IA, in quanto sistema di apprendimento autonomo, utilizza l'inferenza per acquisire informazioni non limitate al dataset iniziale. L'inferenza è quel processo che consente alla macchina di fare previsioni o prendere decisioni su dati nuovi, acquisiti sulla base dei dati noti e dei modelli di addestramento. Per questo il sistema può essere definito intelligente, in quanto raccogliendo e confrontando enormi quantità di dati e sulla base dei modelli da questi estrapolati, riesce a determinare come comportarsi in presenza di input nuovi, che vanno, cioè, al di là dei dati inizialmente somministrati dal programmatore o, meglio, dall'*addestratore*, nella fase di training. Per questo può dirsi che un sistema intelligente è anche un sistema “creativo”, più vicino al modo di ragionare della mente umana.

production, but on values created through the flowing of information”¹².

Dunque, dati e informazioni hanno cominciato ad essere raccolti a livello globale da soggetti privati per finalità commerciali. Questo perché nell'era della datificazione, ogni istante dell'agire è, grazie alle tecnologie digitali, registrato, immagazzinato ed analizzato¹³. Si delinea, dunque, un modello di mercato in cui lo sviluppo tecnologico e i dati sono il principale oggetto di interesse delle imprese e del loro modello di business. Il legame indissolubile tra dati e IA sta ridefinendo gli equilibri economici globali, dando vita a un vero e proprio “capitalismo digitale”¹⁴, in cui l'informazione diventa una risorsa strategica paragonabile alle materie prime del passato. In questo contesto, chi è in grado di avvalersi delle nuove tecnologie, chi detiene le maggiori quantità di dati riveste la qualità di *gatekeeper* del mercato, sviluppando un potere privato per certi versi non dissimile dal potere pubblico. Si assiste, dunque, all'emergere di nuovi poteri privati digitali con cui la dottrina identifica quei soggetti che, seppur in assenza di una qualche legittimazione democratica, rivestono una particolare forza socio-economica che permette loro di incidere unilateralmente sulle sfere giuridiche degli individui con cui entrano in contatto¹⁵. Essi, dunque, danno vita a nuove forme di sovranità. In particolare, gli elementi tradizionalmente posti alla base dell'autorità degli Stati sovrani – come il controllo del

territorio, delle risorse e dell'informazione – sono stati significativamente ridisegnati dall'ascesa di nuovi soggetti che, esercitando un controllo sulle tecnologie su cui transitano i dati, hanno progressivamente acquisito una posizione di dominanza non solo nel mercato, ma nell'intera società¹⁶.

Dunque, il processo di datificazione a cui si è accompagnato l'avvento e il controllo delle nuove tecnologie ha portato a ridefinire il concetto di sovranità, oggi intesa sostanzialmente quale sovranità tecnica. Infatti, a cambiare non è solo la natura del soggetto detentore del potere, ma in tale scenario un rilievo centrale è assunto dal mezzo con cui tale potere viene esercitato¹⁷. Tale mezzo consiste proprio nelle capacità di calcolo e di automazione delle moderne tecnologie e nel controllo dei dati – anche personali – che le alimentano. Ad ogni modo, questi nuovi centri di potere, se lasciati proliferare in assenza di regolazione, rischiano di compromettere i tradizionali valori su cui si basano le democrazie occidentali, tra i quali la libera concorrenza e la tutela dei diritti fondamentali. Sebbene, infatti, le nuove tecnologie possano contribuire alla realizzazione e all'ampliamento delle libertà fondamentali della persona, dall'altro lato possono limitarle. Questo è particolarmente importante in un tempo nel quale la tecnologia concorre alla definizione di criteri valoriali e orienta sempre più le decisioni private e pubbliche¹⁸.

12. DE GREGORIO 2022, p. 80. Inoltre, in dottrina si osserva che l'incidenza di fattori tecnologici ha condotto alla diffusione della concezione del dato come *commodity*, ovvero una risorsa dalla quale è possibile trarre valore economico tanto da utilizzare il termine *consumerizzazione* della privacy. Cfr.: ALAGNA-CENTOFANTI 2021, p. 127. Sul punto si tornerà successivamente.

13. DI PORTO 2016.

14. Cfr. STAAB 2024.

15. CREMONA 2021, p. 881.

16. Il potere delle Big Tech, prive di una qualsivoglia legittimazione democratica, è in grado di influenzare la vita dei consociati in misura pari se non superiore a quella di una autorità pubblica democraticamente eletta. Sul punto, si veda TORREGIANI 2023, p. 132. Inoltre, alcuni autori ravvisano tra le ragioni che hanno permesso l'emergere e il consolidarsi di questi nuovi poteri il “liberalismo” degli ordinamenti democratici occidentali. DE GREGORIO 2022 p. 80: “New actors operating in the digital environment such as online platforms enjoy new areas of power deriving not just from a mix of business opportunities and technologies, but also from the openness of democracies oriented to digital liberalism which has left these actors accumulating powers”.

17. Nell'era digitale, dunque, la sovranità deve essere intesa necessariamente in forme nuove, che non possono prescindere dal mezzo tecnico. Si rimanda a: TORREGIANI 2023, p. 132.

18. Come chiarito nel 2019 da Antonello Soro, allora Garante per la protezione dei dati personali nel suo intervento in occasione della giornata europea per la protezione dei dati. Egli osserva, inoltre, che le innovazioni connesse

Da questa consapevolezza sembrano muovere i recenti atti normativi dell'Unione europea, che disegnano un quadro regolatorio volto a normare lo sviluppo e l'applicazione dell'IA, nonché la gestione e la circolazione dei suoi input essenziali, i dati. In particolare, si ricordano i regolamenti in materia di *data law*¹⁹, il Digital Markets Act²⁰ e il Digital Services Act²¹, nonché l'AI Act²².

Questo rapido avanzamento tecnologico impone, infatti, al diritto di adattarsi e di elaborare nuovi strumenti normativi in grado di governare rischi, opportunità e implicazioni etiche di sistemi sempre più intelligenti e pervasivi.

2. Sfruttamento dei dati personali e AI: il complementare ruolo del *data protection law* e del diritto dei consumatori

Come accennato, la raccolta e lo sfruttamento dei Big Data tramite le nuove tecnologie rappresentano il cuore della data driven economy e delle moderne attività di impresa.

Tra questi dati, rientrano anche dati personali, definiti da autorevole dottrina come il *lifeblood*

per le imprese digitali²³. Negli ultimi anni, infatti, le grandi piattaforme digitali – divenuta la sede principale per lo scambio di beni e servizi – hanno costruito modelli di business fondati sulla raccolta e l'analisi dei dati, che vengono trattati tramite sofisticati algoritmi al fine di trarne informazioni suscettibili di rilievo economico²⁴. Più nello specifico, l'attività di queste imprese si basa principalmente sull'analisi continua dei comportamenti degli utenti online. Le piattaforme online, puntano, infatti, a catturare quanto più possibile l'attenzione del consumatore. Successivamente, esse mirano a far produrre il maggior numero di “azioni” (ad es. *like*, *scroll*, *search*, ecc.) all'utente in modo da immagazzinare quanti più dati possibili. Il risultato di questo meccanismo è la profilazione dell'utente, funzionale ad una proposizione selettiva di servizi e contenuti e personalizzati²⁵. Com'è noto, l'art. 4 del GDPR definisce la profilazione come “qualsiasi forma di trattamento automatizzato di dati personali” volto a valutare, analizzare e prevedere determinati aspetti personali relativi ad una persona fisica, riguardanti “il rendimento professionale, la situazione economica, la salute, le

alle tecnologie digitali sembrano scardinare le coordinate del diritto a partire dal principio di territorialità e dalla nozione di sovranità. Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2019-A.

19. Con tale espressione si fa riferimento alle iniziative legislative aventi ad oggetto i dati. Tra queste si ricordano: Reg. (EU) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati), 27 Aprile 2016; Reg. (EU) 2022/868 del Parlamento Europeo e del Consiglio relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Data Governance Act), 30 maggio 2022; Reg. (EU) 2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 relativo a norme armonizzate sull'accesso equo e l'uso dei dati (Data Act), 13 dicembre 2023.
20. Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati contestabili e equi nel settore digitale (Digital Markets Act), 14 settembre 2022.
21. Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio relativo a servizi digitali nel mercato interno e che modifica la direttiva 2000/31/CE (Digital Services Act), 19 ottobre 2022.
22. Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio relativo all'intelligenza artificiale (Artificial Intelligence Act), 13 giugno 2024.
23. CUOCCI 2024, p. 64.
24. Come più volte chiarito, i dati una volta organizzati ed elaborati, assumono grande rilievo in relazione alle informazioni che sono in grado di fornire e che possono essere utilizzate per scopi commerciali, sociali o politici. Sul punto si rimanda a D'IPPOLITO 2022, p. 58 ss.
25. Perché fortemente collegati alla propria “storia” di attività online. In particolare, il tracciamento dell'utente avviene tramite i c.d. cookie, che costituiscono la più importante modalità di acquisizione dei dati relativi all'utente, consentendone, in via successiva, una precisa profilazione. Il fenomeno è puntualmente spiegato in AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2020 p. 33.

preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica”.

Tra i modelli di business più comuni vi è il c.d. *zero price*²⁶, che ricorre quando il servizio digitale viene offerto all'utente, senza che quest'ultimo debba pagare un corrispettivo di natura pecuniaria²⁷. L'utente dovrà, invece, consentire al trattamento dei suoi dati²⁸, che verranno plausibilmente sfruttati dall'impresa a fini commerciali²⁹. I possessori di tali dati possono, ad esempio, estrarre da essi trend di consumo dei singoli soggetti, ottenendo una serie di informazioni finalizzate ad orientare, sulla base delle preferenze espresse, le scelte commerciali dei clienti. A tal proposito, viene in rilievo il fenomeno del *targeting*, strettamente connesso alla profilazione, il quale consiste nella

proposizione mirata di contenuti (ad es., pubblicità) al consumatore-utente.

Il dato personale mostra, dunque, più che mai la sua natura ambivalente: non solo attributo della personalità oggetto di un diritto fondamentale³⁰, ma anche un asset fondamentale nell'era dell'economia digitale e dell'IA³¹.

Nel contesto descritto – mutuando il pensiero di Rodotà³² – la persona viene ridotta ad oggetto dal quale vengono costantemente estratte, con le tecniche più disparate, tutte le possibili informazioni per costruire profili ed identità, al fine di ritagliare dalla persona ciò che interessa al mercato. Nella c.d. società della sorveglianza, l'esperienza umana viene trasformata in dati sui comportamenti³³. In altri termini, il trattamento di dati personali per finalità di marketing si traduce in un nuovo modo di sfruttamento commerciale della persona³⁴.

26. Tale modello è preso in considerazione dallo stesso legislatore europeo nella direttiva 2019/770, che attribuisce particolare valore giuridico allo scambio di dati contro servizi. Si rimanda all'art. 3 della direttiva – recepito all'art. 135 *octies* Codice del consumo –, il quale sembra codificare il fenomeno della commercializzazione dei dati personali come strumento alternativo al pagamento in denaro. La direttiva si innesta nell'ambito della *Strategia europea per il digital single market* pubblicata dalla commissione nel 2015: doc. COM(2015) 192.

27. BATTELLI 2022-A, p. 355 ss.

28. Si pensi ad esempio ai social o alle piattaforme di e-commerce che memorizzano i dati degli utenti per personalizzare contenuti o prodotti, ma che allo stesso tempo cedono quei dati agli inserzionisti che intendono acquistare spazi pubblicitari. Da qui la definizione di mercato digitale quale *multi-sided market*, capace di offrire più servizi a diversi gruppi di utenti.

29. Ad ogni modo il c.d. *zero price* non esaurisce i modelli di business basati sui dati. Si pensi, ad esempio, al c.d. *personal data economy model*, che implica uno scambio diretto del dato contro moneta: in questo caso alla fornitura dei dati da parte dell'utente segue la corresponsione di una somma di denaro.

30. Come tale tutelato dagli art. 8 Carta di Nizza e 16 TFUE.

31. Si ricorda la sent. TAR Lazio n. 260 del 10 gennaio 2020 secondo cui le potenzialità insite nello sfruttamento dei dati personali possono costituire un asset in senso negoziale suscettibile di sfruttamento economico ed idoneo ad assurgere alla funzione di controprestazione in senso tecnico di un contratto. Inoltre, già nel 2018, l'allora presidente dell'Autorità Garante per la protezione dei dati Antonello Soro, osservava come il dato ad oggi assume “il ruolo tradizionalmente svolto da capitale e lavoro, nella sua duplice veste, tuttavia, di risorsa economica e di oggetto di un diritto fondamentale” (Discorso del Presidente Antonello Soro, *L'universo dei dati e la libertà della persona*, 2018).

32. RODOTÀ 2014, pp. 27-28.

33. Sul punto è significativo quanto affermato da ZUBOFF 2019: “Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as ‘machine intelligence’, and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these prediction products are traded in a new kind of marketplace that I call *behavioural futures markets*”.

34. CUOCCI 2024 p. 65.

È evidente che la raccolta e lo sfruttamento massivo dei dati generati dall'attività *online* – ma anche *offline*³⁵ – degli utenti rischia di compromettere fortemente la loro libertà di determinarsi autonomamente. Infatti, anche laddove il trattamento dei dati personali sia subordinato alla prestazione di un consenso esplicito da parte dell'interessato³⁶, tale garanzia nella prassi si rivela essere una tutela meramente formale. Nella Risoluzione del Parlamento europeo del 25 marzo 2021³⁷ già si evidenziava che l'attuazione dei requisiti relativi al valido consenso è spesso compromessa dal ricorso a modelli occulti, a tracciamenti pervasivi e ad altre pratiche non etiche, soprattutto per quanto riguarda la profilazione algoritmica, il *micro-targeting* o la pubblicità online.

Vi è, infatti, un'acclarata asimmetria informativa che caratterizza i rapporti tra l'utente e la piattaforma digitale della quale egli intende usufruire

per godere di un certo servizio. La scarsa consapevolezza in merito alla raccolta dei dati e alle relative modalità di utilizzo³⁸ rende il consumatore particolarmente vulnerabile e privo di reale autodeterminazione nel momento in cui è di fronte alla scelta di avvalersi o meno di servizi online (ancor più nell'ipotesi in cui tali servizi siano pubblicizzati come gratuiti³⁹), non potendo dirsi – quasi mai – soddisfatti quei requisiti richiesti dal *data protection law* affinché la manifestazione di volontà possa dirsi realmente informata⁴⁰. Per questi motivi, parte della dottrina sostiene che la categoria del consenso informato sia diventata una mera finzione, dovendosi piuttosto parlare di un consenso consapevolmente disinformato⁴¹. A ciò si aggiunge che le tecniche di *data analysis* fondate sull'intelligenza artificiale sono in grado di inferire dati personali anche da dati in astratto non riconducibili ad una persona identificata o identificabile⁴². Infatti,

35. Si pensi, ad esempio, a tutti quei dati generati dall'IoT, vale a dire da tutti quei dispositivi che, come lo smartphone, anche in assenza di un'interazione diretta con l'utente possono fornire dati rilevanti sui suoi comportamenti, abitudini e, quindi, sulle sue preferenze.

36. Com'è noto, il consenso ex art. 6 par. 1 lett. a) del GDPR, è tradizionalmente considerato uno dei principali fondamenti di liceità del trattamento, in quanto idoneo a garantire all'interessato il più ampio potere di controllo sui propri dati personali. Inoltre, la prestazione del consenso esplicito integra, ai sensi dell'art. 22, par. 2, lett. c), una delle tre eccezioni al divieto di sottoporre l'interessato a decisioni basate unicamente su trattamento automatizzato, tra cui la profilazione.

37. Risoluzione del Parlamento Europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del Regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP)).

38. Alcune indagini condotte dall'ACGM nel 2020 dimostrano che il 40% degli utenti intervistati non ha consapevolezza né del fatto che la navigazione in Internet e l'utilizzo di app e servizi online comporti la raccolta di dati personali né del fatto che tali dati possano essere ceduti dal fornitore del servizio a terzi. Cfr.: AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2020, p. 94. I risultati di questi studi possono considerarsi ancora rilevanti allo stato attuale.

39. Come sottolineato anche nell'indagine conoscitiva sui Big Data in particolare, l'utente viene attratto dal *claim* sulla gratuità del servizio offerto nonché dall'agevole e immediata fruibilità dello stesso per poi essere indotto a condividere in rete esperienze personali, dati e informazioni. Ad ogni modo, non sono quasi mai espressamente chiare le finalità remunerative perseguite dalle imprese, che possono ottenere il massimo sfruttamento economico dei dati attraverso la profilazione degli utenti.

40. Sul punto: considerando n. 32 GDPR.

41. CASONATO 2019, p. 107.

42. Com'è noto l'art. 4 del GDPR definisce il dato personale come "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".

l'IA utilizza una enorme mole di dati, molti dei quali rientranti nella definizione di dato personale ai sensi del GDPR, altri anonimi o anonimizzati che però l'IA potrebbe re-identificare. Si osserva, dunque, che con il progredire delle tecnologie di trattamento dei dati, muta la stessa nozione di dato personale, il quale si rivela essere un concetto fluido e cangiante essendo necessario prestare attenzione anche al contesto in cui il dato è estratto⁴³.

Alla luce di quanto espresso, sembra, dunque, svuotarsi di contenuto quel diritto all'autodeterminazione informativa⁴⁴, che rappresenta il punto cardine della disciplina in materia di *data protection*. In tale contesto, risulta quanto mai necessario recuperare il nucleo essenziale di tale diritto, consentendo all'utente un pieno controllo dei suoi dati. In tale scenario, riveste un ruolo centrale l'obbligo di informativa, di cui all'art 12 del GDPR, la quale deve consentire all'utente di avere piena cognizione del fatto che i dati da lui ceduti non saranno utilizzati solo per far funzionare i servizi a cui accede, ma che essi saranno sfruttati dalla piattaforma per fini di lucro.

Tuttavia, come chiarito dalla giurisprudenza attuale, una carente informazione circa le modalità di trattamento dei dati è suscettibile di integrare anche una pratica commerciale scorretta ai sensi del Codice del consumo. Infatti, il rapporto tra l'utente e l'operatore della piattaforma integra un vero e proprio rapporto di consumo, anche in assenza di una controprestazione pecuniaria⁴⁵. Questo perché il patrimonio informativo ceduto dall'utente acquista un evidente valore economico in quanto viene usato dalla piattaforma a fini commerciali, delineandosi, solo in apparenza, un rapporto gratuito. Si ravvisa, dunque, un rapporto di scambio in cui i dati dell'utente – non più un

mero interessato ai sensi del GDPR, bensì un consumatore – rappresentano la controprestazione del servizio fornito dalla piattaforma.

Alla luce di ciò, in una recente sentenza il Consiglio di Stato ha ravvisato una pratica commerciale ingannevole ai sensi dell'art 21 del Codice del consumo, consistente nell'omessa informazione sull'uso per fini commerciali dei dati personali dell'utente⁴⁶, chiarendo che non è sufficiente informare l'utente che i suoi dati saranno usati per la ricezione di comunicazioni di marketing "personalizzate", essendo una tale comunicazione del tutto inidonea a perseguire lo standard richiesto dalla normativa di protezione del consumatore. Questo in quanto la profilazione degli utenti – che è ciò che consente il miglioramento della performance di vendita delle piattaforme digitali – utilizza l'intelligenza artificiale, della quale il grande pubblico intende parlare solo da pochi anni. Nel caso di specie, non poteva dunque presumersi che il consumatore medio fosse in grado di comprendere le conseguenze della cessione dei propri dati, e cioè la profilazione, semplicemente per il fatto di essere stato avvisato che avrebbe ricevuto delle comunicazioni di marketing. Si richiede, così, una maggiore granularità e specificità delle informazioni fornite al consumatore digitale, che devono essere adeguate al concreto atteggiarsi della fattispecie e alla capacità del consumatore medio di comprendere le dinamiche commerciali in atto. Solo in questo modo il consumatore è in grado di autodeterminarsi in maniera consapevole.

Com'è noto, vi è una fisiologica debolezza contrattuale che connota il consumatore nei rapporti Business to Consumer, dovuta prevalentemente ad una asimmetria informativa tra le parti. Tale vulnerabilità risulta essere ancor di più accentuata

43. Sul punto PELUSO 2023 pp. 113-114.

44. Da intendersi quale libertà positiva di controllo e di intervento in favore del soggetto a cui l'informazione è riferita. Sul punto si rimanda a COLAPIETRO 2018, p. 13 ss. Tale principio trova la sua genesi nella sentenza della Corte Costituzionale tedesca del 15 dicembre 1983 BVerfG, BvR 209/83. La Corte delinea l'esistenza di un "diritto che garantisce la facoltà dei singoli di autodeterminarsi" e "di stabilire se divulgare e utilizzare i propri dati personali" e, quindi, di decidere "quando e entro quali limiti rivelare questioni relative alla propria vita personale": tale diritto è ritenuto corollario della dignità umana e della libertà d'agire.

45. Consiglio di Stato, 29 marzo 2021, n. 2631, il quale conferma quanto già espresso dall'AGCM nel provvedimento del 29 novembre 2018 n. 27432.

46. Consiglio di Stato, 2 dicembre 2024, n. 9614. Si trattava di un'omissione informativa posta in essere in occasione dell'attivazione del "profilo" digitale dell'utente (Apple id) circa l'utilizzo a fini commerciali dei dati personali degli utenti, elaborati tramite la profilazione durante le interazioni con il *market place* del provider.

nelle ipotesi in cui il consumatore usufruisce di servizi o prodotti digitali, cedendo come corrispettivo i propri dati personali. Questo in quanto egli non è in grado di comprendere agevolmente il funzionamento delle tecnologie di elaborazione dei dati⁴⁷, specie quando si tratta di algoritmi di autoapprendimento⁴⁸.

Nel caso in esame, il Consiglio di Stato ha, inoltre, qualificato come pratica commerciale aggressiva la scelta di Apple di preimpostare l'acquisizione del consenso al trattamento dei dati personali, rendendo particolarmente difficoltosa la procedura di opt-out per la revoca dello stesso. È, dunque, evidente lo sforzo del giudice amministrativo di attuare la disciplina consumeristica, adattandola alla luce di quelle che possono definirsi "le nuove pratiche commerciali scorrette" al fine di garantire all'utente una maggiore tutela nonché un maggiore controllo delle proprie informazioni personali. In questo senso, la disciplina della privacy e quella consumeristica non sono in rapporto antinomico, ma sono necessarie per garantire una tutela piena ed effettiva all'interessato-consumatore.

Quanto affermato si rivela essere particolarmente innovativo e prezioso nello scenario attuale in cui i grandi operatori economici utilizzano i dati degli utenti, combinati con sofisticate tecniche di intelligenza artificiale al fine di comprimere, ma anche di manipolare, la libertà di autodeterminazione del consumatore, inducendolo a scelte di consumo che altrimenti non avrebbe effettuato. Ne consegue che non solo le carenze informative, ma anche le altre condotte adottate dalla piattaforma-professionista, pur rilevanti ai fini della disciplina sulla protezione dei dati personali, possono integrare violazioni suscettibili di essere valutate anche

alla luce della normativa consumeristica. Si pensi, ad esempio, al già citato fenomeno del *targeting*, consistente nella proposizione mirata di contenuti personalizzati all'utente al fine di orientare le sue decisioni commerciali⁴⁹, fino ad *indurre* nello stesso dei bisogni di acquisto. Nel *targeting*, il trattamento dei dati personali si rivela spesso opaco, potendo comportare un utilizzo dei dati per finalità ulteriori a quelle dichiarate nell'informativa che l'interessato non poteva ragionevolmente prevedere. Questo mina la capacità dell'interessato di esercitare e mantenere un controllo sui propri dati. Ad ogni modo, questo fenomeno non solleva solo problemi di contrasto con i principi del GDPR – in particolare con i principi del consenso, di minimizzazione e finalità –, ma anche in relazione ad altri diritti e libertà fondamentali. Alcune pratiche di *targeting*, infatti, grazie all'uso improprio di sofisticati algoritmi possono fortemente minare la libertà di autodeterminazione del soggetto, ad esempio inviando messaggi personalizzati idonei a sfruttare talune vulnerabilità del soggetto. Tali messaggi possono così arrivare a influenzare il processo di pensiero della persona, le emozioni e i suoi comportamenti⁵⁰ di acquisto.

Ne consegue che anche queste pratiche sono potenzialmente suscettibili di essere attratte nell'ambito di applicazione del Codice del consumo, potendo essere qualificate come pratiche commerciali ingannevoli o addirittura aggressive se idonee a determinare un indebito condizionamento del consumatore digitale ai sensi dell'art. 25 del Codice. Sul punto è utile segnalare quanto affermato dalla Commissione europea, la quale, con riguardo alle pratiche commerciali scorrette basate sui dati, ha chiarito che esse possono

47. Per questo parte della dottrina suggerisce la necessità di una alfabetizzazione digitale, in quanto solo rafforzando la consapevolezza degli utenti sull'utilizzo dei propri dati è possibile governare il potere delle Big Tech. Cfr. PAGNANELLI 2022, p. 24.

48. Il cui funzionamento può essere in parte oscuro allo stesso provider. Infatti, uno dei principali problemi dei sistemi di IA è che essi si atteggiavano come una *black-box*. In altri termini, la poca trasparenza di tali sistemi non consente di prevedere ex ante il loro funzionamento né di spiegarlo ex post. Cfr.: WIGMORE 2023.

49. Esso viene definito come veicolazione di messaggi specifici alle persone fisiche che dispongono di account sui social media. Ad oggi numerosi fornitori di social media forniscono dei servizi di *targeting*. Esso, come le altre pratiche di sfruttamento economico dei dati personali, si fonda sull'analisi e l'elaborazione delle informazioni personali fornite attivamente dagli utenti alla piattaforma o desunte sulla base di comportamenti di navigazione al di fuori della piattaforma stessa.

50. Cfr.: European Data Protection Board (EDPB), *Guidelines 8/2020 on the targeting of social media users*, 13 aprile 2021.

produrre un significativo effetto di manipolazione sui consumatori più vulnerabili⁵¹.

Inoltre, quanto detto sembra confortato anche da quanto sostenuto dall'AGCM nel procedimento avverso la piattaforma Tik Tok⁵². In tale sede, l'Autorità ha qualificato come pratica commerciale scorretta *ex art 25* Codice del consumo l'utilizzo da parte della piattaforma di un sistema di raccomandazione, basato su tecniche di profilazione, idoneo a generare un indebito condizionamento degli utenti. Tale sistema presenta diverse analogie con il *targeting*, in quanto entrambi i sistemi si fondano sulla profilazione algoritmica e mirano a proporre dei contenuti – di regola pubblicitari – personalizzati agli utenti, comprimendone la facoltà di scelta⁵³.

Alla luce di quanto espresso è dunque evidente che i rapporti tra la normativa in materia di data protection e la disciplina consumeristica debbano delinearsi sempre più in termini di una integrazione positiva, nella quale il diritto dei consumi diviene funzionale ad attuare quelle garanzie previste dal *data protection law*, contribuendo ad arginare quei fenomeni di abuso che tendono a limitare progressivamente l'autonomia informativa e decisionale dei consumatori-interessati.

3. Le dinamiche concorrenziali nell'era dei Big Data e dell'Intelligenza Artificiale

Alla luce di quanto chiarito nei precedenti paragrafi, emerge che, sebbene con riguardo all'illecito trattamento automatizzato di dati personali il rispetto del GDPR rimanga pur sempre centrale, esso non esclude l'applicazione di altri corpi normativi laddove il trattamento dei dati coinvolga

comportamenti e situazioni disciplinate da altre fonti giuridiche a presidio di altri valori ed interessi. Solo in questo modo, infatti, può essere garantita una pienezza di tutela delle persone fisiche. Del resto, già la Commissione Ue, nell'attribuire ai dati personali ceduti dagli utenti un valore economico *de facto*, aveva chiarito che una piattaforma che si qualifica come “professionista”, nell'ambito delle sue pratiche commerciali deve sempre rispettare le norme dell'Ue in materia di diritto dei consumatori nonché le norme in materia di concorrenza⁵⁴.

In tale sede è opportuno focalizzare l'attenzione sulle implicazioni concorrenziali connesse all'utilizzo dei Big Data e allo sviluppo delle nuove tecnologie, la cui integrazione nel business delle imprese rappresenta la chiave per mantenere una posizione privilegiata sul mercato.

Come già accennato, l'accentramento del patrimonio informazionale nelle mani degli attori privati comporta un aumento della forza degli stessi nei confronti dei concorrenti. Dunque, dal quadro in esame si evince che la disponibilità di tali dati costituisce per le imprese non solo remunerazione della loro attività, ma anche un importante fattore competitivo nel mercato digitale e non solo. In particolare, si osserva che il possesso – o, meglio, il monopolio – dei Big Data nonché le capacità computazionali per elaborarli, permette alle Big Tech di entrare agevolmente in mercati in cui non sono ancora attive e di dominarli. Ad esempio, gli operatori che rivestono una posizione dominante nel mercato delle piattaforme digitali potrebbero estendere tale posizione di forza economica anche al mercato adiacente dell'IA, dando luogo ad eventuali abusi di posizione dominante *ex art. 102*

51. Commissione europea, *Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno* (2021/C 526/01), 29 dicembre 2021.

52. AGCM, provv. n. 31124 del 5 marzo 2024, PS12543, in “Bollettino” 11/2024.

53. Sebbene l'indagine dell'ACGM non riguardasse direttamente il *targeting* e la pubblicità mirata, essa evidenzia come i meccanismi di profilazione e personalizzazione propri delle piattaforme digitali possano alterare la libertà decisionale degli utenti. Con riguardo al sistema di raccomandazione usato da Tik Tok, la profilazione diventa tanto più precisa quanto più l'utente utilizza la piattaforma perché il sistema apprende in maniera più dettagliata le preferenze. Tale sistema di raccomandazione personalizzata genera nell'utente, specie nei soggetti vulnerabili, un effetto di addiction che la piattaforma riesce a monetizzare, aumentando la redditività degli introiti pubblicitari.

54. Commissione europea, *Orientamenti sull'attuazione/applicazione della Direttiva 2005/29/CE sulle pratiche commerciali scorrette* (SWD(2016) 163), 25 maggio 2016.

TFUE⁵⁵. Questo, in quanto essi dispongono della quantità di dati e della potenza di calcolo necessarie per la progettazione, lo sviluppo e il funzionamento dei sistemi di IA⁵⁶.

In tal senso, si può osservare che il mercato digitale e il mercato dell'IA presentano dei confini piuttosto labili, in quanto i colossi del primo ben potrebbero entrare nel secondo mercato – anche per il tramite di alleanze strategiche con aziende sviluppatrici dominanti nel settore dell'IA – offrendo ai consumatori nuovi *smart products* e servizi basati sull'intelligenza artificiale (si pensi, ad esempio, ai servizi di chatbot che usano l'IA generativa). Ne consegue che le piattaforme digitali dominanti possono sfruttare il loro potere di mercato ponendo in essere pratiche sleali (come il *self-preferencing*, il *tying* o il *bundling*) limitando le scelte dei consumatori e aumentando le barriere all'ingresso per le imprese più piccole.

Un esempio emblematico ed attuale di questa tendenza può essere individuato nella condotta di Meta, che ha integrato il servizio Meta AI all'interno di WhatsApp, imponendo di fatto il nuovo sistema di chatbot ai consumatori. Sulla questione è pendente un procedimento istruttorio dinanzi all'AGCM, al quale si è di recente aggiunto anche un procedimento cautelare⁵⁷ per presunto abuso di posizione di dominante. In particolare, si osserva che attraverso l'abbinamento di Meta AI con WhatsApp, Meta appare in grado di *trainare la*

propria base utenti, dal mercato in cui è già dominante – quello digitale dei servizi di messaggistica – *al nascente mercato dell'IA*, non attraverso una concorrenza basata sui meriti, ma imponendo agli utenti la disponibilità dei due servizi distinti, con potenziale pregiudizio dei servizi concorrenti. Inoltre, è significativo il passaggio del provvedimento dell'Autorità in cui si ricorda che lo sviluppo dei sistemi IA richiede la disponibilità di ampi set di dati per il training degli algoritmi. Tali dati sono input necessari a cui le grandi piattaforme come Meta hanno facilmente accesso. Nel provvedimento, non si esclude che Meta utilizzi i dati dei propri utenti al fine di allenare il suo chatbot.

In questo scenario, il rispetto delle norme sulla privacy può giocare un ruolo centrale nel contribuire a garantire la leale concorrenza tra le imprese della moderna economia⁵⁸.

Come chiarito dalla CGUE⁵⁹, la conformità alla normativa sulla protezione dei dati è un parametro significativo nella valutazione delle condotte di un'impresa dominante nei mercati digitali, soprattutto nell'ambito della valutazione di abuso di posizione dominante *ex 102 TFUE*⁶⁰.

Una efficace regolazione del trattamento dei dati personali può contribuire a rafforzare la concorrenza nel settore dell'intelligenza artificiale, assicurando maggiore fiducia da parte degli utenti⁶¹ e condizioni paritarie di accesso ai dati, evitando che singoli operatori conseguano vantaggi

55. Il quale, come chiarito dalla giurisprudenza europea, non vieta solo l'abuso posto in essere nel mercato in cui l'impresa è dominante, ma censura anche il comportamento dell'impresa che sfrutta la sua posizione dominante in un certo mercato, per estenderla in un mercato contiguo, ma separato. CGUE, C-48/22 P, *Google LLC and Alphabet Inc. v European Commission*, 10 settembre 2024.

56. Cfr.: G7 Competition Authorities, *Digital Competition Communiqué*, 4 ottobre 2024 “The concentrated control of crucial AI inputs has the potential to place a small number of firms in key market positions”.

57. AGCM, provv. n. 31634, 22 luglio 2025; ACGM, provv. n. 31728, 25 novembre 2025.

58. PITRUZZELLA 2016, p. 27.

59. CGUE, C252/21, *Meta Platforms Inc. and Others v. Bundeskartellamt*, 4 luglio 2023.

60. Ciò appare coerente anche con quanto già sostenuto da una parte della dottrina che propone da tempo un adattamento delle categorie tradizionali del diritto antitrust ai mercati *data-driven*. Sul punto BAGNOLI 2016, secondo cui la raccolta e l'utilizzo dei Big Data inducono a ripensare la nozione di potere di mercato e di mercato rilevante.

61. In tal senso il già citato G7 Digital Competition Communiqué: “safeguarding personal data is crucial to maintaining public trust and ensuring that AI development respects individual rights”. Similmente, sebbene con riguardo ai servizi digitali, v. PITRUZZELLA 2016 p. 27, secondo cui “Privacy is an important element of trust and trust in digital service is necessary for online markets to work smoothly and to be an engine for work and competitiveness”.

anticoncorrenziali derivanti da pratiche illegittime di raccolta e uso dei dati. La stessa Commissione Ue⁶² nella sua *Notice on the Definition of Relevant Market* ha individuato nella *privacy protection* garantita dal professionista un parametro da tenere in considerazione. I consumatori potrebbero, infatti, preferire soluzioni che consentano di fornire la quantità minore di dati possibile o di mantenere il maggior controllo possibile sull'utilizzo dei dati personali forniti.

Ne consegue che la protezione dei dati personali e, quindi, la garanzia di una maggiore consapevolezza da parte del consumatore sull'uso dei propri dati, possono rappresentare fattori qualitativi rilevanti per il confronto concorrenziale tra gli operatori del mercato digitale e del mercato dell'IA.

L'*European Data Protection Board* osserva che: "strengthening the link between the protection of personal data and competition can contribute to the protection of individuals and the well-being of consumers by reinforcing the common consideration of respect for their fundamental rights and the proper functioning of competitive markets"⁶³. Sebbene, infatti, la normativa sulla protezione dei dati e il diritto della concorrenza perseguano differenti obiettivi, essi condividono dei tratti in comune, rinvenibili nella tutela degli individui e delle loro scelte.

È opportuno sottolineare che la protezione dei dati personali – quale diritto fondamentale – deve essere coniugata con l'esigenza di promuovere la libera circolazione di tali dati e, dunque, una maggiore apertura del mercato dell'innovazione digitale. Tale interpretazione sembra essere accolta dallo stesso GDPR, il quale già nei considerando sancisce che la protezione dei dati personali non è da intendersi quale diritto assoluto, ma deve essere temperata con altri diritti fondamentali,

compresa la libertà d'impresa, in ossequio al principio di proporzionalità. Il regolamento, infatti, unitamente alla tutela della persona, ha come obiettivo quello di assicurare la libera circolazione dei dati anche al fine di favorire il progresso economico e il rafforzamento del mercato interno⁶⁴.

Il diritto alla protezione dei dati personali non rappresenta così un ostacolo alla libera concorrenza, la quale, tuttavia, deve essere attuata nel rispetto dei valori fondamentali della persona⁶⁵.

In questo quadro, favorire una circolazione dei dati, anche personali, che sia al tempo stesso libera, ma sicura e consapevole, si rivela imprescindibile al fine di evitare una eccessiva concentrazione di quelli che sono i principali fattori di sviluppo dell'intelligenza artificiale. Infatti, l'accesso equo alle risorse – le quali comprendono i dati personali e non – è quanto mai necessario per lo sviluppo e l'implementazione dell'IA. In questo senso, garantire la portabilità dei dati e assicurare entro certi limiti una interoperabilità tra i sistemi che li trattano può favorire il leale gioco della concorrenza stimolando l'innovazione e la diversificazione dell'offerta. Come osservato dall'OECD (*Organisation for Economic Co-operation and Development*), la mancanza di portabilità e di interoperabilità può facilitare la concentrazione di dati proprietari (c.d. *data silos*⁶⁶), determinando barriere all'entrata⁶⁷ in diversi settori di mercato nei quali l'IA già svolge (o svolgerà in futuro) un ruolo importante e sempre maggiore.

Ad ogni modo, si ribadisce che la promozione della libera circolazione dei dati e dello sviluppo delle nuove tecnologie non possono tradursi in un sacrificio dei diritti fondamentali della persona e, in particolare, del diritto alla protezione dei dati personali, che costituisce un limite invalicabile⁶⁸.

62. Commissione europea, *Notice on the Definition of the Relevant Market for the Purposes of Union competition Law* (C/2024/1645), 22 febbraio 2024.

63. Cfr.: European Data Protection Board (EDPB), *Position Paper on Interplay Between Data Protection and Competition Law*, 16 gennaio 2025.

64. Si vedano i considerando n. 2 e n. 4, nonché l'art. 1 del Regolamento.

65. BATTELLI 2022-B, p. 1096 ss.

66. Si tratta di dati raccolti ed utilizzati da un'unica piattaforma che non vengono resi in alcun modo accessibili a terzi o riutilizzabili da terzi.

67. OECD 2025, p. 31 ss.

68. BATTELLI 2022-C, p. 21 ss.

Questo è chiarito anche nell'*AI Act*, che mira allo sviluppo di un'intelligenza artificiale affidabile, antropocentrica e rispettosa dei diritti fondamentali, e tra essi il diritto alla protezione dei dati che deve essere assicurato durante l'intero ciclo di vita del sistema.

Da tali consapevolezze prendono le mosse il *Data Governance Act* e il *Data Act*, gli atti normativi complementari adottati dall'Ue che, in attuazione della *European Data Strategy*, mirano a promuovere la disponibilità dei dati – personali e non – all'interno dell'Unione e a potenziarne i relativi meccanismi di condivisione.

Tali interventi normativi devono essere interpretati in maniera coordinata e sistematica con il *Digital Markets Act*, il quale sancisce divieti e impone una serie di obblighi nei confronti dei c.d. *gatekeeper*⁶⁹ al fine di limitare un accentramento del potere di controllo sui dati, prevenendo condotte anticoncorrenziali. Sebbene tale regolamento abbia come primario ambito di applicazione i mercati digitali – costituendo un'imprescindibile strumento di regolazione *ex ante* –, la sua attuazione è idonea a produrre effetti rilevanti anche nel mercato dell'intelligenza artificiale, trattandosi di un mercato strettamente connesso a quello digitale. In particolare, le obbligazioni imposte ai *gatekeeper* sono in grado di incidere – quanto meno indirettamente – anche in questo secondo mercato in quanto gli attori destinatari del DMA sono ormai attivi nella filiera dell'AI, offrendo servizi basati su tale tecnologia. Si pensi, ad esempio, a tutti quegli obblighi di accesso ai dati e di interoperabilità previsti dall'art. 6 par. 9, 10, 11 e

12 nonché dall'art. 7 del DMA, volti a favorire la condivisione dei dati raccolti dai *gatekeeper* con imprese terze e utenti commerciali, sebbene pur sempre nel rispetto del GDPR laddove entrino in gioco dati personali⁷⁰.

È evidente che obblighi del genere sono idonei a prevenire l'accumulo di dati proprietari in capo a singole imprese, garantendo un mercato dell'IA aperto alla competitività e all'innovazione nonché più vicino al benessere del consumatore.

Infine, si aggiunge che i *gatekeeper* in quanto fornitori di servizi basati sull'IA, sono sottoposti alle regole dell'*AI Act* e saranno considerati responsabili in caso di mancata conformità agli obblighi che esso prevede⁷¹.

4. Riflessioni conclusive

L'intelligenza artificiale e lo sfruttamento economico dei dati personali rappresentano l'avanguardia dei nuovi modelli di business.

L'analisi condotta evidenzia come la regolazione delle nuove tecnologie configura un ambito in cui la tutela dei dati personali, la protezione dei consumatori e il diritto della concorrenza sono destinati a intersecarsi in maniera sempre più stretta. Da un lato, infatti, il ruolo del *data protection law* rimane centrale, assumendo la privacy sempre più la natura di un *meta-diritto* il cui godimento è necessario per la realizzazione degli altri diritti⁷². Si pensi, ad esempio, al ruolo pro-concorrenziale della privacy nel mercato. Dall'altro lato, tuttavia, si è visto come l'applicazione di altre discipline, quale la normativa consumeristica, contribuisca a rafforzare la

69. Si rinvia alla definizione di cui all'art. 3 del DMA: "Un'impresa è designata come *gatekeeper* se: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (*gateway*) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro". Il par. 2 prevede, poi, le condizioni in presenza delle quali, si presumono soddisfatti i requisiti di cui al par. 1.

70. Questo è più volte ribadito dal DMA che si applica senza pregiudicare le norme derivanti da altri atti di diritto dell'Unione tra i quali il reg. 2016/679. Sul punto, è rilevante il considerando 61 secondo cui "Nel fornire accesso ai suoi dati di ricerca, è opportuno che il *gatekeeper* garantisca la protezione dei dati personali degli utenti finali, anche da eventuali rischi di reidentificazione, con mezzi adeguati, come l'anonimizzazione di tali dati personali, senza compromettere in maniera sostanziale la qualità o l'utilità dei dati".

71. Si rimanda a PERUGINI 2025, p. 71, in cui si osserva che il DMA si interseca inevitabilmente con l'AI Act.

72. COLAPIETRO 2021, p. 832. Sul punto, si ricordano, inoltre, le parole di Antonello Soro, il quale qualifica la protezione dei dati un "requisito di tutela del consumatore e di *antitrust by design*", cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI 2019-B.

tutela del (consumatore) soggetto-interessato, assicurando quel diritto all'autodeterminazione informativa alla base del GDPR.

La protezione del consumatore e, dunque, anche la protezione della sua privacy, costituiscono a loro volta uno strumento funzionale a garantire l'efficienza del mercato e il leale gioco della concorrenza. Del resto, come osserva la dottrina, regolare il mercato significa regolamentare le singole iniziative economiche che in esso trovano attuazione e,

dunque, i singoli atti di autonomia privata⁷³, al fine di evitare che i fallimenti dell'autonomia privata si traducano in fallimenti del mercato.

Nello scenario attuale, dunque, le singole discipline non agiscono più in maniera isolata, ma si pongono in un rapporto di integrazione positiva, al fine di garantire mercati aperti e competitivi, tutelando al contempo la libertà di autodeterminazione dei singoli cittadini.

Riferimenti bibliografici

- I.M. ALAGNA, N. CENTOFANTI (2021), *La consumerizzazione della privacy tra California Consumer Privacy Act e GDPR*, in L. Bolognini (a cura di), "Privacy e libero mercato digitale", Giuffrè, 2021
- AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2020), *Indagine conoscitiva sui Big Data*, 2020
- V. BAGNOLI (2016), *The Big Data Relevant Market*, in "Concorrenza e Mercato", 2016, n. 1
- E. BATTELLI (2024), *La giustizia predittiva nella twin transition*, in "Tecnologie e Diritto", 2024, n. 2
- E. BATTELLI (2022-A), *I modelli negoziali di business degli operatori digitali a "prezzo zero" non sono "gratuiti"*, in "I Contratti", 2022, n. 3
- E. BATTELLI (2022-B), *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in "Rivista di diritto di famiglia e delle persone", 2022, n. 3
- E. BATTELLI (2022-C), *Negoziabilità dei dati come strumento di regolazione del mercato e di protezione della persona utente di servizi digitali*, in "Rivista di diritto dell'impresa", 2022, n. 1
- C. CASONATO (2019), *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in "Diritto pubblico comparato europeo", Numero speciale, 2019
- C. COLAPIETRO (2021), *Circolazione dei dati, automatizzazione e regolazione*, in "Osservatorio sulle fonti", 2021, n. 2
- C. 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
- E. CREMONA (2021), *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione anti-trust*, in "Osservatorio sulle fonti", 2021, n. 2
- V.V. CUOCCI (2024), *Persone vulnerabili e scelte (in)consapevoli: riflessioni su neuromarketing e protezione dei dati personali nell'era dell'intelligenza artificiale*, in S. Orlando (a cura di), "Profili giuridici del neuromarketing", Sapienza University Press, 2024
- G. DE GREGORIO (2022), *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022
- A. DE MAURO, M. GRECO, M. GRIMALDI (2016), *A Formal Definition of Big Data Based on its Essential Features*, in "Library Review", vol. 65, 2016, n. 3

73. Sul punto ERRIGO 2023, p. 79.

- G. D'IPPOLITO (2022), *Monetizzazione, patrimonializzazione e trattamento dei dati personali*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022
- F. DI PORTO (2016), *La rivoluzione dei big data, un'introduzione*, in "Concorrenza e Mercato", 2016, n. 1
- E. ERRIGO (2023), *Sulle nuove libertà economiche. Criticità e prospettive del mercato digitale tra concorrenza, nuovi beni e autonomia negoziale*, in "Diritto Costituzionale", 2023, n.1
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2019-A), *Discorso di apertura dei lavori del Presidente Antonello Soro*, in "I Confini del Digitale. Nuovi scenari per la protezione dei dati" (Roma, 29 gennaio 2019), 2019
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2019-B), *L'universo dei dati e la libertà della persona*, Relazione 2018, 7 maggio 2019
- V. MAYER-SCHÖNBERGER, K. CUKIER (2013), *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Eamon Dolan, 2013
- OECD (2025), *Artificial intelligence and competitive dynamics in downstream markets*, in "OECD Roundtables on Competition Policy Papers", OECD Publishing, 14 novembre 2025
- OECD (2016), *Big Data: Bringing Competition Policy to the Digital Era*, OECD Publishing, 30 settembre 2016
- V. PAGNANELLI (2022), *Una "valutazione d'impatto della privacy delle Big Tech". Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. Cremona, F. Laviola, V. Pagnanelli (a cura di), "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022
- M.G. PELUSO (2023), *Intelligenza artificiale e tutela dei dati*, Giuffrè, 2023
- S. PERUGINI (2025), *L'AGCM di fronte all'intelligenza artificiale*, in M. Rabitti, F. Bassan (a cura di), "L'applicazione dell'IA Act in Italia e la tutela del consumatore", Roma TrE-Press, 2025
- G. PITRUZZELLA (2016), *Big Data, Competition and Privacy. A Look From the Antitrust Perspective*, in "Concorrenza e Mercato", 2016, n. 1
- S. RODOTÀ (2014), *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014
- P. STAAB (2024), *Markets and Power in Digital Capitalism*, Manchester University Press, 2024
- P. STONE, R. CALO, R. BROOKS et al. (2016), *Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence*, Stanford University Press, 2016
- S. TORREGIANI (2023), *Il Data Act: una versione europea del Data Nationalism?*, in "Rivista italiana di informatica e diritto", 2023, n. 2
- I. WIGMORE (2023), *Definition of Black Box IA*, in "Whatls.com", 2023
- S. ZUBOFF (2019), *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Public Affairs, 2019



ELISA SORRENTINO – ANNA FEDERICA SPAGNUOLO

Cybersecurity e sovranità digitale: un modello normativo integrato

La trasformazione digitale ha riconfigurato il cyberspazio da infrastruttura tecnica a dominio funzionale dell'esercizio dei poteri pubblici e della tutela dell'interesse generale. La cybersecurity costituisce il presupposto operativo dell'ordinamento digitale e l'unico ambito dotato di una disciplina vincolante, su cui può svilupparsi una governance della sovranità digitale, ancora priva di tipizzazione giuridica e affidata a strumenti di soft law. Il lavoro analizza le principali fonti nazionali ed europee in materia di cybersicurezza e propone un modello regolatorio integrato che, attraverso parole chiave strategiche, traduce la sovranità digitale in principio giuridico operativo, intrecciando protezione delle infrastrutture con la tutela dei diritti fondamentali e il governo dell'ecosistema digitale, nell'ottica di un quadro normativo armonizzato, resiliente e multilivello.

Cybersecurity – Sovranità Digitale – Governance integrata – Diritti fondamentali

Cybersecurity and digital sovereignty: An integrated regulatory model

The digital transformation has reconfigured cyberspace from a technical infrastructure into a functional domain of the exercise of public powers and the protection of the general interest. Cybersecurity constitutes the operational premise of the digital legal order and the only domain endowed with a binding regulatory discipline, upon which a broader governance of digital sovereignty can be built, a concept still lacking legal typification and largely entrusted to soft law instruments. The paper analyzes the main national and European sources on cybersecurity and proposes an integrated regulatory model that, through strategic keywords, translates digital sovereignty into an operative legal principle, intertwining the protection of infrastructures with the safeguarding of fundamental rights and the governance of the digital ecosystem, with the objective of building a harmonized, resilient and multilevel legal framework.

Cybersecurity – Digital sovereignty – Integrated governance – Fundamental rights

A.F. Spagnuolo è tecnologo, E. Sorrentino è CTER presso l'Istituto di Informatica e Telematica del CNR, Sede di Cosenza

Questo lavoro è il risultato di una ricerca comune e condivisa condotta da entrambe le Autrici ed è stato parzialmente realizzato nell'ambito delle attività del progetto "Security and Rights in the CyberSpace – SERICS (PE00000014)" – Piano Nazionale di Ripresa e Resilienza MUR finanziato dall'Unione Europea – NextGenerationEU, CUP B53C22003950001

SOMMARIO: 1. Introduzione. – 2. Oltre la cybersecurity: verso una governance digitale multilivello per la sovranità digitale europea. – 3. Mappatura e classificazione delle fonti giuridiche e strategiche della cybersicurezza e della sovranità digitale. – 4. Parole chiave per una governance europea della sovranità digitale. – 5. Conclusioni.

1. Introduzione

La progressiva digitalizzazione delle strutture economiche, amministrative e sociali ha profondamente riconfigurato gli equilibri istituzionali e giuridici, trasformando il cyberspazio da semplice infrastruttura tecnica a luogo strategico per l'esercizio del potere sovrano. In questo scenario, i concetti di cybersecurity¹ e sovranità digitale², sebbene distinti sotto il profilo definitorio, assumono un ruolo centrale, configurandosi come chiavi interpretative dell'intersezione tra tecnologia e diritto nell'ecosistema digitale. L'attuale eterogeneità del quadro normativo, a livello tanto sovranazionale quanto statale, introduce significative discontinuità nella governance cibernetica, incidendo sul coordinamento e sull'effettività delle strategie di protezione delle infrastrutture e delle risorse digitali³. In questo contesto frammentato si colloca il nodo teorico centrale: la mancanza di un impianto ermeneutico adeguatamente strutturato, capace di sistematizzare in modo coerente le molteplici e crescenti articolazioni della sovranità digitale. Il presente lavoro si colloca in tale vuoto normativo e concettuale, proponendo un avanzamento metodologico che, attraverso un modello olistico, mira

a ricondurre principi, funzioni e strumenti entro un'unica architettura teorica coerente.

Le fasi di mappatura e di classificazione integrata delle fonti costituiscono il presupposto metodologico di quello che definiremo modello normativo integrato, finalizzato a supportare un'organizzazione coerente dei documenti giuridico-politici più rilevanti. Questo processo analitico permette di identificare parole chiave strategiche, che agiscono come strumenti concettuali capaci di tradurre in termini concreti e operativi il concetto di sovranità digitale, fornendo una chiave interpretativa sistemica di fronte alle sfide emergenti. L'approccio proposto rappresenta l'originalità metodologica del contributo, integrando la semantica normativa nell'ordinamento digitale e delineando una visione multidimensionale della sovranità digitale, la cui articolazione dettagliata è sviluppata nei paragrafi che seguono.

2. Oltre la cybersecurity: verso una governance digitale multilivello per la sovranità digitale europea

Nell'attuale panorama digitale, la cybersecurity rappresenta un fondamento operativo imprescindibile per la protezione delle infrastrutture critiche e dei

1. Per un'analisi del concetto di cybersecurity, TADDEO 2019; ZICCARDI 2019; BRIGHI–CHIARA 2021; NATIONAL CYBER SECURITY CENTRE 2024.

2. Per una panoramica della letteratura in tema di sovranità digitale si rinvia all'analisi di HUMMEL–BRAUN–TRETTER–DABROCK 2021. Gli autori passano in rassegna oltre seicento articoli in materia e identificano sei differenti nozioni di sovranità. Si veda ancora HELLMEIER–VON SCHERENBERG 2023. Sulla polisemia dell'espressione *sovranità digitale* si veda, inoltre, MOEREL–TIMMERS 2021. Sul punto BIN 2013. Si veda ancora SIMONCINI 2017.

3. ROBERTS–COWLS–CASOLARI et al. 2021.

dati, costituendo il primo baluardo contro minacce informatiche e vulnerabilità sistemiche⁴. L'evoluzione della società digitale, tuttavia, impone l'adozione di un approccio proattivo che superi una logica meramente difensiva, affermando il principio di sovranità digitale⁵, inteso come la capacità condivisa degli Stati e delle istituzioni europee di governare i propri dati, le infrastrutture e le regole dell'ecosistema digitale, promuovendo al contempo forme di maggiore tutela e coordinamento con gli attori privati e sovranazionali. La sovranità digitale, tuttavia, si configura ancora come una costruzione politica in divenire, priva di una cornice giuridica condivisa e vincolante a livello europeo. È proprio questa ambiguità⁶ a renderne urgente una profonda riconfigurazione teorica e normativa, capace di ancorarla ai valori fondamentali dell'Unione europea per generare un ecosistema digitale resiliente, democratico e orientato al bene comune⁷. Il passaggio dalla cybersecurity alla sovranità digitale non si configura come un mero ampliamento di ambiti materiali, ma come una trasformazione qualitativa del modo

stesso di concepire l'intervento pubblico nello spazio digitale: da funzione prevalentemente reattiva a governance strutturale, multilivello e strategica del cyberspazio⁸. Tale evoluzione impone una revisione dei presupposti teorici tradizionali, non più adeguati a descrivere l'interdipendenza tra infrastrutture, dati, potere regolatorio e diritti fondamentali⁹ nello spazio digitale¹⁰. Lungi dal sostituirsi alla cybersecurity, la sovranità digitale ne integra e amplia i presupposti, delineando una visione del digitale in cui la protezione dei sistemi si intreccia con la valorizzazione dei principi e delle libertà costituzionali¹¹. Del resto, in un contesto geopolitico profondamente mutato, caratterizzato da tensioni globali, interdipendenze tecnologiche e competizione per il controllo dei dati e delle infrastrutture strategiche, la capacità degli Stati e delle istituzioni europee di esercitare una politica digitale efficace assume una rilevanza cruciale, non solo ai fini della tutela della sicurezza nazionale e della resilienza economica¹², ma anche quale elemento per preservare l'autonomia strategica in un mondo sempre più interconnesso. La crescente dipendenza

4. Si veda GUARDA 2008; FAINI 2018; BRIGHI-CHIARA 2021; DI CORINTO 2022; PONTI 2024; RESTA 2024.

5. Si veda CARDONE 2025.

6. PALLADINO 2023. L'esigenza di definire in modo preciso ed entro parametri normativi ben delineati il concetto di sovranità digitale nasce proprio dall'ambiguità che questo termine porta con sé e dalle conseguenze che genera. Infatti, come evidenzia Palladino la nozione di sovranità nel cyberspazio si presenta intrinsecamente ambivalente: da un lato, si rifà alla tradizionale sovranità territoriale, che attribuisce agli Stati controllo esclusivo su infrastrutture e dati all'interno dei confini nazionali; dall'altro lato, emerge una concezione post-territoriale che sposta il quadro verso autonomia e potere di governo sui flussi digitali indipendentemente dal territorio fisico. Questa doppia interpretazione determina tensioni normative e geopolitiche, sovrapposizioni e conflitti di giurisdizione, confermando quanto sia necessario stabilire definizioni chiare e condivise per evitare derive e ambiguità nel governo del cyberspazio.

7. RODOTÀ 2021.

8. Si veda SANTANIELLO 2022, che evidenzia come la sovranità digitale sia una risposta strategica alle sfide poste dalla globalizzazione delle tecnologie e dalla necessità di tutelare i diritti digitali fondamentali. Si veda ancora SORRENTINO-SPAGNUOLO 2024, che sottolineano la necessità di implementare misure legislative che garantiscano la sicurezza delle infrastrutture e dei dati, nel pieno rispetto dei diritti fondamentali, evidenziando la sovranità digitale come nuova frontiera della governance statale sulle risorse critiche digitali. Si veda ancora DE ROSA 2021; GATTI 2019.

9. MANGIAMELI 2023; CUSTERS 2022.

10. LONGO 2023.

11. SPINIELLO 2025, che esamina come il costituzionalismo digitale, inteso come radicamento dei diritti e principi costituzionali nel contesto digitale, starebbe evolvendo insieme all'idea di sovranità digitale nell'Ue e negli ordinamenti nazionali.

12. In questo scenario, la regolazione della datasfera, intesa come lo spazio digitale dove si generano, transitano e si accumulano dati, diventa "una delle nuove frontiere del potere statale, che si esercita su una dimensione immateriale ma non per questo meno strategica". Si veda ZENO-ZENCOVICH 2018.

da soluzioni tecnologiche sovranazionali aumenta l'esposizione di governi, imprese e cittadini a rischi rilevanti, tra cui violazioni dei dati personali, attacchi a settori critici (energia, trasporti, sanità), squilibri informativi e concentrazioni monopolistiche¹³. Un governo responsabile e consapevole dell'ecosistema digitale richiede, dunque, l'elaborazione di un quadro teorico integrato, ancora mancante, e la definizione di un modello normativo organico, in grado di armonizzare norme e regole tecniche e di dare piena attuazione al principio di sovranità digitale. Nonostante il progressivo rafforzamento del quadro regolatorio europeo e nazionale, permane difatti un

divario significativo. Mentre la cybersecurity dispone ormai di un impianto normativo rafforzato, la sovranità digitale resta ancora affidata prevalentemente a strumenti di soft law¹⁴, linee guida e dichiarazioni politiche non vincolanti¹⁵ che riflettono la complessità e la mutevolezza delle trasformazioni in atto¹⁶. Questa asimmetria non costituisce un mero squilibrio tecnico, ma segnala l'assenza di una grammatica normativa comune, capace di integrare le diverse dimensioni dell'ordinamento digitale segnato tuttora da una serie di interventi settoriali e privi di un disegno unitario¹⁷ capace di assicurarne la coerenza complessiva (a titolo esemplificativo: tutela dei

13. In altri termini la protezione dei dati personali assume ormai una dimensione transnazionale, nella quale “gli ordinamenti nazionali appaiono spesso inadeguati a fronteggiare le sfide poste dalla globalizzazione digitale”. Si veda RESTA-ZENO-ZENCOVICH 2016.
14. I principali riferimenti sono: Commissione europea, *Analisi comparativa dei progressi dell'iniziativa eEurope 2002*, 5 febbraio 2002, doc. COM (2002) 62; Comitato delle Regioni, *Parere sulla Comunicazione della Commissione – Sicurezza delle reti e sicurezza dell'informazione: Proposta di un approccio strategico europeo*, 3 maggio 2002; Commissione europea, *Comunicazione sulla strategia dell'UE per l'Unione della sicurezza*, 24 luglio 2020, doc. COM (2020) 605; Consiglio dell'Unione europea, *Conclusioni del Consiglio – Plasmare il futuro digitale dell'Europa*, 9 giugno 2020; Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi*, 2 dicembre 2020; Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale*, 22 marzo 2021; Consiglio dell'Unione europea, *Conclusioni del Consiglio – Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio*, 8 ottobre 2021; Commissione europea, Alto Rappresentante dell'Unione, *Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale*, 2021, doc. JOIN (2021) 14; Parlamento europeo, *Risoluzione sulla strategia UE per la cibersicurezza*, 10 giugno 2021, doc. 2020/2667(RSP); Consiglio dell'Unione europea, *Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica*, 23 maggio 2022; Consiglio dell'Unione europea, *Conclusioni del Consiglio su un quadro per una risposta coordinata dell'UE alle campagne ibride*, 2022; Consiglio dell'Unione europea, *Conclusioni del Consiglio sulla sicurezza delle catene di approvvigionamento delle TIC*, 17 ottobre 2022; Commissione europea, *European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers*, 15 gennaio 2024.
15. Tra i documenti non vincolanti vi sono: Von der Leyen U., *Discorso sullo stato dell'Unione*, Parlamento europeo, Strasburgo, 16 settembre 2020, doc. SPEECH/20/1655; Ministri UE e EFTA, *Tallinn Declaration on eGovernment*, Conferenza ministeriale sull'eGovernment, Tallinn, 6 ottobre 2017; Merkel A., *Speech at the Annual Meeting of the World Economic Forum*, Davos, 23 gennaio 2020; Macron E., intervento a VivaTech, Parigi, 16-19 giugno 2021. Il discorso di Von der Leyen (2020), pur rilevante per aver posto in primo piano l'autonomia tecnologica dell'Unione europea e la necessità di una maggiore sovranità digitale rispetto agli Stati Uniti e alla Cina, non ha la forza di un atto normativo. Allo stesso modo, anche la Dichiarazione di Tallinn (2017), pur sottolineando l'importanza della sicurezza cibernetica e dell'autonomia digitale, non crea obblighi legali per gli Stati membri.
16. Lo sviluppo tecnologico delle società contemporanee ha avuto un notevole impatto sulle figure giuridiche tradizionali e sulla identificazione di nuovi diritti. Si veda a tal proposito FARALLI 2018.
17. Le principali normative sovranazionali sull'argomento includono: Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA); Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004; Accordo interistituzionale tra il Parlamento europeo, il Consiglio

dati personali, identità digitale¹⁸, mercato unico¹⁹, sicurezza informatica²⁰ e contrasto al cybercrime²¹).

dell'Unione europea e la Commissione europea per l'istituzione di una squadra di pronto intervento informatico (CERT-UE) permanente, 2018; Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

18. Le principali normative sovranazionali sull'argomento includono: 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 (eIDAS); 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 (GDPR); Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa 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; Regolamento (UE) 2021/1232 del Parlamento europeo e del Consiglio, del 14 luglio 2021, relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE ai fini della lotta contro gli abusi sessuali online sui minori; Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati (Data Governance Act); 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 (Data Act); EDPB, *Guidelines 9/2022 on personal data breach notification under GDPR*, Version 2.0, adottate il 28 marzo 2023; Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act).
19. Le principali normative sovranazionali sull'argomento includono: Direttiva 90/387/CEE del Consiglio, del 28 giugno 1990, sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni; Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (ePrivacy); Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche; Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale (Digital Markets Act – DMA); Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali (Digital Services Act – DSA).
20. Le principali normative sovranazionali sull'argomento includono: Commissione europea, Alto Rappresentante dell'Unione, *Strategia dell'Unione europea per la cybersicurezza: un ciberspazio aperto e sicuro*, 7 febbraio 2013, doc. JOIN (2013) 1, Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS1); Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, 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 (Cybersecurity Act); Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione (NIS2); Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario (DORA); Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio; Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, recante misure per un livello comune elevato di cybersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione; Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali (Cyber Resilience Act).
21. Le principali normative sovranazionali sull'argomento includono: 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; Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento,

Sebbene la competenza sovrana sulle infrastrutture e sulla sicurezza²² resti formalmente attribuita agli Stati membri, l'Unione europea esercita un ruolo di coordinamento strategico che ne rivela l'intrinseca ambivalenza, non una mera armonizzazione tecnica ma autentica riconfigurazione del locus del potere sovrano nello spazio digitale. Iniziative come la *Bussola Digitale 2030*²³ tracciano un orizzonte normativo volto alla costruzione di un ecosistema digitale resiliente, etico e competitivo, ma la loro efficacia rimane sospesa, perché la sovranità digitale europea esige non soltanto resilienza tecnica, ma anche una cooperazione fondata su fiducia ontologica tra gli Stati, interoperabilità strutturale e una governance partecipativa, capace di incarnare principi

fondamentali in pratiche operative evitando che essi si riducano a mera retorica istituzionale. Sul piano nazionale, questa dinamica genera una frattura concettuale profonda, poiché la tensione tra sovranità statale e imperativi europei non si limita a produrre frammentazione normativa, ma mette in luce la crisi ontologica del paradigma giuridico tradizionale, ormai incapace di integrare coerentemente la *datasfera* con valori costituzionali e diritti fondamentali²⁴. La digitalizzazione, infatti, erode la storica territorialità della sovranità, rivelando l'insufficienza dei modelli statocentrici di fronte a flussi transnazionali di dati e infrastrutture interconnesse²⁵. Anche il nostro Paese, pur avendo adottato norme strategiche²⁶, recepito normative europee²⁷ e disposizioni

indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi; Direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio; Consiglio europeo, *Conclusioni del Consiglio europeo sulla rete giudiziaria europea per la criminalità informatica*, 2016; Consiglio europeo, *Conclusioni del Consiglio europeo sulle attività informatiche dolose*, 2018; Consiglio dell'Unione europea, *Quadro strategico dell'UE in materia di ciberdifesa*, aggiornamento 2018.

22. Parlamento europeo, *Lo Stato di diritto nell'ordinamento giuridico dell'Unione europea*, EPRS/Servizio Ricerca del Parlamento europeo, PE 745.685, luglio 2023. Questo studio è parte di un progetto più ampio di diritto comparato. Analizza il principio dello Stato di diritto come valore fondamentale dell'Unione europea, sancito nel Trattato sull'Unione Europea (TUE) e declinato in numerose fonti normative vincolanti e non vincolanti. Il documento illustra i meccanismi preventivi e repressivi volti a garantire il rispetto dello Stato di diritto da parte degli Stati membri, inclusa la procedura prevista dall'articolo 7 TUE in caso di violazioni gravi. Viene inoltre evidenziata la complessità semantica della nozione di Stato di diritto e le prospettive di sviluppo legate a una sua interpretazione evolutiva. Lo studio sottolinea come il rispetto dello Stato di diritto sia intrinsecamente connesso alla democrazia e ai diritti fondamentali, garantendo che tutti i poteri pubblici operino entro i limiti della legge, sotto il controllo di organi giurisdizionali indipendenti e imparziali. Inoltre, la relazione annuale della Commissione europea sullo Stato di diritto (2023) fornisce una valutazione aggiornata della situazione nei singoli Stati membri, evidenziando le sfide e le misure adottate per assicurare il rispetto del principio nei diversi ordinamenti nazionali (Commissione europea, *Relazione annuale sullo Stato di diritto 2023*, Bruxelles, 5 luglio 2023, doc. SWD (2023) 812). Per approfondimenti si veda CRESPI 2024.
23. Commissione europea, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, Bruxelles, 9 marzo 2021, doc. COM (2021) 118.
24. Si veda CATANZARITI 2024; DE GREGORIO–RADU 2022.
25. PIERUCCI 2025; CHANDER–SUN 2023.
26. In Italia, le principali norme di indirizzo strategico includono: Presidenza del Consiglio dei Ministri, D.P.C.M. 24 gennaio 2013, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*; mPresidenza del Consiglio dei Ministri, D.P.C.M. 17 febbraio 2017, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*.
27. Le principali norme italiane di recepimento direttive e regolamenti europei: Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione; Decreto legislativo 8 novembre 2021, n. 207, Norme di attuazione del regolamento (UE) 2019/881 relativo all'ENISA e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (Cybersecurity

trasversali²⁸, definito assetti organizzativi e istituzionali²⁹, resta intrappolato in una frammentazione strutturale che rivela l'insufficienza esistenziale degli approcci settoriali e la mancanza di un coordinamento efficace sin dalla fase progettuale.

3. Mappatura e classificazione delle fonti giuridiche e strategiche della cybersicurezza e della sovranità digitale

Alla luce delle criticità concettuali e normative fin qui analizzate, si è ipotizzata la costruzione di un modello normativo integrato per la gestione regolatoria della sicurezza cibernetica e della sovranità digitale. Tale modello funge da strumento operativo capace di tradurre la sovranità digitale da mera nozione teorica a principio giuridico pienamente efficace. La sua definizione presuppone una cornice metodologica rigorosa, volta a garantire coerenza concettuale, concretezza normativa e replicabilità analitica, superando le discontinuità generate dalla frammentazione regolatoria vigente. Il percorso metodologico si sviluppa in due momenti sequenziali e complementari: una prima fase di mappatura sistemica delle fonti normative e strategiche, seguita da una fase di classificazione interpretativa. La trasparenza e la chiarezza dei criteri organizzativi assicurano la replicabilità del metodo e ne consolidano il valore come strumento per l'elaborazione di soluzioni regolatorie innovative. La

selezione delle fonti ha privilegiato atti dotati di efficacia giuridica vincolante o di comprovata rilevanza strategica per la definizione delle politiche digitali a livello europeo e nazionale, delineando un corpus analitico coerente. Documenti settoriali o atti tecnici di peso normativo limitato sono stati esclusi, al fine di concentrare l'analisi su strumenti capaci di orientare concretamente le scelte regolatorie e di costituire un fondamento solido per il modello stesso. L'approccio metodologico è dinamico e multilivello, in grado di integrare prospettive differenti e di far emergere interdipendenze, priorità strategiche e relazioni tra norme e principi. In questo quadro, la mappatura svolge la funzione di fondamento analitico, fornendo le basi per l'elaborazione di modelli giuridici coerenti, integrati e resilienti, in grado di tradurre concetti complessi in strumenti operativi concretamente applicabili. La successiva fase di classificazione interpretativa si muove lungo due binari complementari. Il primo raggruppa tre categorie tematiche: rischio, minacce e attori coinvolti, al fine di cogliere la logica sostanziale sottesa alle norme. Il secondo si fonda sul rango giuridico e sulla natura delle fonti, graduando l'influenza delle diverse disposizioni e consentendo di ricostruire gerarchie, interazioni e relazioni di forza tra strumenti normativi. Nel dettaglio, il procedimento di mappatura e analisi si è concretizzato in tre passaggi distinti: (1)

Act); Decreto legislativo 4 settembre 2024, n. 134, Attuazione della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, in GU Serie Generale n. 223 del 23 settembre 2024; Decreto legislativo 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

28. In Italia, le principali norme complementari e trasversali sono: Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, come modificato dal decreto legislativo 10 agosto 2018, n. 101; Decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (CAD); Legge 28 giugno 2024, n. 90, Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici; AGID, *Piano triennale per l'informatica nella Pubblica Amministrazione 2024-2026*, Roma, 2024; AGID, *Linee guida per l'adozione di intelligenza artificiale nella pubblica amministrazione*, Versione 1.0, 14 febbraio 2025 (in consultazione).
29. Le principali norme organizzative e istitutive italiane sono: Decreto-legge 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (PSNC); Legge 18 novembre 2019, n. 133, Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica; Presidenza del Consiglio dei Ministri, D.P.C.M. 30 luglio 2020, n. 131, Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105; Decreto-legge 14 giugno 2021, n. 82, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

identificazione e selezione delle fonti pertinenti; (2) estrazione delle componenti semantiche rilevanti; (3) aggregazione delle ricorrenze all'interno di una tassonomia tematico giuridica. Pur caratterizzato da sistematicità e rigorosità, il metodo riconosce un limite intrinseco nella continua evoluzione del quadro regolatorio e strategico che mantiene inevitabilmente aperto il perimetro delle fonti, richiedendo aggiornamenti e interpretazioni costanti.

Sulla base della classificazione interpretativa, il corpus delle fonti è stato organizzato secondo una partizione funzionale che distingue due ambiti principali: da un lato, le fonti relative alla cybersicurezza, focalizzate sulla protezione di dati, sistemi e infrastrutture critiche; dall'altro, le fonti pertinenti alla sovranità digitale, orientate all'autonomia strategica e al controllo delle tecnologie e dei flussi informativi. Questa distinzione non mira a separare rigidamente le due dimensioni, ma a facilitare l'analisi delle interdipendenze tra sicurezza

e governance digitale, evidenziando come scelte normative apparentemente settoriali contribuiscano a costruire un quadro unitario di sovranità digitale e resilienza cibernetica. La classificazione interpretativa, articolata lungo i due assi analitici precedentemente delineati, consente di scomporre la complessità del sistema regolatorio in componenti strutturate e interconnesse, offrendo una visione sistemica anche in contesti ad alta densità normativa³⁰. In questo quadro, le tre categorie tematiche – rischio³¹, minaccia³² e attori³³ – assumono il ruolo di chiavi interpretative trasversali, capaci di collegare la dimensione tecnica a quella normativa e di trasformare concetti astratti in criteri analitici. In particolare, la categoria del rischio assume un ruolo centrale, identificando vulnerabilità³⁴ e orientando interventi normativi mirati alla tutela delle infrastrutture, dei dati personali e della privacy degli utenti. Si tratta di un criterio dinamico, capace di guidare proporzionalità,

30. SORRENTINO-SPAGNUOLO 2024.

31. In un ecosistema digitale estremamente complesso e in rapida trasformazione è fondamentale adottare approcci dinamici e adattivi per valutare il rischio cyber. La continua evoluzione delle minacce e delle tecnologie richiede di "ricostruire i contorni" di questo ecosistema in modo continuo, per comprendere le interdipendenze tra gli asset digitali, le nuove vulnerabilità e le superfici di attacco emergenti. Solo con una visione sistemica e aggiornata è possibile garantire efficacemente la sicurezza e la resilienza delle infrastrutture digitali. Si veda COMMISSIONE EUROPEA 2024. Il report della Commissione europea (2024) mette in evidenza come la sovranità digitale nell'Unione europea richieda una comprensione profonda e aggiornata dell'intero ecosistema digitale, caratterizzato da continui cambiamenti tecnologici, geopolitici e di minacce informatiche. Per garantire l'autonomia strategica e la sicurezza, è fondamentale ricostruire in modo dinamico e costante i contorni di questo ecosistema, identificando nuove vulnerabilità, rischi emergenti e interdipendenze critiche tra infrastrutture, fornitori e tecnologie. Questa necessità nasce dall'evoluzione continua delle tecnologie digitali e dalle minacce sofisticate che mettono a rischio la resilienza e la protezione degli asset digitali europei. In particolare, il report insiste sull'importanza di adottare strategie flessibili, cicliche e sistemiche di valutazione e gestione dei rischi, così da mantenere un controllo efficace sulla complessità in rapido mutamento dell'ecosistema digitale.

32. Nel contesto della governance digitale, il concetto di minaccia si riferisce alle evoluzioni continue delle minacce informatiche sofisticate, che caratterizzano l'ecosistema digitale in rapido mutamento, richiedendo strategie di monitoraggio dinamico per identificare interdipendenze critiche e superfici di attacco emergenti. Si veda a tal proposito ABO MHARA-ABDULRAHMAN-BAROUD 2024; EL-SHROUK 2023; AHMED 2022.

33. La categoria degli attori nella governance digitale si articola in un modello multistakeholder inclusivo, comprendente governi, imprese, associazioni non governative, istituti di ricerca, organizzazioni intergovernative, società civile, cittadini e altri stakeholder, i quali collaborano in modo condiviso per definire policy digitali evolute. Tale approccio decentralizzato e privo di gerarchie rigide integra enti pubblici come Agenzia per l'Italia Digitale (AgID), Agenzia per la Cybersicurezza Nazionale (ACN) e Garante privacy, oltre a figure professionali dedicate alla transizione digitale. Si veda BALDAZZINI-BOTTOS-DANNA et al. 2024; PLIAUŠKAITĖ 2024; MILLARD 2023.

34. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024. July 2023 to June 2024*. Il rapporto fornisce un'analisi dettagliata delle minacce emergenti nel panorama europeo, sottolineando la natura dinamica e interconnessa delle minacce cyber, e la necessità di un approccio integrato per la loro gestione.

adeguatezza e responsabilità dell'azione normativa; in tal senso il General Data Protection Regulation (GDPR)³⁵ rappresenta un riferimento paradigmatico, collegando sicurezza dei dati, valutazione del rischio e responsabilità normativa³⁶. La categoria della minaccia costituisce la materializzazione operativa del rischio, includendo eventi dannosi, dolosi o accidentali, interni o esterni, che possono compromettere l'integrità, la disponibilità o la riservatezza dei sistemi. L'analisi delle minacce evidenzia la necessità di strumenti normativi flessibili e adattabili, in grado di rispondere alla natura mutevole degli attacchi. Infine, la categoria degli attori consente di comprendere la distribuzione policentrica delle responsabilità, evidenziando come ruoli e competenze siano intrecciati a livello nazionale, sovranazionale e transnazionale. Il livello giuridico, diversamente dalle categorie tematiche che collegano la logica sostanziale delle norme, si concentra sull'ordinamento sistematico delle fonti secondo la loro forza cogente e il potenziale impatto strategico. Questo approccio permette di distinguere con chiarezza le fonti che, pur differenziandosi per grado di vincolatività, contribuiscono in maniera determinante a regolare e orientare le politiche digitali³⁷, offrendo un quadro coerente e integrato per l'interpretazione e l'applicazione delle norme. Nella fase applicativa, la distinzione tra forza giuridica formale e impatto sostanziale è stata applicata in modo sistematico alla classificazione delle fonti. Le fonti vincolanti (regolamenti, direttive e norme primarie) sono state identificate come strumenti dotati di potere cogente immediato, capaci di orientare direttamente le politiche pubbliche. In parallelo, i documenti di soft law, comprese strategie, linee guida e dichiarazioni

politiche, sono stati considerati fonti a impatto sostanziale, il cui valore risiede nella capacità di indirizzare decisioni regolatorie, modellare comportamenti istituzionali e orientare l'interpretazione delle norme cogenti. Questa doppia lettura consente di costruire una mappa normativa multi-livello, in cui forza formale e influenza sostanziale delle fonti vengono trattate come variabili interconnesse. Attraverso questo approccio, il modello permette di mettere in relazione fonti eterogenee, evidenziando come norme vincolanti e indicazioni strategiche, pur differenziandosi per natura e grado di vincolatività, contribuiscano congiuntamente a definire un quadro unitario di sovranità digitale e resilienza cibernetica. In tale prospettiva, il panorama nazionale di cybersecurity e governance digitale si prospetta come un percorso evolutivo, in cui strumenti fondativi e interventi più recenti concorrono a delineare un'architettura regolatoria sempre più integrata e interconnessa, capace di coniugare coerenza normativa, tutela dei diritti fondamentali e orientamento strategico. A questo schema sistemico si innesta il complesso apparato normativo nazionale, in cui la legge 18 novembre 2019, n. 133³⁸, istitutiva del Perimetro di sicurezza nazionale cibernetica, assume il ruolo di fondamento strutturale, definendo responsabilità istituzionali, procedure di vigilanza e requisiti di protezione per reti, sistemi e servizi di rilevanza strategica. Su questa base si colloca il recepimento della Direttiva (UE) 2022/2555 (NIS2)³⁹, recepita con il d.lgs. 4 settembre 2024, n. 138⁴⁰, che estende la platea dei soggetti "essenziali" e "importanti", innalza gli standard di gestione del rischio, chiarisce il regime di responsabilità e abroga contestualmente il d.lgs. 65/2018⁴¹, attuativo della precedente

35. Regolamento (UE) 2016/679.

36. *Ibidem*. Si veda GONÇALVES 2019.

37. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024. July 2023 to June 2024*. Si veda ancora NODEHI-BERISHA-DA SILVA et al. 2024.

38. Legge 18 novembre 2019, n. 133.

39. Direttiva (UE) 2022/2555 (NIS2).

40. Decreto legislativo 4 settembre 2024, n. 138, Recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

41. Decreto legislativo 18 maggio 2018, n. 65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Direttiva NIS (UE) 2016/1148⁴², segnando il passaggio verso un modello regolatorio più ampio, uniforme e coordinato. In questa prospettiva, la NIS1 mantiene valore ricostruttivo quale primo tentativo europeo di armonizzazione in materia di sicurezza delle reti e dei sistemi informativi, ma è la NIS2 a determinare un effettivo salto qualitativo, rafforzando la resilienza digitale⁴³ complessiva e ponendo l'accento su interoperabilità, continuità operativa, coordinamento nella gestione degli incidenti⁴⁴ e omogeneità degli standard nazionali, in un'ottica di coesione tra gli Stati membri e di consolidamento della capacità di risposta comune. Parallelamente, la legge 23 settembre 2025, n. 132⁴⁵, in armonia con il Regolamento UE 2024/1689 (AI Act), istituisce un quadro organico per l'intelligenza artificiale, attribuendo all'Agenzia per l'Italia Digitale (AgID) e all'Agenzia per la Cybersicurezza Nazionale (ACN) compiti precisi di vigilanza, autorizzazione, monitoraggio e sanzione degli usi dell'intelligenza artificiale, con particolare attenzione a sicurezza, trasparenza, tutela dei diritti fondamentali e protezione dei dati. L'insieme di queste norme testimonia come il sistema nazionale stia assumendo una configurazione integrata e stratificata, in cui la protezione delle infrastrutture critiche, la gestione dei rischi informatici e la regolazione delle tecnologie emergenti non siano

ambiti separati, ma componenti interconnesse di una governance digitale complessa.

Il livello giuridico internazionale costituisce la cornice entro cui le norme e gli standard acquisiscono forza e significato, delineando i confini entro cui le politiche nazionali possono essere coerentemente orientate. Standard riconosciuti globalmente, quali ISO/IEC 27001⁴⁶ e il NIST Cybersecurity Framework⁴⁷, svolgono una funzione metodologica di orientamento, definendo pratiche di gestione del rischio condivise e interoperabili. La versione 2.0 del NIST (2024), articolata nelle funzioni Governare, Identificare, Proteggere, Rilevare, Rispondere e Recuperare⁴⁸, offre una struttura flessibile, facilmente raccordabile tanto agli strumenti normativi vincolanti, quali regolamenti e direttive europee, quanto agli atti di soft law.

A tale dimensione si affianca il profilo dell'origine delle fonti e del loro impatto sistemico. L'impianto normativo europeo si struttura in atti sovranazionali che definiscono standard e logiche di intervento in materia digitale, cui si aggiungono strumenti nazionali che recepiscono e implementano le priorità europee, contribuendo alla costruzione di un quadro regolamentare sempre più coeso e integrato⁴⁹. L'analisi deve inoltre considerare l'influenza di iniziative come GAIA-X⁵⁰ e di fonti esterne all'ordinamento dell'Unione come

42. Direttiva (UE) 2016/1148.

43. European Union Agency for Cybersecurity, *ENISA Threat Landscape 2025, October 2025*.

44. La Direttiva NIS2 impone una governance strutturata e responsabilità dirette agli organi aziendali, spostando il baricentro della sicurezza cyber dal tecnico al gestionale, con l'obbligo di gestione agile, proattiva e trasparente del rischio informatico. Per approfondimenti si veda AGENDA DIGITALE 2025; ICT SECURITY MAGAZINE 2025; NETRIBE GROUP 2025; SS GROUP 2024.

45. Legge 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale.

46. ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), *Information Security Management Systems – Requirements* (ISO/IEC 27001:2022/Amd 1:2024), Geneva, February 2024.

47. National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024, ultima versione del Framework che aggiorna e rafforza l'approccio risk-based alla cybersecurity.

48. EDWARDS 2024.

49. European Commission 2025, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future*, COM (2025) 290, Brussels, 2025. Il Rapporto sottolinea l'importanza strategica della sovranità digitale e la necessità di una governance integrata a livello europeo. Tuttavia, rimangono rilevanti lacune normative e una predominanza di linee guida e strategie rispetto a norme vincolanti e armonizzate, riflettendo così lo stato ancora in evoluzione della disciplina.

50. European Cloud Federation 2022, *GAIA-X: A Federated Data Infrastructure for Europe*, Brussels, 2022. Progetto europeo per la creazione di un'infrastruttura cloud sicura e autonoma.

il Cloud Act statunitense⁵¹, che intervengono sulla definizione dei requisiti di sicurezza e sovranità dei dati, sull'elaborazione di standard di interoperabilità e sulle strategie di localizzazione, incidendo così sulla configurazione dello spazio europeo della sovranità digitale. Considerata nella sua interezza, questa complessa architettura dischiude un ordine normativo dinamico in cui le interazioni, le continuità e le tensioni tra i diversi piani non si risolvono in semplici sovrapposizioni, ma compongono un paradigma sistemico di natura evolutiva. In tale orizzonte, perfettamente coerente con l'impianto metodologico delineato, si manifesta la *ratio essendi* di un equilibrio rigoroso tra fonti cogenti, strumenti di soft law, vincoli giuridici e direttive strategiche.

4. Parole chiave per una governance europea della sovranità digitale

L'analisi metodologica condotta nei paragrafi precedenti, dalla mappatura sistematica delle fonti, alla classificazione interpretativa lungo assi tematici e giuridici, fino all'articolazione multilivello delle norme cogenti e degli strumenti di soft law, ha messo in luce la complessità e le interdipendenze dell'ecosistema normativo europeo e nazionale, offrendo le basi per la costruzione di un modello normativo integrato. Come abbiamo già osservato, mentre la cybersecurity è ampiamente regolamentata da un quadro normativo consolidato, la sovranità digitale, pur essendo al centro del dibattito politico e strategico europeo, rimane una nozione sfuggente, priva di un inquadramento normativo esaustivo che ne definisca chiaramente presupposti, finalità e implicazioni operative⁵². Da qui la necessità di isolare termini chiave capaci di sintetizzare la complessità del quadro regolatorio europeo e nazionale. Le parole chiave non sono semplici etichette ma rappresentano nodi concettuali, in cui si condensano principi, tensioni normative e orientamenti strategici, permettendo di tradurre la sovranità digitale da nozione teorica a strumento operativo. Proprio

l'assenza di una definizione unitaria, infatti, genera una frizione sistemica che ostacola l'armonizzazione delle discipline vigenti in materia di sicurezza informatica, protezione dei dati e governance delle infrastrutture critiche, complicando la gestione delle minacce digitali e rallentando l'emersione di un'autonomia tecnologica pienamente coerente con i principi del diritto internazionale⁵³. In questo contesto, l'individuazione dei termini ricorrenti si configura come esito naturale della metodologia comparativa e sistematica adottata divenendo uno strumento interpretativo capace di collegare l'elaborazione teorica alla prassi decisionale.

In particolare, la ricorrenza dei termini è stata accertata mediante un'analisi sistematica non solo quantitativa, ma anche qualitativa, capace di cogliere il loro peso semantico all'interno dei contesti d'uso. L'annotazione manuale, adottata come scelta metodologica consapevole, ha permesso di intercettare nessi concettuali, sfumature lessicali e impliciti normativi che gli strumenti automatizzati tendono a elidere, trasformando ciò che potrebbe apparire come un limite operativo in un vero punto di forza ermeneutico. La manualità, lungi dall'essere un retaggio pre-analitico, diviene la condizione previa, consentendo di valutare non soltanto che cosa ricorre, ma come e perché.

Dal processo analitico, così condotto, emergono tre assi interpretativi, capaci di chiarire la trama concettuale prevalente nelle fonti esaminate e di offrire chiavi di lettura stabili senza ridurre la complessità del fenomeno. La loro validità teorica è confermata dalla letteratura scientifica di settore che, pur non avendo orientato la selezione o condizionato la classificazione dei documenti, ha validato *a posteriori* i risultati ottenuti.

Si è definita come prima area concettuale quella della *Autonomia Tecnologica e della Resilienza Strategica*, comprendente termini quali "autonomia tecnologica", "resilienza" e "infrastrutture critiche". Tale area è rafforzata e valorizzata dalla Dichiarazione europea sui diritti e principi digitali⁵⁴, che

51. U.S. Congress 2018, *Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*, Pub. L. 115-141, Division V, 23 marzo 2018, Normativa statunitense che ha influenzato il dibattito europeo sulla protezione dei dati.

52. European Commission 2025, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future*, COM (2025) 290, Brussels, 2025.

53. GUERRA 2025.

54. Parlamento europeo, Consiglio europeo, Commissione europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, 2023/C 23/01. La Dichiarazione punta a stabilire un quadro costituzionale per la società

offre un quadro valoriale human-centric finalizzato a guidare l'attuazione dell'*open autonomy*⁵⁵ promosso dalla Commissione europea e riconosciuto nei principali documenti strategici comunitari.

La seconda area concettuale, denominata *Controllo Normativo e Infrastrutturale*, incorpora concetti quali "sicurezza cibernetica", "protezione dei dati" e "regolamentazione delle piattaforme digitali" riflettendo l'esigenza di strumenti giuridici chiari ed efficaci⁵⁶. La definizione di quest'asse segue l'evoluzione normativa europea (GDPR, DSA, DMA, NIS2), in cui la sovranità digitale si configura come capacità regolatoria dello Stato sulle architetture digitali, sui flussi informativi e sulle piattaforme medesime.

La terza area, infine, denominata *Diritti Fondamentali e Partecipazione Democratica*, include concetti come "diritti digitali", "giustizia algoritmica", "partecipazione democratica" e "solidarietà internazionale". Questa dimensione mette in evidenza l'intreccio tra politiche tecnologiche e valori costituzionali⁵⁷.

L'analisi sistematica delle parole chiave, organizzate nei tre assi interpretativi, non serve solo a chiarirne il significato lessicale, ma diventa uno strumento capace di interpretare e anticipare l'evoluzione del panorama normativo attorno al concetto di sovranità digitale. I termini emergenti funzionano come nodi concettuali in grado di svolgere una duplice funzione: chiariscono i

concetti e indicano i possibili sviluppi normativi, integrando sicurezza, autonomia tecnologica e tutela dei diritti traducendo un concetto frammentato e ambiguo in principio guida per una nuova architettura giuridica⁵⁸.

Attraverso questa prospettiva, il *Digital constitutionalism*⁵⁹ appare come il traguardo teleologico verso cui tende la regolazione della sovranità digitale. Non è una realtà già compiuta, ma un progetto normativo e istituzionale che trasla nell'ecosistema digitale i valori fondanti del costituzionalismo tradizionale (tutela dei diritti fondamentali, separazione dei poteri, limiti all'autorità e garanzie democratiche). In questo modo contribuisce a modellare strumenti, processi e responsabilità⁶⁰.

5. Conclusioni

L'analisi condotta ha evidenziato che per affrontare in modo efficace le sfide poste da un ecosistema digitale globale, in continua evoluzione e sempre più esposto a minacce informatiche sofisticate, è necessario un quadro giuridico solido, coerente e integrato. In tale contesto, la sistematizzazione delle fonti normative e l'individuazione di parole chiave strategiche non si configurano come un esercizio meramente classificatorio, ma divengono un passaggio interpretativo essenziale per guidare l'elaborazione di strategie normative in grado di coniugare sicurezza, innovazione e tutela dei diritti fondamentali. Il modello normativo integrato

digitale. Come altre iniziative simili, punta ad aggiornare le norme costituzionali per rispondere alle sfide imposte dalla rivoluzione digitale, mettendo in evidenza i diritti e i principi che devono guidare gli attori europei durante questa trasformazione.

55. Il concetto di *open strategic autonomy* è stato introdotto dalla Commissione europea nel 2021 nella *Trade Policy Strategy* per sottolineare la necessità di rendere l'apertura commerciale compatibile con la sua autonomia. Da giugno 2023 l'Ue si è concentrata sullo sviluppo di una *Economic Security Strategy*, al fine di integrare politiche economiche e commerciali incentrate sull'autonomia strategica aperta, sicurezza energetica ed economica, resilienza della catena di approvvigionamento agli shock esterni e riduzione del rischio.

56. FRATINI–HINE–NOVELLI et al. 2024. Il testo offre una mappatura critica dei diversi modelli di sovranità digitale (statale, dei diritti, di mercato), utile per situare il proprio modello interpretativo.

57. AMORETTI–SANTANIELLO 2024.

58. FLORIDI 2020. L'autore fornisce un approfondimento accademico sul ruolo della razionalizzazione normativa nella costruzione della sovranità digitale.

59. Il *Digital constitutionalism* può essere definito come un insieme di principi, strumenti e iniziative volti a trasferire i valori fondamentali del costituzionalismo nell'ambiente digitale, attraverso norme, codici, dichiarazioni e policy che organizzano la governance di Internet e delle infrastrutture digitali, pur senza costituire un corpus normativo unitario e codificato. Si veda a tal proposito CELESTE 2021; CELESTE 2019; REDEKER–GILL–GASSER 2018.

60. DE GREGORIO–RADU 2022.

articola la sovranità digitale lungo i tre assi interpretativi (Autonomia Tecnologica e Resilienza Strategica, Controllo Normativo e Infrastrutturale, Diritti Fondamentali e Partecipazione Democratica), da cui emergono le parole chiave come nodi concettuali che offrono una lente privilegiata per interpretare l'attuale quadro normativo e anticiparne le possibili evoluzioni, trasformando concetti frammentati in strumenti progettuali capaci di tracciare traiettorie normative future. La sovranità digitale, intesa come capacità di esercitare un controllo autonomo, responsabile e democraticamente legittimato sulle risorse digitali, costituisce la naturale evoluzione del paradigma della cybersecurity. Essa non si limita alla difesa da minacce esterne, ma si estende alla gestione proattiva di infrastrutture critiche, dati sensibili, algoritmi decisionali e piattaforme strategiche, assumendo una rilevanza

concreta e immediata nell'architettura costituzionale degli Stati e nell'equilibrio tra potere pubblico, mercato e cittadini. Il bilanciamento tra autonomia tecnologica, sicurezza cibernetica e tutela dei diritti fondamentali emerge come una delle sfide più complesse e decisive del nostro tempo, soprattutto in un contesto segnato da crescenti interdipendenze geopolitiche e da una competizione globale per il controllo delle tecnologie strategiche che rischiano di minare le basi del vivere democratico. La piena operatività di questo paradigma richiede il rafforzamento delle infrastrutture critiche, l'adozione di una cultura di responsabilità digitale e la promozione di trasparenza e inclusività regolativa guidando la costruzione di strumenti e processi volti ad armonizzare innovazione, sicurezza e protezione dei diritti fondamentali.

Riferimenti bibliografici

- M.A.O. ABO MHARA, A.A.A. ABDULRAHMAN, A.A.S. BAROUD (2024), *Cyber Attacks And Threats: Study Of The Types Of Cyber Attacks: Hacking, Viruses, Targeted Attacks, And Electronic Espionage*, in "The International Journal of Electrical Engineering and Sustainability (IJEES)", vol. 2, 2024, n. 4
- AGENDA DIGITALE (2025), *Nis2, come adeguarsi ai nuovi obblighi cyber: i punti chiave*, in "Agenda Digitale", 2025
- S. AHMED (2022), *A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age*, in "Journal of Cybersecurity & Information Management", vol. 10, 2022, n. 2
- F. AMORETTI, M. SANTANIELLO (2024), *Sovranità e costituzionalismo digitale*, in "Tecnologia, Politica, Società", 2024
- A. BALDAZZINI, G. BOTTOS, R. DANNA, E. DESIATA, F. NASI, O. PALMINI, A. VENIERI (2024), *La governance del digitale in Italia. Innovazione, democraticità e sviluppo sociale*, Nous Media, 2024
- R. BIN (2013), *La sovranità nazionale e la sua erosione*, in A. Pugiotto (a cura di), "Per una consapevole cultura costituzionale. Lezioni magistrali", Jovene Editore, 2013
- 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, n. 21
- M. CARDONE (2025), *Punti di Vista sulla sovranità digitale – Difendere il cyberspazio: la nuova frontiera della sovranità digitale*, in "IRPA – Osservatorio sullo Stato Digitale", 21 marzo 2025
- M. CATANZARITI (2024), *Disconnecting sovereignty: how data fragmentation reshapes the law*, Springer Nature, 2024
- E. CELESTE (2021), *Digital constitutionalism: mapping the constitutional response to digital technology's challenge*, in "Direitos Fundamentais & Justiça", 2021, n. 45
- E. CELESTE (2019), *Digital constitutionalism: a new systematic theorisation*, in "International Review of Law, Computers & Technology", vol. 33, 2019, n. 1

- A. CHANDER, H. SUN (a cura di) (2023), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford University Press, 2023
- COMMISSIONE EUROPEA (2024), *State of the Digital Decade 2024*, COM (2024) 400, Bruxelles, 2024
- S. CRESPI (2024), *La protezione dello Stato di diritto nel sistema dell'Unione europea*, in "Eurojus.it", 2024, n. 2
- B. CUSTERS (2022), *New digital rights: Imagining additional fundamental rights for the digital era*, in "Computer Law & Security Review", vol. 44, 2022
- G. DE GREGORIO, R. RADU (2022), *Digital constitutionalism in the new era of Internet governance*, in "International Journal of Law and Information Technology", vol. 30, 2022, n. 1
- P. DE ROSA (2021), *Concetto di Stato e nuove tecnologie. Quale ruolo per lo Stato nello spazio digitale?*, in "Media Laws", Law and Media WPS n. 1/2021
- A. DI CORINTO (2022), *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in "Rivista italiana di informatica e diritto", 2022, n. 1
- J. EDWARDS (2024), *A Comprehensive Guide to the NIST Cybersecurity Framework 2.0: Strategies, Implementation, and Best Practice*, John Wiley & Sons, 2024
- A. EL-SHROUK (2023), *Comprehensive cybersecurity review: Modern threats and innovative defense approaches*, in "International Journal of Computers and Informatics (Zagazig University)", 2023, n. 1
- F. FAINI (2018), *Dati, informazioni e società digitale: il cambiamento nei confini del diritto*, in R. De Giorgi (a cura di), "Limiti del diritto. Prospettive di riflessione e analisi", Pensa MultiMedia, 2018
- C. FARALLI (2018), *Diritto, diritti e nuove tecnologie*, Editoriale Scientifica, 2018
- L. FLORIDI (2020), *The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU*, in "Philosophy & Technology", vol. 33, 2020, n. 3
- S. FRATINI, E. HINE, C. NOVELLI, H. ROBERTS, L. FLORIDI (2024), *Digital sovereignty: A descriptive analysis and a critical evaluation of existing models*, in "Digital Society", vol. 3, 2024, n. 3
- A. GATTI (2019), *Istituzioni e anarchia nella rete. I paradigmi tradizionali della sovranità alla prova di internet*, in "Il diritto dell'informazione e dell'informatica", 2019, n. 3
- M.E. GONÇALVES (2019), *The risk-based approach under the new EU data protection regulation: a critical perspective*, in "Journal of Risk Research", vol. 23, 2019, n. 2
- P. GUARDA (2008), *Data Protection, Information Privacy and Security Measures: an Essay on the European and the Italian Legal Frameworks*, in "Cyberspazio e diritto", vol. 9, 2008, n. 1
- M. GUERRA (2025), *Le prospettive di collaborazione tra Autorità indipendenti nell'era digitale*, in "Rivista italiana di informatica e diritto", 2025, n. 1
- M. HELLMEIER, F. VON SCHERENBERG (2023), *A delimitation of data sovereignty from digital and technological sovereignty*, in "ECIS 2023 Research Papers", 306, 2023
- P. HUMMEL, M. BRAUN, M. TRETTER, P. DABROCK (2021), *Data sovereignty: A review*, in "Big Data & Society", vol. 8, 2021, n. 1
- ICT SECURITY MAGAZINE (2025), *NIS2 e oltre: la cybersicurezza diventa governance aziendale*, in "ICT Security Magazine", 3 dicembre 2025
- E. LONGO (2023), *La ricerca di un'antropologia costituzionale della società digitale*, in "Rivista italiana di informatica e diritto", 2023, n. 2

- S. MANGIAMELI (2023), *La sovranità digitale*, in A.C. Amato, G. Saraceni (a cura di), “Cento e una voce di informatica giuridica”, Giappichelli, 2023
- J. MILLARD (2023), *Impact of Digital Transformation on Public Governance*, Publications Office of the European Union, 2023
- E.M.L. MOEREL, P. TIMMERS (2021), *Reflections on Digital Sovereignty*, in “EU Cyber Direct, Research in Focus series”, 2021
- NATIONAL CYBER SECURITY CENTRE (2024), *NCSC Annual Review 2024*, in National Cyber Security Centre (NCSC), 2024
- NETRIBE GROUP (2025), *Direttiva NIS2: nuove responsabilità cybersecurity degli imprenditori*, in Netribe Group, 22 aprile 2025
- N.R. NODEHI, F. BERISHA, L. DA SILVA, Z. POURZOLFAGHAR, M. HELFERT (2024), *Integrating Cybersecurity, Data Sovereignty and Trustworthiness in Agri-data Sharing Environments: A Conceptual Framework*, in “2024 Cyber Research Conference – Ireland (Cyber-RCI)”, Carlow, Ireland, 2024
- N. PALLADINO (2023), *The Ambiguity of Digital Sovereignty between Territorialization of the Cyberspace, Extraterritorial Claims and Digital Rights: Analysing Data Transfer Policies in EU, US and China*, in giga-net.org, 2023
- F. PIERUCCI (2025), *Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace*, in “Digital Society”, vol. 4, 2025, n. 1
- L. PLIAUŠKAITĖ (2024), *Digital Governance in Europe: A Stakeholder Map of European Institutions and Regulators*, in iapp.org, 2024
- 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
- D. REDEKER, L. GILL, U. GASSER (2018), *Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights*, in “International Communication Gazette”, vol. 80, 2018, n. 4
- F. RESTA (2024), *Cybersicurezza e protezione dati: un rapporto ambivalente*, in “Rivista italiana di informatica e diritto”, 2024, n. 2
- G. RESTA, V. ZENO-ZENCOVICH (a cura di) (2016), *La Protezione Transnazionale dei Dati Personali*, RomaTrE-Press, 2016
- H. ROBERTS, J. COWLS, F. CASOLARI, J. MORLEY, M. TADDEO, L. FLORIDI (2021), *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, in SSRN, 2021
- S. RODOTÀ (2021), *Tecnologie e diritti*, il Mulino, 2021
- M. SANTANIELLO (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in “Rivista italiana di informatica e diritto”, 2022, n. 1
- A. SIMONCINI (2017), *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), “Diritti e libertà in internet”, Mondadori Education, 2017
- 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
- C. SPINIELLO (2025), *È (ancora) tempo di costituzionalismo digitale*, in “Rivista italiana di informatica e diritto”, 2025, n. 1
- SS GROUP (2024), *La Direttiva NIS2: Nuove Regole per la Cybersecurity e la Responsabilità Aziendale*, in SSG Scai Solution Group, 19 aprile 2024

- M. TADDEO (2019), *Is cybersecurity a public good?*, in “Minds and Machines”, vol. 29, 2019, n. 3
- V. ZENO-ZENCOVICH (2018), *La “datasfera”. Regole giuridiche per il mondo digitale parallelo*, in L. Scafardi (a cura di), “I ‘profili’ del diritto. Regole, rischi e opportunità nell’era digitale”, Giappichelli, 2018
- G. ZICCARDI (2019), *La Cybersecurity nel quadro tecnologico (e politico) attuale*, in G. Ziccardi, P. Perri (a cura di), “Tecnologia e Diritto”, III, Giuffrè, 2019



LAURA LA CORTE

La natura relativa e contestuale della nozione di dato personale alla luce della sentenza *Deloitte*

Il contributo analizza l'evoluzione della nozione di dato personale alla luce della sentenza *Deloitte* del 4 settembre 2025, evidenziando come il tradizionale confine tra dato personale e dato anonimo risulti oggi sempre più incerto e labile. Muovendo dalla definizione ampia accolta dal GDPR, fondata sul criterio dell'identificabilità, si evidenzia come tale requisito non costituisca una qualità intrinseca dell'informazione, ma dipenda dal contesto, dai mezzi ragionevolmente utilizzabili e dalle finalità del trattamento. Particolare attenzione è dedicata alle tecniche di pseudonimizzazione e anonimizzazione, le quali mettono in crisi il tradizionale modello dicotomico tra dato personale e non personale. L'evoluzione delle tecnologie di analisi dei dati e dell'intelligenza artificiale accresce infatti il rischio di re-identificazione, mostrando come nessuna tecnica garantisca un'anonimizzazione assoluta. In questa prospettiva, la sentenza *Deloitte* segna un passaggio decisivo, affermando che la qualificazione giuridica di un dato può variare in base al contesto del trattamento e alle concrete possibilità di re-identificazione in capo al soggetto che lo tratta. Ne deriva la necessità di un modello di *governance* dinamico e fondato sul rischio, capace di bilanciare la tutela dei diritti fondamentali con le esigenze di circolazione dei dati nell'ecosistema digitale contemporaneo.

Dato personale – Identificabilità – Pseudonimizzazione – Anonimizzazione – Valutazione del rischio

The relative and contextual nature of the concept of personal data in the light of the *Deloitte* judgment

The article examines the evolution of the concept of personal data in light of the *Deloitte* judgment of September 4, 2025, highlighting how the traditional boundary between personal and anonymous data became increasingly blurred and uncertain. Drawing upon the broad definition adopted by the GDPR, based on identifiability, the author demonstrates that this requirement does not constitute an intrinsic property of information. Rather, it depends on the context, on the means reasonably likely to be used and on the purposes of the processing. The analysis focuses on pseudonymization and anonymization techniques, which challenge the traditional binary distinction between personal and non-personal data. The evolution of data analysis technologies and artificial intelligence indeed increases the risk of re-identification, proving that no technique can guarantee absolute irreversibility. In this regard, the *Deloitte* judgment marks a significant turning point by affirming that the legal data qualification may vary depending on the processing context and the concrete possibilities of re-identification available to the entity handling the data. This leads to the need for a dynamic, risk-based governance model capable of balancing the protection of fundamental rights and the necessity of data circulation within the contemporary digital ecosystem.

Personal data – Identifiability – Pseudonymisation – Anonymisation – Risk assessment

L'Autrice è dottoranda di ricerca in Discipline giuridiche pubblicistiche, curriculum Discipline pubblicistiche, internazionalistiche ed europee, presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre

SOMMARIO: 1. La nozione di dato personale tra esigenze di innovazione e di tutela. – 2. La nozione dinamica di dato personale. – 3. Anonimizzazione e pseudonimizzazione dei dati: crisi del modello dicotomico. – 4. Conclusioni: verso un modello di governance dei dati basato sul rischio e sul contesto.

1. La nozione di dato personale tra esigenze di innovazione e di tutela

Il presente contributo si propone di indagare la nozione di dato personale muovendo dalla consapevolezza che il confine tra dato personale e dato anonimo fosse, fin dalla sua formulazione, intrinsecamente labile, posto che l'identificabilità non dipende solo dal contenuto dell'informazione ma dai mezzi concretamente impiegabili per ricondurla ad un individuo¹.

L'evoluzione tecnologica e le crescenti possibilità di re-identificazione ne hanno progressivamente accentuato la permeabilità²: la sentenza *Deloitte* del 4 settembre 2025³ offre l'opportunità di analizzare un ulteriore momento di relativizzazione.

In tale contesto, la transizione digitale impone al giurista di confrontarsi con trasformazioni che, dissolvendo progressivamente i tradizionali confini tra sfera privata e spazio pubblico, incidono sul sistema di tutela dei diritti fondamentali.

Se, da un lato, l'impianto europeo appare costruito per garantire un'elevata protezione della persona anche in contesti tecnologicamente avanzati,

dall'altro lato l'evoluzione delle tecniche di trattamento, fondate su capacità sempre più sofisticate di condivisione delle informazioni, mette alla prova la tenuta delle categorie giuridiche tradizionali⁴.

Sullo studioso grava, quindi, il compito di verificare in quale misura il progresso tecnologico richieda l'elaborazione di nuove regole, oppure se le esigenze emergenti possano essere affrontate alla luce di regole e principi già applicati in materia di protezione dei dati personali⁵.

La nozione ampia di dato personale accolta dal Regolamento generale sulla protezione dei dati personali⁶ sembra offrire strumenti potenzialmente idonei ad accompagnare l'innovazione.

Tuttavia, l'espansione delle tecniche di profilazione induce a mettere in discussione la solidità della tradizionale distinzione tra dato relativo ad una persona identificata o identificabile e dato anonimo, specialmente considerando la "difficoltà tecnica di separare chirurgicamente i dati personali dai dati non personali"⁷.

La possibilità tecnica di ricondurre, anche indirettamente, informazioni apparentemente neutre a una persona fisica impone di interrogarsi

1. Come già ampiamente rilevato in dottrina, cfr. *ex multis* D'ACQUISTO-NALDI 2017.

2. Come già ampiamente rilevato in dottrina, cfr. *ex multis* CALZOLAIO 2017.

3. Corte di giustizia Ue, sent. 4 settembre 2025, C-413/23 P.

4. Secondo il tradizionale insegnamento di Paolo Barile, infatti, "valgono regole opposte circa il segreto nel pubblico ed il segreto nel privato. L'apparato della democrazia ha per regola la trasparenza, ed il segreto costituisce una eccezione. I diritti costituzionalmente garantiti al soggetto privato in democrazia (la libertà nella comunità) hanno per regola la privacy, e per eccezione la pubblicità" (così BARILE 1987, p. 29 ss.).

5. PASSAGLIA 2016, p. 332.

6. Art. 4, n. 1 e, in particolare, cons. 26, Regolamento (UE) n. 2016/679 (GDPR).

7. PALMIRANI 2019, p. XII.

sull'efficacia delle misure di protezione previste e sulla capacità dell'ordinamento di prevenire i rischi di re-identificazione.

In questo scenario, un ruolo decisivo è svolto dalla Corte di giustizia dell'Unione europea⁸, il cui intervento ha rafforzato la centralità dei diritti contenuti nella Carta dei diritti fondamentali dell'Unione europea che, proprio nel preambolo, evidenzia la necessità di “rafforzare la tutela dei diritti fondamentali, alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici”⁹.

Particolarmente significativa, in questo senso, è la sentenza *Deloitte*, laddove stabilisce che la qualificazione dei dati deve essere valutata in modo contestuale e relativo, non dipendendo solo dalla natura astratta dell'informazione ma tenendo conto dei mezzi effettivamente disponibili per il soggetto che li tratta.

In particolare, nella vicenda sottoposta al giudizio della Corte, i dati pseudonimizzati possono essere considerati anonimi per *Deloitte*, alla quale sono stati trasmessi senza l'accesso ai dati identificativi originari, e, dunque, nell'impossibilità concreta di re-identificare.

Di conseguenza, la valutazione dell'identificabilità va effettuata, ad avviso della Corte, al momento della raccolta dei dati e dal punto di vista del responsabile del trattamento.

Ciò solleva interrogativi di fondo: la pseudonimizzazione può rappresentare un punto di equilibrio sostenibile tra protezione e circolazione, o rischia di attenuare la responsabilità in caso di pericolo di re-identificazione? L'anonimizzazione è davvero compatibile con una tutela effettiva del dato personale in un ambiente digitale caratterizzato da una costante riaggregazione dei dati? È ancora adeguata una distinzione netta tra dato personale e dato non personale, oppure occorre ripensare in chiave graduale e dinamica il rapporto tra dato e persona?

È lungo queste direttrici, e alla luce della sentenza *Deloitte*, che si sviluppa la riflessione che segue, volta ad indagare la nozione di dato personale e a verificare se l'attuale impianto normativo sia ancora idoneo a garantire, nel contesto tecnologico attuale, una protezione effettiva dei diritti fondamentali senza sacrificare, al contempo, le esigenze di circolazione e valorizzazione dei dati.

2. La nozione dinamica di dato personale

Nell'attuale ecosistema digitale, il dato personale è in continua trasformazione, sospeso tra la tutela dell'identità individuale e la crescente valorizzazione economica dell'informazione¹⁰.

La natura ambivalente del dato personale¹¹, in quanto oggetto di un diritto fondamentale e bene di valore economico, determina una tensione tra la circolazione dei dati e la protezione degli stessi, concepita non come un fine assoluto, bensì come uno strumento di tutela degli interessi, di volta in volta, sottostanti.

Nonostante la recente spinta verso la condivisione e apertura dei *big data*, a beneficio del mercato e della collettività, la disciplina del GDPR, focalizzandosi sui dati a carattere personale, mostra la scelta assunta dal legislatore, al bivio tra i due interessi in gioco: la protezione dei dati – ovvero la protezione di un diritto fondamentale sancito dalla Carta europea dei diritti fondamentali (art. 8) – prima della circolazione¹².

Tuttavia, di fronte al necessario sviluppo delle tecnologie digitali, è opportuna una riflessione anche sui dati non personali, categoria residuale e limitata in modo significativo dalla natura ampia e mutevole del concetto stesso di dato personale.

Il macro-ambito della nozione di dato, comprende, infatti, oltre ai dati personali, anche i dati non personali, la cui residualità emerge dalla definizione “negativa” offerta dall'art. 3, punto 1, del Regolamento UE 1807/2018¹³, come “dati diversi

8. Sull'impatto della giurisprudenza della Corte di giustizia v. AMALFITANO–FERRI 2023, p.17 ss.

9. Preambolo della Carta dei diritti fondamentali dell'Unione europea.

10. Sul valore e la circolazione dei dati v. CREMONA–LAVIOLA–PAGNANELLI 2022; NICITA 2019.

11. FAINI 2023, p. 388.

12. TORREGIANI 2020, p. 319; MONTAGNANI 2019, p. 15.

13. Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea del 14 Novembre 2018.

dai dati personali definiti dall'art. 4, punto 1, del Regolamento (UE) 2016/679".

La problematicità della differenziazione tra dati personali e non personali emerge con particolare evidenza se si guarda non solo alla qualificazione del dato, ma anche allo statuto giuridico che l'ordinamento europeo riconosce alle due categorie, comportando l'applicazione di discipline diverse proprio sotto il profilo della circolazione, dell'accessibilità e del trasferimento verso Paesi terzi.

Mentre i dati personali sono sottoposti al sistema di garanzie del GDPR, fondato sui principi di liceità, minimizzazione, limitazione delle finalità, *accountability* e sulle rigorose condizioni previste dagli artt. 44 ss. per i trasferimenti internazionali, i dati non personali sono invece assoggettati, in linea di principio, ad un regime ispirato alla libera circolazione, come espressamente previsto dal Regolamento (UE) 2018/1807, che vieta restrizioni alla localizzazione dei dati all'interno dell'Unione salvo esigenze di sicurezza pubblica.

La dicotomia tra dato personale e non personale, continuamente messa in discussione da strumenti volti a rilevare "connessioni 'invisibili' tra i dati"¹⁴ per ricavare nuove informazioni, determina il campo di applicazione del GDPR. Di conseguenza, è proprio nell'interpretazione dell'art. 4, che si individua il suo ambito di operatività.

La definizione fornita dall'art. 4 del GDPR, rimasta immutata rispetto alla Direttiva 95/46, qualifica il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)"¹⁵.

Risulta evidente che la disciplina della protezione dei dati si fonda sull'interazione di quattro elementi chiave, in cui è possibile scomporre la definizione. Il primo è il riferimento a "qualsiasi informazione"; il secondo è l'aggettivo verbale "riguardante"; il terzo, l'espressione "una persona fisica"; infine, la caratteristica di "identificata o identificabile"¹⁶.

Per cogliere l'effettiva portata della nozione di dato personale è, dunque, necessario analizzare i suddetti aspetti fondamentali, poiché è proprio il concetto di identificabilità che, tradizionalmente, traccia la linea di confine tra quanto è soggetto alla normativa del GDPR e ciò che, invece, non rientra nel suo ambito di applicazione.

Emerge, anzitutto, la scelta di un linguaggio onnicomprensivo, che, offrendo il vantaggio di abbracciare con lungimiranza anche le situazioni nuove e non prevedibili dal legislatore, originate dalla rapida e continua evoluzione del mondo digitale, è sintomo di una sempre maggiore presa di coscienza della "eccedenza della vita rispetto alle regole"¹⁷.

La scelta lessicale dell'espressione "qualsiasi informazione", che apre la disposizione, è il primo

14. TORREGIANI 2020, p. 318.

15. Interviene sulla nozione di dato personale sancita dall'art. 4, par. 1, GDPR la Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e le direttive 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 per quanto riguarda la semplificazione del quadro legislativo nel settore digitale e che abroga i regolamenti (UE) 2018/1807, (UE) 2019/1150 e (UE) 2022/868 e la direttiva (UE) 2019/1024 (omnibus digitale). L'articolo 3, *Modifiche del Regolamento (UE) 2016/679* (GDPR) stabilisce, infatti, che "l'articolo 4 è così modificato: (a) al punto 1) sono aggiunte le frasi seguenti: le informazioni relative a una persona fisica non sono necessariamente dati personali per qualsiasi altra persona o entità per il solo fatto che un'altra entità può identificare tale persona fisica. Le informazioni non sono personali per una determinata entità se quest'ultima non è in grado di identificare la persona fisica cui si riferiscono le informazioni, tenendo conto dei mezzi di cui tale entità si può ragionevolmente avvalere. Tali informazioni non diventano personali per tale entità per il solo fatto che un potenziale destinatario successivo dispone di mezzi di cui si può ragionevolmente avvalere per identificare la persona fisica cui le informazioni si riferiscono". Il *Digital Omnibus Package*, inserendosi nel contesto di una complessiva strategia di razionalizzazione avviata dopo il rapporto di Mario Draghi sul futuro della competitività europea, orientata a semplificare la normativa digitale per sostenere la crescita industriale e il progresso tecnologico, accoglie una qualificazione di dato personale che non deriverebbe da una valutazione oggettiva della natura dell'informazione, bensì dipenderebbe dalle caratteristiche specifiche del soggetto che ne è in possesso.

16. BOLOGNINI-BISTOLFI 2016, p. 4.

17. COLAPIETRO 2018, p. 16.

indice dell'elasticità che permea la definizione di dato personale, in quanto, lungi dall'essere una formulazione generica, è una precisa scelta normativa, volta ad attribuire alla nozione di dato personale una portata ampia, tale da ricomprendere ogni elemento informativo che, direttamente o indirettamente, possa riguardare una persona fisica.

Nella consapevolezza che l'identità di un individuo può emergere da una pluralità di informazioni, anche apparentemente neutre o frammentarie, si consente, così, alla definizione di operare anche a fronte di dati generati da nuovi strumenti digitali e di tutelare l'integrità della persona nel mutevole ecosistema digitale contemporaneo.

In particolare, nel recepire gli orientamenti contenuti nel Parere n. 4/2007 del Gruppo *ex art.* 29¹⁸, la nozione di dato personale si ritiene onnicomprensiva tanto dal punto di vista della natura dell'informazione (sia essa soggettiva, oggettiva, veritiera o meno) quanto sotto il profilo del contenuto (relativo a dati generali e sensibili), ma anche in riferimento alla forma (indipendentemente dal supporto utilizzato, che sia cartacea, numerica, alfabetica, fotografica o sonora).

L'ampiezza della formulazione fin qui esaminata è, tuttavia, ristretta dal successivo requisito richiesto affinché si possa parlare di dato personale: che l'informazione sia "riguardante" l'interessato, cui il dato si riferisce.

In particolare, per considerare un dato riguardante un individuo, devono sussistere tre caratteristiche alternative¹⁹.

Il primo criterio è la presenza di un elemento di contenuto, che ricorre quando, dal contenuto stesso dei dati, è possibile identificare direttamente una persona fisica, indipendentemente dalle finalità del trattamento. In altre parole, l'informazione concerne chiaramente un individuo: ad esempio, un referto medico che indica il nome del paziente²⁰.

Il secondo elemento, quello della finalità, ricorre quando, anche in assenza di un collegamento

diretto tra i dati e la persona fisica, lo scopo del trattamento è tale da influenzare lo status o il comportamento dell'interessato. Un esempio è rappresentato dai registri chiamate di un'azienda: a seconda della finalità del trattamento, i dati possono riferirsi ai dipendenti o ai clienti. Dunque, è l'obiettivo per cui i dati vengono trattati a determinare a chi essi si riferiscono.

Infine, l'elemento del risultato si riferisce ai casi in cui il trattamento dei dati produce effetti nella sfera giuridica o personale dell'interessato. Ad esempio, un sistema di localizzazione che assegna automaticamente una corsa al tassista più vicino al cliente può generare informazioni sul comportamento del conducente stesso, come i percorsi abituali, producendo, così, effetti sulla sua attività professionale²¹.

La dinamicità della nozione di dato personale²² è rafforzata dall'interpretazione di persona "identificabile", da tenere distinta rispetto a quella "identificata". Infatti, un individuo è identificato quando è distinto in modo certo da tutti gli altri membri di un gruppo. Sarà, invece, identificabile quando, pur non essendo ancora stato identificato, esistono elementi significativi grazie ai quali si può risalire, direttamente o indirettamente, alla sua identità, restringendo sempre più il gruppo al quale appartiene²³.

Nonostante l'estensione dell'espressione, rintracciamo delle linee guida interpretative nei considerando 26 e 30 del GDPR.

Il primo sottolinea che "per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi" valutando "l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici". Si noti qui l'utilizzo dell'avverbio "ragionevolmente", che orienta

18. Data Protection Working Party (WP29), *Parere 4/2007 sul concetto di dati personali*.

19. STALLA-BOURDILLON-KNIGHT 2017; DI RESTA 2018, p. 8 s.

20. Rientrano in questa categoria non solo i nomi, ma anche gli identificatori univoci, come un numero di passaporto, che consente di risalire in modo inequivocabile all'interessato.

21. Sui criteri esaminati cfr. anche LEE BYGRAVE-DOCKSEY-KUNER 2020 e RICCIO-SCORZA-BELISARIO 2018.

22. Cfr. la tesi espressa in dottrina da COLAPIETRO-IANNUZZI 2017 e CALZOLAIO 2017.

23. BOLOGNINI-BISTOLFI 2016, p. 4.

verso una concezione ampia di dato personale, a supporto del modello finora descritto²⁴.

Il secondo considerando citato chiarisce che, sempre ai fini dell'identificabilità "le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

Tale disposizione è la codificazione degli approdi raggiunti dalla giurisprudenza della Corte di giustizia, in particolare con la sentenza *Breyer*²⁵, in cui l'indirizzo IP dinamico²⁶ di un utente di un sito web è stato considerato un dato personale²⁷, in base alle informazioni detenute dal provider di accesso a internet.

Infatti, la possibile combinazione degli indirizzi IP con le informazioni degli abbonati del fornitore del servizio Internet consentirebbe di identificare in modo certo l'utente e configurare, dunque, un dato personale, per scopo o per risultato, essendo, in qualche modo, assimilabile a un dato di localizzazione²⁸. Pertanto, per determinare se gli indirizzi IP costituiscano dati personali, è fondamentale considerare quali informazioni vengono associate ad essi e gli scopi per cui i dati sono trattati, poiché è la combinazione di diversi identificatori a consentire il passaggio dall'essere una persona identificabile all'essere una persona identificata, risultando necessaria una valutazione basata sul contesto.

L'esame dei casi concreti, evidenzia, infatti, una certa complessità nel definire un criterio

uniforme di identificabilità, portando a preferire un approccio di tipo relativo.

Una simile impostazione, che valorizza il contesto d'uso del dato più che la sua natura ontologica, trova un interessante parallelismo nel diritto cinese, che distingue concettualmente tra *personal information* e *data*, attribuendo alle due nozioni un differente statuto giuridico in base alla funzione che assolvono e agli interessi che vengono in rilievo²⁹.

Da un lato, la nozione di *personal information*, accolta dal *Personal Information Protection Law* (PIPL), rileva quando l'informazione sia idonea a incidere sui diritti ed interessi della persona fisica; dall'altro, la nozione di *data*, presente nel *Data Security Law* (DSL) e nel *Cybersecurity Law* (CSL), assume rilievo quando l'interesse in gioco sia l'interesse pubblico, quale risorsa strategica per la sicurezza e la sovranità digitale dello Stato.

L'adozione della nozione di informazione in luogo di quella di dato comporta rilevanti conseguenze sul piano giuridico, poiché sposta l'attenzione dalla dimensione ontologica del dato al suo profilo funzionale.

In questa prospettiva, ai fini dell'applicazione della disciplina in materia di protezione dei dati personali, rileva la concreta possibilità che il titolare del trattamento utilizzi i dati per ricavare informazioni riferibili ad una persona fisica. Ne consegue che, ai fini della tutela della persona, la nozione di informazione personale consente meglio di calibrare l'applicazione delle garanzie normative alle effettive caratteristiche del trattamento e del rischio per l'interessato.

Una simile articolazione di categorie suggerisce la possibilità di superare anche in Europa la tradizionale e piuttosto semplice distinzione tra dati personali e dati non personali, in favore di

24. DI RESTA 2018, p. 14.

25. Corte di giustizia Ue, sentenza in causa C-582/14, *Patrick Breyer vs Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

26. Un indirizzo IP dinamico è un indirizzo che cambia ad ogni connessione Internet e viene assegnato automaticamente a un dispositivo quando si connette a una rete.

27. Cf. ENISA, *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*, November 2019, in cui gli indirizzi IP, insieme agli indirizzi e-mail, vengono analizzati come casi d'uso di pseudonimizzazione.

28. STALLA-BOURDILLON-KNIGHT 2017.

29. CALZOLAIO 2023.

una disciplina più idonea all'era contemporanea dell'IA e della datificazione.

È alla luce di tali considerazioni che va letto il primo motivo di decisione della Corte di giustizia nella sentenza *Deloitte*, laddove stabilisce che “la natura particolare delle opinioni e dei pareri personali (...) in quanto espressione del pensiero di una persona, sono necessariamente strettamente legati a quest'ultima”³⁰. Non era, pertanto, necessario, in tal caso, un esame del contenuto, scopo o effetti dei commenti rilasciati dagli azionisti alla SRB, risultando pacifico che fossero espressione degli autori e, quindi, dati personali.

L'interpretazione adottata dalla Corte è supportata dalla sentenza del 20 dicembre 2017, *Nowak* (C-434/16), in cui, in riferimento ai commenti di un esaminatore sulle prove scritte di un candidato in sede di esame, si rilevava che gli stessi riflettono inevitabilmente la personale valutazione dell'esaminatore e sono, dunque, a quest'ultimo riferibili.

Si legge, infatti, in tale pronuncia, che “l'uso dell'espressione ‘qualsiasi informazione’ (...) riflette l'obiettivo del legislatore dell'Unione di attribuire un'accezione estesa a tale nozione, che non è limitata alle informazioni sensibili o di ordine privato, ma comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano “concernenti” la persona interessata”^{31 32}.

3. Anonimizzazione e pseudonimizzazione dei dati: crisi del modello dicotomico

Se l'identificabilità rappresenta il criterio cardine per l'applicazione del GDPR, occorre allora interrogarsi su quali siano gli strumenti tecnici e

giuridici attraverso i quali il legislatore europeo la attenua o esclude. È in questa prospettiva che si inseriscono le tecniche di anonimizzazione e pseudonimizzazione dei dati³³, nonché la sentenza *Deloitte*, nell'affermare che “i dati pseudonimizzati non devono essere considerati come costituenti, in tutti i casi e per ogni persona, dati personali ai fini dell'applicazione del regolamento 2018/1725, nella misura in cui la pseudonimizzazione può, a seconda delle circostanze del caso, impedire effettivamente a persone diverse dal responsabile del trattamento di identificare l'interessato in modo tale che, per loro, l'interessato non sia o non sia più identificabile”³⁴.

Il considerando 26 del GDPR stabilisce che il Regolamento non si applica al trattamento di informazioni anonime, “vale a dire 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”³⁵. Tali tecniche trovano applicazione sia nella conservazione dei dati sia nella loro eventuale comunicazione a terzi, in particolare in ambiti di natura statistica, storica o scientifica.

Al contrario, il GDPR si applica integralmente ai dati pseudonimizzati, in quanto, pur essendo sottoposti a tecniche di riduzione dell'identificabilità, conservano la qualificazione di dati personali.

La pseudonimizzazione³⁶ è definita all'art. 4 del GDPR 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

30. Corte di giustizia Ue, sent. 4 settembre 2025, C-413/23 P.

31. Corte di giustizia Ue, sent. 20 dicembre 2017, *Nowak*, C-434/16.

32. Assume rilievo, in questo quadro, la clausola contenuta nel primo comma dell'art. 21 Cost., inserita con lungimiranza, lì dove prevede la possibilità di esercitare la libertà di pensiero con “ogni mezzo di diffusione”, così da garantire nuove forme di tutela costituzionale anche a nuove forme di espressione, frutto dell'evoluzione delle moderne tecnologie. Analogamente, l'art. 15 Cost. prevede, al primo comma, che “la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili”.

33. D'ACQUISTO-NALDI 2017.

34. Corte di giustizia Ue, sent. 4 settembre 2025, C-413/23 P., punto 86.

35. Reg. UE 679/2016, considerando 26.

36. GABEL-SCHIERING 2018; EDPB, *Guidelines 01/2025 on Pseudonymisation*.

organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile”.

Tale definizione è al tempo stesso restrittiva e molto ampia. È restrittiva nella misura in cui non comprende i processi di trattamento che non riescano a garantire l'attribuzione dei dati personali a una persona fisica identificabile. Dall'altro lato, è una definizione ampia, in quanto non richiama la collegabilità dei dati come problema fondamentale alla base del rischio che gli individui possano ancora essere individuati, anche dopo l'applicazione di tecniche di pseudonimizzazione³⁷.

In particolare, maggiore è la quantità di informazioni relative ad un individuo, maggiore è la probabilità che queste vengano impiegate per identificarlo o per ottenere dati a lui riferibili. Il rischio di re-identificazione è legato, quindi, all'aggregazione, ovvero la combinazione di dati, tale da generare una nuova informazione.

Si pensi che uno studio condotto dalla professoressa Latanya Sweeney³⁸ dimostra che la combinazione di un codice postale, della data di nascita e del genere è sufficiente a identificare l'87% degli individui negli Stati Uniti. Questo perché i dati non personali non esistono mai isolati ma sono parte di un insieme dinamico di informazioni disponibili per ogni individuo³⁹.

Il Parere 5/2014 del Gruppo di Lavoro Art. 29⁴⁰, a tal proposito, fa riferimento alla necessità di valutare molteplici fattori in costante evoluzione, che contribuiscono al contesto in cui le tecniche di de-identificazione operano, quali lo stato della tecnologia, le finalità del trattamento, la disponibilità

di informazioni ulteriori, evidenziando la presenza di un “rischio intrinseco residuo di reidentificazione”⁴¹ tale che “nessuna tecnica è di per sé esente da carenze”⁴².

Per questi motivi, l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) ha contribuito a individuare una serie di principi generali di progettazione che ogni titolare del trattamento dovrebbe considerare nella scelta delle tecniche di pseudonimizzazione⁴³.

Il primo obiettivo ivi previsto è quello di garantire che lo pseudonimo non consenta facilmente a terzi di re-identificare. Verificato questo aspetto, il titolare deve adottare misure che impediscano a terzi di riprodurre gli stessi pseudonimi.

È bene, però, tenere presente che non è possibile eliminare del tutto il rischio di re-identificazione degli individui⁴⁴.

In quest'ottica, diventa fragile il confine tra dati personali e dati anonimi, la cui dicotomia è fondata su un approccio statico legato ad una qualità intrinseca del dato. Al contrario, lo stato dei dati sottoposti a misure di pseudonimizzazione e, ancor di più, a misure di anonimizzazione, deve essere valutato in modo dinamico, alla luce del contesto e mediante monitoraggi continui, poiché, nell'impossibilità di tracciare un vademecum valido in ogni caso, è necessario adottare un approccio orientato al rischio⁴⁵.

Infatti, tra le critiche sollevate, in particolare nei confronti della “anonimizzazione come una sorta di panacea di tutti i mali”⁴⁶, che consente al titolare del trattamento di liberarsi dalle maglie del GDPR, assume rilievo quella di Paul Ohm⁴⁷. Egli

37. STALLA-BOURDILLON-KNIGHT 2017, p. 17 s.

38. SWEENEY 2000.

39. In questi termini SCHWARTZ-SOLOVE 2011, p. 1843.

40. Gruppo di Lavoro Art. 29 per la protezione dei dati, *Parere 05/2014 sulle tecniche di anonimizzazione* (WP216, 0829/14/IT), 10 aprile 2014 [di seguito Parere 05/2014].

41. Parere 05/2014, p. 7.

42. *Ivi*, p. 12.

43. ENISA, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation*, November 2018; ENISA, *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*, November 2019.

44. *Ibidem*. V. anche TROVATO-RAUCCIO 2022.

45. FOGLIA 2019, p. 311 ss.

46. *Ivi*, p. 310.

47. OHM 2010.

sostiene che l'anonimizzazione di tipo “*release and forget*” è una promessa illusoria e propone di abbandonare la tradizionale distinzione tra dati personali e non personali, attraverso una valutazione dei rischi concreti di re-identificazione, più aderente alla realtà.

In un simile ripensamento del paradigma, così proposto da Ohm, sarebbe necessario considerare le molteplici sfumature di “identificabilità” comprese tra i due poli dei dati riferibili a soggetti identificati e quelli anonimi poiché non è possibile escludere con certezza la possibilità di re-identificare un dato reso anonimo.

Lo sviluppo delle tecniche di analisi dei dati e la crescente diffusione delle politiche di *open access* rendono, infatti, sempre più irrealizzabile un'anonimizzazione rigorosa, così che l'irreversibilità non è più un requisito assoluto, ma un obiettivo cui il titolare del trattamento deve tendere, al fine di ridurre il rischio entro termini accettabili⁴⁸. In sostanza, un dato che oggi non è personale potrebbe diventarlo in futuro, in quanto l'identificabilità dipende dal contesto.

È stato osservato come l'evoluzione tecnologica potrebbe condurre a trasformare il diritto alla protezione dei dati personali in un “*law of everything*”⁴⁹, poiché un numero sempre più crescente di dati sarà potenzialmente riconducibile alla nozione di dato personale e, conseguentemente, assoggettato all'ambito di applicazione del GDPR.

In ecosistemi digitali sempre più “intelligenti”, infatti, ogni informazione può potenzialmente essere ricondotta, direttamente o indirettamente, a una persona fisica.

Ciò non significa accettare la tesi di Ohm secondo cui “*data can be useful or perfectly anonymous but not both*”⁵⁰ che, se presa alla lettera, condurrebbe ad un disincentivo nell'uso delle misure di anonimizzazione⁵¹. Il fatto che non sia possibile eliminare in modo assoluto il rischio di re-identificazione, non implica la mancanza di utilità di tali tecniche che, sebbene non garantiscano

l'eliminazione del rischio, lo riducono ragionevolmente, in linea con l'altro grande principio del GDPR: quello della valutazione, che spetta al titolare svolgere, finalizzata alla riduzione in concreto dei rischi per i diritti dell'interessato (cd. *risk based approach* e *accountability*).

Di conseguenza, dipenderà dal contesto la definizione stessa di dato personale poiché, se l'anonimizzazione non è una caratteristica intrinseca del dato, neppure la personalizzazione (cioè la qualificazione del dato come personale) può essere considerata proprietà del dato in quanto tale. Essa deve essere piuttosto riferita al contesto in cui il dato è inserito, in quanto, sebbene l'identificabilità sia un elemento chiave nella definizione di dato personale, non è l'unico da tenere in considerazione⁵².

Per “contesto” si intendono, infatti, la finalità (concreta) del trattamento e, dunque, l'intenzione del titolare del trattamento, ma anche gli utilizzi attuali e potenziali, ad esempio, mediante future combinazioni con altri tipi di dati che il titolare è in grado effettivamente di mettere in atto.

In particolare, l'ambiente dei dati si può ritenere composto da quattro elementi chiave⁵³: il primo sono gli “altri dati”, cioè i dati con cui il dato anonimizzato può entrare in connessione; il secondo elemento sono gli utenti dei dati che, in seguito alla condivisione dei dati, li analizzano, trasformano, combinano con altre informazioni; il terzo elemento è relativo ai processi di governance che regolano le relazioni tra utenti e dati; infine, l'infrastruttura, composta da sistemi fisici e software che controllano l'accesso e l'interazione con i dati.

Dunque, la linea di demarcazione tra dati personali e non personali è fluida e può mutare nel tempo, determinando la possibilità che i dati anonimizzati al tempo *t1* diventino nuovamente dati personali al tempo *t2*, considerando che, una volta che i dati confluiscono nell'oceano digitale, è sempre più difficile contenere il rischio di re-identificazione.

48. TORREGIANI 2020, p. 325.

49. FINCK-PALLAS 2020, p. 20.

50. “I dati possono essere utili o perfettamente anonimi, ma non entrambi”, OHM 2010.

51. ELLIOT-O'HARA-RAAB et al. 2018, p. 10.

52. STALLA-BOURDILLON-KNIGHT 2017, p. 28 s.

53. ELLIOT-O'HARA-RAAB et al. 2018, p. 17.

D'altra parte, prevedere la distruzione di un dataset correttamente anonimizzato risulta essere un obbligo troppo stringente in capo al titolare del trattamento, poiché ne risentirebbe il flusso di dati, la cui fruizione è essenziale in settori basati proprio sull'analisi e la conservazione dei dati stessi (c.d. *data driven innovation*).

Se l'obiettivo è quello di agevolare la circolazione dei dati, occorre allora adottare una prospettiva diversa, che tenga conto non solo del dato in sé, ma anche del soggetto che lo tratta e del relativo contesto.

In alternativa all'approccio tradizionale, è stato infatti proposto un modello basato sull'uso dei dati (*use model*)⁵⁴ in cui si sposta il focus dalla fase di raccolta dei dati a quella del loro utilizzo. L'idea alla base è che il momento in cui tali dati vengono effettivamente impiegati determina rischi e benefici, i quali devono guidare le decisioni sull'utilizzo, tenendo conto del centrale elemento del contesto.

Questo approccio tende a ridurre l'attenzione sulla distinzione tra dati personali e non personali, concentrandosi piuttosto sugli effetti concreti che l'uso delle informazioni può produrre sugli individui.

In tale ottica, il soggetto terzo a cui venga trasferito un dataset anonimizzato entrerebbe in possesso di un insieme di dati da considerarsi per lui anonimi, in riferimento ai quali, pertanto, non assumerebbe la qualifica di titolare del trattamento, in quanto il GDPR non troverebbe applicazione.

A seconda del punto di vista adottato, il medesimo dato potrebbe avere natura diversa e, per l'appunto, dinamica: per il titolare originario, che conserva la disponibilità del dataset autentico ed è in grado di risalire all'identità degli interessati, le informazioni "anonimizzate" continuano ad essere dati pseudonimizzati, e quindi personali; al contrario, per il soggetto terzo, tale dato può assumere natura effettivamente anonima, e quindi non personale, qualora il contesto del trattamento comporti un rischio di re-identificazione inferiore alla soglia di accettabilità⁵⁵.

Il quadro descritto viene recepito anche dal GDPR che, a prima vista, sembra mantenere netta la distinzione tra dati anonimi e pseudonimizzati/personali. Tuttavia, una lettura più attenta rivela, "tra le righe", la possibilità di individuare una fascia

di dati intermedia, comprensiva di diversi livelli di identificabilità cui corrispondono più gradazioni di rischio e, di conseguenza, obblighi di intensità diversa per i titolari del trattamento.

In particolare, l'art. 11 stabilisce che "se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente Regolamento", coerentemente con il principio di minimizzazione. L'articolo prosegue affermando che "qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione".

Siamo davanti, quindi, a dati personali – che, nel corso del trattamento, vengono pseudonimizzati fino a lambire l'anonimizzazione per il titolare – che perdono progressivamente il carattere dell'identificabilità per il titolare stesso, il quale non può operare il collegamento con la persona fisica, a meno che non gli vengano fornite *ex novo* informazioni aggiuntive. Pertanto, i diritti dell'interessato previsti dagli articoli da 15 a 20 del GDPR, in assenza di tali ulteriori informazioni, non troveranno oggetto (cioè i dati personali) per la loro applicazione.

Così, anche l'impiego di misure di pseudonimizzazione può, a seconda del contesto, generare dati collocabili in gradini diversi della scala di identificabilità, a ognuno dei quali si associa un diverso grado di re-identificazione e da cui, in ultima analisi, consegue l'applicazione o meno del GDPR⁵⁶.

Si noterà che questa impostazione ha un effetto significativo: i titolari del trattamento sarebbero davvero incentivati a percorrere la via di una pseudonimizzazione seria e sistematica, poiché ciò implica una loro minor esposizione a responsabilità

54. OCSE, *Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21 March 2014, p. 14 ss.

55. In questi termini TORREGIANI 2020, p. 328.

56. In questi termini anche IRTI 2022, p. 53 ss.

giuridica. Ne deriverebbe, su larga scala, una tutela più efficace dei diritti e delle libertà degli interessati.

4. Conclusioni: verso un modello di governance dei dati basato sul rischio e sul contesto

La sentenza *Deloitte* costituisce un punto di snodo nel percorso di progressiva relativizzazione della nozione di dato personale, ponendo in evidenza come l'identificabilità non sia una qualità intrinseca dell'informazione, bensì il risultato di una valutazione che dipende dal contesto del trattamento e dai mezzi concretamente disponibili in capo al soggetto che tratta i dati.

Nel riconoscere che un dato pseudonimizzato possa assumere natura diversa a seconda del destinatario e delle sue capacità di re-identificazione, la Corte di giustizia prende definitivamente le distanze da una concezione statica e assoluta del dato, aprendo la strada ad un modello fondato sulla relazione tra dato e informazione personale, tra soggetto e ambiente tecnologico.

Tale approdo giurisprudenziale si inserisce in un ecosistema digitale in cui il dato tende a perdere il proprio ancoraggio all'oggetto materiale, soprattutto nei contesti di *cloud computing* che dematerializzano i dati in luoghi virtuali e rendono difficile il diretto controllo dell'interessato⁵⁷.

In tale quadro, il dato personale non coincide con un bene di cui il soggetto dispone, ma rappresenta una proiezione della persona nello spazio

pubblico digitale, con il rischio di "un'intimità (...) sradicata"⁵⁸, che richiede all'utente di non essere relegato al ruolo di mero spettatore del contesto digitale in cui è immerso ma di esercitare la propria autodeterminazione informativa⁵⁹.

Tuttavia, è necessario muovere dalla consapevolezza che l'individuo non è più in grado di mitigare i nuovi potenziali rischi attraverso i tradizionali strumenti di tutela basati sul consenso e sull'autodeterminazione, in quanto "i dati generano altri dati"⁶⁰, sempre più spesso creati senza il diretto coinvolgimento dell'individuo stesso.

Da qui discende la necessità di ripensare il valore da riconoscere alle tecniche di anonimizzazione e pseudonimizzazione dei dati al fine di valorizzare una protezione efficace dei dati personali e di accettare una governance dinamica del GDPR⁶¹.

Come evidenziato, la tradizionale concezione dell'anonimizzazione come "stato del dato"⁶² e strumento idoneo a recidere il legame tra dato e persona appare da tempo insufficiente se non accompagnata da una valutazione contestuale e dinamica del rischio di re-identificazione⁶³.

La nozione stessa di dato anonimo risulta problematica, generando l'illusione di un confine definitivo tra dati personali e non personali che, nella realtà tecnologica contemporanea, risulta sempre più difficile da sostenere⁶⁴. Per questa ragione, il criterio fondato sul rischio accolto dal considerando 26 del GDPR sembra rappresentare il parametro più idoneo.

57. GALIANO-LEOGRANDE-MASSARI-MASSARO 2020, p. 63. Sui diritti dell'interessato v. CALISAI 2019, p. 327 ss.; COLAPIETRO-IANNUZZI 2017, p. 85 ss.

58. ESPOSITO 2021, p. 498.

59. Sul fondamentale ruolo del consenso v. CAGGIA 2019, p. 249 ss.; COLAPIETRO-IANNUZZI 2017, p. 85 ss.

60. ABRAMS 2014, p. 9.

61. Si individuano quattro modelli emergenti di governance dei dati che rappresentano diverse configurazioni del rapporto tra dato, attori e ambiente tecnologico: le *Data Sharing Platforms* (DSP), cioè iniziative tra titolari di dati, che aggregano dati provenienti da fonti diverse per creare maggiore valore attraverso la loro combinazione; le *Data Cooperatives* (DC), che introducono una dimensione maggiormente partecipativa, in cui i soggetti dei dati assumono un ruolo attivo nella gestione collettiva delle informazioni; *Public Data Trusts* (PDT), in cui è il soggetto pubblico ad assumere il ruolo di fiduciario dei dati. In questo caso, la governance si basa su un rapporto di fiducia istituzionalizzata tra cittadini ed enti pubblici, con l'obiettivo di garantire un uso etico e orientato al bene comune dei dati; *Personal Data Sovereignty* (PDS), che attribuisce ai soggetti dei dati un controllo diretto sulle proprie informazioni attraverso spazi personali dei dati. Sul punto v. MICHELI-PONTI-CRAGLIA-BERTI SUMAN 2020.

62. BOLOGNINI-BISTOLFI 2016, p. 2.

63. Cfr. VIOLA DE AZEVEDO CUNHA-DONEDA-ANDRADE 2010, pp. 641-655.

64. FINCK-PALLAS 2020, p. 20.

Di conseguenza, i titolari del trattamento sono chiamati a garantire un livello di sicurezza adeguato e ad effettuare periodiche valutazioni del rischio di identificabilità, alla luce dei mezzi ragionevolmente utilizzabili dal titolare del trattamento ma anche dal terzo a cui vengono trasferiti i dati, poiché le sue caratteristiche e il suo ambiente tecnologico incidono sulla possibilità di re-identificazione⁶⁵.

Tale dovere di monitoraggio impone di “superare il modello del *release and forget* o, ancor meglio, quello del *release and complete freedom*”⁶⁶ a favore di una maggior responsabilizzazione effettiva degli attori coinvolti nella circolazione dei dati, inclusi i destinatari di dataset formalmente anonimizzati, i quali non possono ritenersi del tutto estranei alla disciplina del GDPR, anche se non sono (ancora) titolari del trattamento.

Questo approccio consente, da un lato, di salvaguardare la circolazione delle informazioni, in quanto la qualificazione di un dataset come anonimo, e dunque come dato non personale, non comporta soltanto l'uscita dall'ambito applicativo del GDPR, ma produce un effetto di vera e propria “liberalizzazione regolatoria”, consentendo una circolazione significativamente più ampia del dato, anche in contesti globali di *cloud computing*, *data sharing* e sviluppo di sistemi di intelligenza artificiale, favorendo, così, il riutilizzo dei dati⁶⁷; dall'altro, permette di modulare il livello di tutela in funzione dei rischi concreti per gli interessati, conducendo ad una concezione graduale del dato, a beneficio della ricerca scientifica, dello sviluppo di algoritmi di intelligenza artificiale e, più in generale, di molte aziende, per le quali si apre una nuova stagione di *compliance*, orientata ad una conformità alla legge non più passiva ma proattiva.

In altri termini, la nozione dinamica di dato personale ha il carattere della reversibilità: se da un lato, il dato pseudonimizzato può essere anonimo – e quindi non personale – per un terzo soggetto che lo tratta e non è in grado di identificare

il potenziale interessato, dall'altro, se un soggetto che tratta dati anonimi è materialmente in grado di re-identificare l'interessato, allora il “dato” riacquisisce il suo carattere “personale” e quel terzo diventa un titolare/responsabile del trattamento cui si applica il GDPR.

A tal fine, i titolari del trattamento e, fra questi, in modo particolare le imprese dovranno guidare l'innovazione, secondo una modalità che tende a valorizzare il ruolo centrale del DPO, attraverso solidi programmi di governance che richiedono di mappare i flussi e il regime tecnico dei dati, integrare le nuove tecnologie (come l'IA) e applicare con attenzione e lungimiranza le misure di pseudonimizzazione e anonimizzazione, in modo da poter dimostrare, in ogni momento, che il titolare non persegue, quale finalità del trattamento, l'identificazione delle persone fisiche e, di conseguenza, adotta misure idonee ad impedirne l'identificazione.

La prospettiva adottata dalla Corte di giustizia nella sentenza *Deloitte* si presta, dunque, ad essere letta come espressione di una più ampia evoluzione del diritto alla protezione dei dati personali, mostrando come sia sufficiente cambiare lo sguardo sulle norme già esistenti del GDPR, in quanto quest'ultimo è in grado di adattarsi all'innovazione tecnologica mediante i criteri di ragionevolezza e bilanciamento.

Anche le autorità di *data protection* dovranno ora tenere conto di questa nuova lettura del dato normativo, che supera la distinzione “sculpta nella pietra” tra dato anonimo e dato personale e apre la strada ad un modello di protezione dei dati fondato sulla responsabilizzazione del soggetto che tratta i dati, quando questi sono effettivamente personali, e su una valutazione elastica, orientata dall'uso in concreto delle informazioni personali.

Si tratta, in ultima analisi, di un orientamento non distante da un' impostazione che valorizza il principio di lealtà nel trattamento dei dati personali e che sembra farsi strada anche nella dottrina di oltreoceano⁶⁸.

65. ELLIOT-O'HARA-RAAB et al. 2018 propongono una “anonimizzazione funzionale”, cioè un approccio che considera anche l'ambiente di trattamento del dataset e che richiede al titolare del trattamento di progettare tale ambiente, prevedendo chiare responsabilità in relazione alla comprensione dei rischi, alla predisposizione di controlli di accesso e di un piano per gli eventi avversi.

66. STALLA-BOURDILLON-KNIGHT 2017, p. 37.

67. Sul diritto alla protezione e alla circolazione dei dati, con particolare attenzione ai vantaggi derivanti dall'anonimizzazione v. FORESTA 2024.

68. RICHARDS-HARTZOG 2021; RICHARDS-HARTZOG-FRANCIS 2023.

Riferimenti bibliografici

- M. ABRAMS (2014), *The origins of Personal Data and its implication for Governance*, in SSRN, 2014
- C. AMALFITANO, F. FERRI (2023), *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. Torino, S. Zorzetto (a cura di), "La trasformazione digitale in Europa. Diritti e principi", Giappichelli, 2023
- P. BARILE (1987), *Democrazia e segreto*, in "Quaderni costituzionali", 1987, n. 1
- L. BOLOGNINI, C. BISTOLFI (2016), *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation*, in "Computer Law & Security Review", vol. 33, 2016, n. 2
- F. CAGGIA (2019), *Libertà ed espressione del consenso*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019
- F. CALISAI (2019), *I diritti dell'interessato*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019
- S. CALZOLAIO (2023), *Dalla protezione dei dati personali all'ordinamento dei dati (l'evoluzione del diritto cinese e del diritto europeo dei dati)*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023
- S. CALZOLAIO (2017), *Protezione dei dati personali*, voce in "Digesto delle discipline pubblicistiche. Aggiornamento", 2017
- C. 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
- C. COLAPIETRO, A. IANNUZZI (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679", Editoriale Scientifica, 2017
- E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di) (2022), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, 2022
- G. D'ACQUISTO, M. NALDI (2017), *Big Data e privacy by Design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli, 2017
- F. DI RESTA (2018), *La nuova "privacy europea"*, Giappichelli, 2018
- M. ELLIOT, K. O'HARA, C. RAAB, C.M. O'KEEFE, E. MACKEY, C. DIBBEN, H. GOWANS, K. PURDAM, K. McCULLAGH (2018), *Functional Anonymisation: Personal Data and the Data Environment*, in "Computer Law & Security Review", vol. 34, 2018, n. 2
- A. ESPOSITO (2021), *Dove sono i "miei" dati? Privacy e reificazione nell'era digitale*, in "Etica & Politica/Ethics & Politics", vol. XXIII, 2021, n. 1
- F. FAINI (2023), *Il dato personale tra protezione giuridica e valorizzazione economica*, in "Osservatorio sulle fonti", 2023, n. 2
- M. FINCK, F. PALLAS (2020), *They who must not be identified – distinguishing personal from non-personal data under the GDPR*, in "International Data Privacy Law", 2020, n. 1
- C. FOGLIA (2019), *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in R. Panetta (a cura di), "Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 e al novellato d.lgs. n. 196/2003", Giuffrè, 2019

- D. FORESTA (2024), *Pseudonimizzazione e anonimizzazione dei dati personali contenuti nelle decisioni giudiziarie*, in “Persona e Mercato”, 2024, n.1
- A. GABEL, I. SCHIERING (2018), *Privacy Patterns for Pseudonymity*, in E. Kosta, J. Pierson, D. Slamanig (Eds.), “Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data”, Springer, 2018
- 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
- C. IRTI (2022), *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised, De-identified Data*, in R. Senigaglia, C. Irti, A. Bernes (Eds.), “Privacy and Data Protection in software services”, Springer, 2022
- A. LEE BYGRAVE, C. DOCKSEY, C. KUNER (2020), *The EU General Data Protection Regulation (GDPR): a commentary*, Oxford University Press, 2020
- M.L. MONTAGNANI (2019), *La libera circolazione dei dati al bivio: tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in “Mercato, concorrenza, regole”, 2019, n. 2
- M. MICHELI, M. PONTI, M. CRAGLIA, A. BERTI SUMAN (2020), *Emerging models of data governance in the age of datification*, in “Big data and society”, 2020, n. 2
- A. NICITA (2019), *Il dato profilato nella prospettiva economica tra privacy, propertization, secrecy*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), “I dati personali nel diritto europeo”, Giappichelli, 2019
- P. OHM (2010), *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in “UCLA Law Review”, 2010
- M. PALMIRANI (2019), *Prefazione*, in F. Faini, “Data society”, Giuffrè, 2019
- P. PASSAGLIA (2016), *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in “Consulta online”, 2016, n. 3
- G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di) (2018), *GDPR e normative privacy: commentario*, Wolters Kluwer, 2018
- N. RICHARDS, W. HARTZOG (2021), *A Duty of Loyalty for Privacy Law*, in “Washington University Law Review” vol. 99, 2021, n. 961
- N. RICHARDS, W. HARTZOG, J. FRANCIS (2023), *A concrete proposal for data loyalty*, in “Harvard Journal of Law & Technology”, vol. 37, 2023, n. 3 Symposium
- P.M. SCHWARTZ, D.J. SOLOVE (2011), *The PII problem: privacy and a new concept of personally identifiable information*, in “New York University Law Review”, 2011
- S. STALLA-BOURDILLON, A. KNIGHT (2017), *Anonymous data v. personal data – a false debate: an Eu perspective on anonymization, pseudonymization and personal data*, in “Wisconsin International Law Journal”, 2017
- L. SWEENEY (2000), *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, 2000
- S. TORREGIANI (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1870: tra anonimizzazione, ownership e Data by design*, in “federalismi.it”, 2020, n. 18
- C.A. TROVATO, C. RAUCCIO (2022), *L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia “dato personale-non personale”*, in “Ciberspazio e Diritto”, 2022, n. 2
- M. VIOLA DE AZEVEDO CUNHA, D. DONEDA, N. ANDRADE (2010), *La reidentificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in “Ciberspazio e diritto”, 2010, n. 4



VILARD BYTYQI

Measures for the metering of telephone calls and the interception of telecommunications in criminal proceedings: Legal aspects and implications for human rights and public safety – The case of Kosovo

This paper deals with the measures of metering of telephone calls and interception of telecommunications in Kosovo, in particular the legal framework, as well as the impact they have on human rights and public safety. From the study of domestic legislation, ECHR standards, and ECtHR jurisprudence, it is evident that investigative measures should be applied only when there are no other less intrusive means to achieve the same goal. The paper deals with the content of the standards of Directive 2014/41/EU on the European Investigation Order, assessing that, although Kosovo has no formal obligations towards it, as it is in the pre-accession phase, the harmonization of its legislation in this field with European standards is necessary. The results of this study show that, although these measures are necessary for the fight against organized crime and the strengthening of public safety, they carry real risks for fundamental rights, in particular the right to privacy, freedom of expression, and freedom of thought. Their misuse can damage citizens' trust in state institutions and violate the essence of guaranteed rights. In conclusion, it is recommended to strengthen judicial oversight, increase institutional transparency, and harmonize Kosovo's legislation with international standards.

Metering of telephone calls – Interception of telecommunications – Right to privacy – Public safety – Human rights

Misure di acquisizione dei dati di traffico telefonico e intercettazione delle telecomunicazioni nel procedimento penale: aspetti giuridici e implicazioni per i diritti umani e la sicurezza pubblica – L'esperienza del Kosovo

Il contributo analizza le misure di acquisizione dei dati di traffico telefonico e di intercettazione delle telecomunicazioni nel procedimento penale in Kosovo, con riguardo al quadro normativo e al loro impatto sui diritti umani e sulla sicurezza pubblica. Dall'analisi della legislazione nazionale, degli standard della CEDU e della giurisprudenza della Corte EDU emerge che tali misure investigative dovrebbero essere applicate solo quando non siano disponibili altri strumenti meno invasivi. Sono esaminati inoltre gli standard previsti dalla Dir. 2014/41/UE sull'Ordine europeo di indagine penale, rilevando che, sebbene il Kosovo non sia formalmente vincolato a essa, risulta comunque necessaria un'armonizzazione della normativa nazionale con gli standard europei. Lo studio evidenzia che, pur essendo essenziali per contrastare la criminalità organizzata e rafforzare la sicurezza pubblica, tali misure comportano rischi per i diritti fondamentali, in particolare per il diritto alla vita privata e le libertà di espressione e di pensiero. Un loro uso improprio o sproporzionato può compromettere la fiducia dei cittadini nelle istituzioni pubbliche e incidere sull'essenza dei diritti. In conclusione, si raccomanda di rafforzare il controllo giurisdizionale, incrementare la trasparenza istituzionale e armonizzare ulteriormente la legislazione del Kosovo con gli standard internazionali ed europei in materia.

*Acquisizione dei dati di traffico telefonico – Intercettazione delle telecomunicazioni – Diritto alla privacy
Sicurezza pubblica – Diritti umani*

SUMMARY: 1. Introduction. – 2. Methodology. – 3. Definition of the measure of metering of telephone calls and interception of telecommunications. – 4. Fundamental principles for the implementation of the measure of interception of telecommunications. – 5. Circumstances and conditions for authorizing the implementation of measures of metering of telephone calls and interception of telecommunications. – 6. EU Directive on the European Investigation Order in criminal matters. – 7. Human rights exposed to risk during the implementation of special investigative measures. – 8. The strategic combination of special investigative measures in criminal investigations. – 9. The role and impact of measures of interception and metering of telephone calls on public safety. – 10. Conclusion.

1. Introduction

Contemporary states are increasingly confronted with serious forms of criminality, such as criminal offenses related to terrorism, corruption, and organized crime. The societal necessity to address criminality in an effective manner has led to the inclusion of covert and technical surveillance and investigative measures within the repertoire of mechanisms for the detection and evidentiary substantiation of criminal offenses in almost all contemporary criminal procedural legislations¹. Traditional investigations, which are essentially reactive, have become increasingly ineffective in tackling modern crime, particularly organized and complex crime. This has made it necessary to advance proactive investigations led by intelligence and the use of covert investigative measures². The modern evolution of organized crime, as well as corruption, has led to the implementation of proactive intelligence-led investigations, as well as the use of special investigative techniques, including communications interception, as essential tools for securing evidence³. Intelligence-led and data-driven investigative techniques, when insufficiently supported by empirical verifica-

tion and lacking appropriate procedural safeguards, can lead to investigative bias, tunnel vision and, in some cases, serious miscarriages of justice. This reinforces the need for strict legal regulation, effective judicial oversight and proportionate enforcement of these measures⁴. Furthermore, research shows that advanced investigative techniques, when implemented without sufficient institutional capacity, without procedural guarantees and without effective judicial control, often remain largely formal and fail to achieve the objectives for which they were intended in practice⁵.

In the context of technological developments and the increase in criminal offences related to their use, measures of metering of telephone calls and interception of telecommunications have become important legal instruments for criminal investigation and prosecution in Kosovo. The Criminal Procedure Code and the Law on Interception of Electronic Communications constitute the legal basis for the implementation of these measures, which play an important role in the detection of criminal offences, especially in the fight against organized crime and corruption. However, the

1. SAHITI–MURATI–ELSHANI 2014.

2. Council of Europe, *Deployment of Special Investigative Means*, Council of Europe Office in Belgrade, 2013.

3. CONTE 2010.

4. DEVERY 2010.

5. MAGUIRE–KING 2013.

implementation of these measures should not be treated as an instrument that is easily used for investigative purposes. Their use should only be considered when other less intrusive means have proven unsuccessful or for other justified reasons⁶. The balance between public security interests and the protection of human rights is essential, given that a democratic society cannot rely solely on the power of surveillance, but must at the same time guarantee fundamental freedoms and rights. Another important issue that has emerged in the efforts to prevent and combat terrorism and organized crime is precisely related to this balance between security interests and human rights. Today, there are different approaches to this relationship, which try to define stable boundaries and clear guarantees between the protection of fundamental rights and freedoms and the interests of national security⁷. In light of these contemporary developments, the Republic of Kosovo has foreseen in its legislation the possibility of applying special investigative measures, when the legal conditions are met, including, among others, the implementation of measures of metering of telephone calls and interception of telecommunications.

The Republic of Kosovo has included these measures in its legislation, aiming to harmonize with international human rights standards, such as those set out in the ECHR and the jurisprudence of the ECtHR. However, challenges in the fair and proportionate implementation of these measures remain, including the need for effective judicial oversight and transparency in investigative procedures.

This study aims to identify and analyze the legal provisions that regulate the measures of telephone call metering and telecommunications interception in Kosovo, examining in particular their compatibility with the Constitution of the Republic of Kosovo and the ECHR. It also aims to analyze the impact that these measures have on public security and the protection of human rights. Through this research, it is intended to contribute to the development of a fairer and more effective legal framework, which guarantees a sustainable balance between the need for public safety and the protection of the fundamental rights of citizens.

2. Methodology

This study is based on an in-depth examination of Kosovo's legal framework and international standards regulating the measures of metering of telephone calls and interception of telecommunications. Legal Analysis Method: Domestic laws, including the Criminal Procedure Code of Kosovo and the Law on Electronic Interceptions, have been reviewed to identify definitions, rules, and procedures governing the implementation of these measures. Additionally, the Constitution of the Republic of Kosovo and the provisions of the European Convention on Human Rights have been analyzed to assess the compliance of national legislation with international standards. Comparative Method: The paper includes a comparison of Kosovo's legislation with European Union directives, particularly Directive 2014/41/EU on the European Investigation Order in Criminal Matters. This comparison aims to identify gaps and opportunities for improving Kosovo's legal framework. Jurisprudence Analysis: The study examines decisions of the European Court of Human Rights related to electronic surveillance and interception, identifying best practices and standards that Kosovo's institutions should follow. Literature Review: The research is also supported by analyses of legal doctrine and relevant scholarly literature addressing issues of human rights, public safety, and special investigative measures. Through this methodology, the paper aims to provide a comprehensive overview of metering and interception measures in Kosovo, offering concrete recommendations for improving the legal framework and institutional practices in line with international standards.

3. Definition of the measure of metering of telephone calls and interception of telecommunications

The measures of "metering of telephone calls" and "interception of telecommunications" are two special investigative measures provided by the Criminal Procedure Code of Kosovo. Essentially, both measures are similar, but they differ in the type of

6. United Nations Office on Drugs and Crime, *Current practices in electronic surveillance in the investigation of serious and organized crime*, United Nations Publications, 2009.

7. SELVADURAI-KISSWANI-KHALAILEH 2016.

evidence that can be obtained from each measure, as well as in the authorities that authorize these measures.

This distinction becomes increasingly blurred in technologically advanced investigative practices. As highlighted in comparative legal scholarship, digital investigative tools are often capable of simultaneously collecting metadata, intercepting communications, and accessing stored data, thereby expanding the scope of intrusion far beyond traditional interception measures⁸.

The measure of “metering of telephone calls” refers to the collection of data from telephone calls made from a specific phone number (incoming and outgoing), including but not limited to the verification of the specific number’s identification, telephone number verification, geographic location, device location, subscriber verification, or device identification marks (IMEI)⁹. For the purposes of this paper, metering of telephone calls refers to traffic and location data (metadata) and does not include the content of communications, whereas interception of telecommunications refers to accessing the content of communications. The measure of “interception of telecommunications” refers to the interception of voice communications, text communications, or other forms of communication through fixed or mobile telephone networks. This includes any technological means or similar systems that transmit data primarily intended to be private¹⁰. A similar definition to that provided by the Criminal Procedure Code is given by the Law on Electronic Interceptions, which stipulates that the interception of electronic communications refers to the interception of voice communications, text communications, or other forms of communication through fixed or mobile telephone networks. This includes any technological means or similar systems that transmit data primarily intended to be private¹¹.

4. Fundamental principles for the implementation of the measure of interception of telecommunications

The Law on the Interception of Electronic Communications establishes two fundamental principles on which interception can be conducted. The first principle is the respect for human rights and freedoms, and the second is the principle of legality, specifically the issuance of a judicial order for the implementation of the interception¹². The law clarifies the first principle, which implies the full implementation and respect of the constitutional principles, rules, and standards that guarantee the freedoms and human rights defined by the Constitution and the jurisprudence of the European Court of Human Rights (ECHR). The jurisprudence of the ECHR is one of the judicial practices that must be respected by the justice system in Kosovo, particularly by the judiciary, as Article 53 of the Constitution of the Republic of Kosovo stipulates: “Human rights and fundamental freedoms guaranteed by this Constitution shall be interpreted in harmony with the judicial decisions of the European Court of Human Rights”¹³. The Law on Electronic Interceptions also places special emphasis on the respect for the principle of legality, while incorporating judicial oversight of the measure to be implemented, in this case, the interception measure. This is in line with the Criminal Procedure Code, as the CPC explicitly requires adherence to all rules governing special investigative measures; otherwise, “Evidence obtained through a special investigative measure shall be inadmissible if the order for the measure and its implementation is unlawful”¹⁴.

In addition to adhering to the procedures for authorizing a specific order, the Law on Electronic Interceptions also prescribes special conditions

8. FLOR-PANATTONI 2023.

9. Art. 85(12), Criminal Procedure Code, Official Gazette of the Republic of Kosovo, No. 24/2022, 17 August 2022, Code No. 08/L-032.

10. *Ivi*, Art. 85 (4).

11. Art. 3(1)(3), Law on Interception of Electronic Communications, Official Gazette of the Republic of Kosovo, No. 18/2015, 13 July 2015, Law No. 05/L-030.

12. *Ivi*, Art. 4 (1).

13. Art. 53, Constitution of The Republic of Kosovo, Official Gazette of the Republic of Kosovo, No. 20/2008, 15 June 2008, Act No. K-09042008.

14. Art. 95(1), Criminal Procedure Code.

that must be respected when issuing the order, which are in accordance with the Constitution of the Republic of Kosovo and the European Convention on Human Rights. These special conditions include situations that contain the following elements. When making the decision for interception, the competent court has the obligation to ensure:

- the essence of the rights and freedoms of the individuals for whom the interception request has been made;
- the importance, necessity of the interception, and proportionality;
- the nature, means, and scope of the interception;
- the relationship between the intended objective and the possibility of achieving this objective through other investigative methods; and
- the confidentiality and objectivity during the execution of the interception¹⁵.

5. Circumstances and conditions for authorizing the implementation of measures of metering of telephone calls and interception of telecommunications

The measure of “metering of telephone calls” can be ordered only by the State Prosecutor in accordance with Article 86 (1)(9), while the measure of “interception of telecommunications” can be ordered only by the pre-trial judge in accordance with Article 86 (2)(3). Regarding the order for the interception of telecommunications, the law stipulates that only the state prosecutor may submit a request for the authorization of the interception measure. The law explicitly specifies the institutions or agencies that may submit a request to the state prosecutor to initiate the procedures for the interception order. In this regard, the law provides that the authorized institutions to propose a request to the State Prosecutor for lawful interception for the purposes of criminal procedure are: the Kosovo Police, the Kosovo Customs, the Kosovo Police Inspectorate, the Kosovo Tax Administration, and the European Union Rule of

Law Mission in Kosovo (EULEX), in accordance with the competencies granted by the legislation in force in the Republic of Kosovo¹⁶.

Both of these special investigative measures may be authorized for implementation within the legal deadlines specified in Article 91 of the Criminal Procedure Code. They must begin to be implemented within 15 days from the date the order is issued and are valid for a period of up to 90 days. The duration may be extended for an additional 90-day period, with all extensions falling within a total period of one calendar year, i.e., 365 days. The order for metering of telephone calls must include all elements necessary for identifying each specific phone. The order for the interception of telecommunications must contain all elements required for identifying each phone subject to interception¹⁷.

The order for the interception of telecommunications and the use of the IMSI (International Mobile Subscriber Identity) catcher used to identify mobile users, the interception of telecommunications through computer networks, the metering of telephone calls, the inspection of postal deliveries, the controlled delivery of postal items, or the disclosure of financial data must include an additional written instruction for individuals, other than authorized police officers, whose assistance may be necessary for the implementation of the order. This written instruction must be sent to the director or responsible official of the telecommunications system, computer network, postal service, bank, or other financial institutions and should include only the information required to assist in the execution of the order¹⁸.

When implementing the order for the interception of telecommunications and the use of the IMSI catcher, the interception of telecommunications through computer networks, the inspection of postal deliveries, the controlled delivery of postal items, and the metering of telephone calls, the individuals responsible for managing telecommunications, computer networks, or postal services must facilitate the execution of the order under the supervision of the director or the re-

15. Art. 4 (2), Law on Interception of Electronic Communications.

16. *Ivi*, Art. 8 (1) and (2).

17. Art. 90 (6), Criminal Procedure Code.

18. *Ivi*, Art. 90 (10).

sponsible official of the telecommunications system, computer network, or postal service¹⁹.

At the request of the State Prosecutor, the order for the interception of telecommunications and the use of the IMSI catcher may include only a general description of the phones that can be intercepted when the pre-trial judge of the competent basic court determines that there is a well-founded suspicion that the suspect is using multiple phones to evade surveillance by authorized police officers; and that the phone or phones specified in the order are being used or will be used by the suspect²⁰.

When the order for the interception of telecommunications and the use of the IMSI catcher has been issued by the pre-trial judge, after the execution of the order for a specific phone, the authorized police officers must immediately inform the judge in writing about the relevant facts, including the phone number²¹. It is very important to emphasize that every order issued by the judge must be executed in full compliance with the contents of the issued order, and the conditions and procedures under which such an order is issued must not be exceeded. In this regard, it cannot be used to intercept the telecommunications of a person who is not a suspect, as this would be in violation of the rules established by the Criminal Procedure Code on this matter.

According to Kosovo legislation, the competence to authorize and supervise special investigative measures belongs exclusively to the prosecutorial and judicial authorities, and their implementation is carried out through special technical equipment deployed and administered by public authorities, namely the Kosovo Police. In this sense, the execution of the measure remains under state institutional control and does not involve operational cooperation with private entities. Contemporary literature has noted that modern surveillance practices increasingly operate through forms of structural integration between state authorities and “private surveillance intermediaries”. As Keenan argues, the material basis of surveillance has gradually shifted from direct state-controlled

interception to a systemic dependence on privately owned communication infrastructure and digital platforms²². Although Kosovo has a clear system whereby only public authorities authorize these measures, their implementation in practice depends on private technological infrastructure. This raises important issues regarding transparency and effective judicial oversight. For this reason, proportionality must not only be assessed at the moment of formal authorization, but also during the implementation of the measure, ensuring that it remains within the limits established by law in a democratic society.

6. EU Directive on the European Investigation Order in criminal matters

The European Union has established specific standards and rules that serve as a basis for developing national legislation, specifically to harmonize them with EU directives in the field of surveillance. In this regard, Directive 2014/41/EU of the European Parliament and the Council, dated April 3, 2014, concerning the European Investigation Order in criminal matters, is of particular importance.

This directive stipulates that the European Investigation Order is a judicial decision issued or validated by a judicial authority of a Member State to carry out one or more specific investigative measures in another Member State (“the executing state”) to obtain evidence for criminal matters in accordance with the directive. The European Investigation Order may also be issued for the collection of evidence already in the possession of the competent authorities of the executing state, evidence that has already been gathered through another procedure conducted by national authorities but is relevant to criminal proceedings in other states. Member States shall execute a European Investigation Order based on the principle of mutual recognition and in accordance with the directive²³.

This directive also addresses the issue of interception of telecommunications in Chapter V. It deals with the interception of telecommunications

19. *Ivi*, Art. 91 (5).

20. *Ivi*, Art. 90 (7).

21. *Ibidem*.

22. KEENAN 2025.

23. Art. (1)(3), Directive 2014/41/EU.

in the context of mutual cooperation between the Member States of the European Union and does not include third countries that are not part of the EU. In this regard, this instrument cannot serve as a basis for cooperation with third countries that do not have legal ties with the European Union as its Member States. All the 27 EU Member States can use this instrument as a platform for implementing special investigative measures in accordance with the EU legal framework and the internal legal rules governing national procedures.

The Republic of Kosovo has no obligations toward this directive and cannot use it as a basis for cooperation, specifically for requests for assistance or technical support with EU Member States. However, such requests must be made in accordance with the specific rules of international criminal law that govern the aspect of inter-state cooperation in criminal matters.

A European Investigation Order may be issued for the interception of telecommunications in the Member State from which technical assistance is required. When more than one Member State is capable of providing the full technical assistance necessary for the same interception of telecommunications, the European Investigation Order shall be sent to only one of them. Priority shall always be given to the Member State where the subject of the interception is or will be located. Such a European Investigation Order shall also include the following information:

- (i) information for the purpose of identifying the subject of the interception;
- (ii) the desired duration of the interception; and
- (iii) sufficient technical data, in particular the identifier of the target, to ensure that the European Investigation Order can be executed²⁴.

The issuing authority, in this case the state issuing the order, shall clarify in the European Investigation Order the reasons why it considers such an investigative measure important for the purpose of the criminal proceedings. Additionally, on well-founded grounds, the state from which such assistance is requested may refuse to execute such an order²⁵. In

addition, recent case law of the Court of Justice of the European Union has highlighted that access by competent authorities to retained traffic and location data represents a substantial interference with the rights to privacy and data protection. Consequently, such access may be justified only for the purpose of combating serious crime or preventing serious threats to public safety. The Court further emphasized that access to such data must be subject to prior review by a court or an independent administrative authority. A public prosecutor's office that directs the pre-trial procedure and subsequently acts as a party to the proceedings does not meet the required standard of independence²⁶.

In this context, early academic commentary on the proposed European Investigation Order warned that a "one-size-fits-all" mutual recognition model, adopted in the absence of harmonized admissibility and procedural standards, could undermine equality of arms and the effective protection of fundamental rights²⁷. These concerns reflected broader structural tensions inherent in the mutual recognition framework, particularly in the absence of fully harmonized criminal procedural safeguards across Member States.

The European Investigation Order is founded on the principle of mutual recognition but does not fully harmonize the legal criteria allowing the use of intrusive investigative measures. As Armada points out, the Directive gives cross-border effect to national decisions on the gathering of evidence, while the assessment of necessity and proportionality remains primarily within the competence of the issuing authority. This may lead to differences in the level of fundamental rights protection between Member States, in particular with regard to the right to respect for private life under Article 8 of the European Convention on Human Rights. Although the Directive provides for the possibility of refusing execution on grounds of fundamental rights protection, the practical effectiveness of this guarantee depends on its interpretation and practical implementation by national law enforcement authorities²⁸.

24. *Ivi*, Art. (30)(1-3).

25. *Ivi*, Art. (30)(4-5).

26. CJEU, *H.K. v. Prokuratuur*, Case C-746/18 (Grand Chamber), ECLI:EU:C:2021:152.

27. HEARD-MANSELL 2011.

28. ARMADA 2015.

Furthermore, the Directive does not expressly regulate the so-called principle of speciality in the context of cross-border gathering of evidence, namely the limitations on the use of evidence obtained through the European Investigation Order for purposes or proceedings other than those for which it was initially requested. As Barbosa e Silva notes, this silence has generated doctrinal debate and divergent practices among Member States, in particular as regards the further use of evidence once it has been transferred on the basis of the principle of mutual recognition. In the absence of a clear limitation, the free movement of evidence within the European Union framework may raise concerns not only in terms of legal certainty but also in relation to procedural fairness under Article 6 of the ECHR and, depending on the nature of the investigative measure, regarding the protection of private life under Article 8 of the ECHR. For this reason, a clearer expression of the principle of speciality within the framework of the European Investigation Order would contribute to strengthening safeguards against possible abuse and to enhancing the effective protection of fundamental rights²⁹.

Such a European Investigation Order may be executed by: (a) immediately transmitting the telecommunications to the issuing state; or (b) intercepting, recording, and subsequently transmitting the results of the interception of telecommunications to the issuing state. When issuing a European Investigation Order, the issuing authority, if there is a specific reason to do so, may also request a transcription, decoding, or decryption of the recording, subject to the agreement of the executing authority. Additionally, in all situations where the state conducting the interception in another country does not require technical assistance and carries it out independently, it is obligated to notify the state where the interception is being conducted about such a measure and, after the interception is completed, to inform it of the results of the interception³⁰.

7. Human rights exposed to risk during the implementation of special investigative measures

The ECtHR has consistently examined the compatibility of electronic communications interception with Article 8 of the ECHR, in particular in the context of the use of interception in the context of national security and the fight against serious crime. In the cases of *Big Brother Watch and Others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden*, the Court set advanced standards for the assessment of mass interception regimes. According to the content of the judgment, the interception and mass collection of communications are not in principle incompatible with Article 8 of the Convention, but their lawfulness depends entirely on the existence of sufficient and effective safeguards against their arbitrary and abusive use³¹.

In these decisions, the Court identified a set of minimum criteria that must be met to ensure effective control and oversight at all stages of the surveillance process, including authorization, selection of data, storage, analysis and destruction. The Court accepted that sharing intelligence with partners from other states is, in principle, permissible, provided that domestic legal safeguards are met and that sufficient mechanisms exist to guarantee and protect privacy³².

In the light of the above-mentioned cases, the assessment of special investigative measures requires the application of a structured proportionality test to determine whether the fundamental principles governing the restriction of the rights guaranteed by the Convention are actually respected in practice. The European Court of Human Rights has made it clear that such an assessment must examine not only the legal basis of the measure but also its necessity, proportionality, and the existence of effective safeguards against abuse. Some of the rights guaranteed by the Convention are particularly exposed to increased risks in the

29. BARBOSA E SILVA 2019.

30. Art. 31, Directive 2014/41/EU.

31. European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom*. Nos. 58170/13, 62322/14 and 24960/15, Judgment, 13 September 2018; European Court of Human Rights, *Centrum för Rättvisa v. Sweden* No. 35252/08, Judgment, 19 June 2018.

32. European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom*. Nos. 58170/13, 62322/14 and 24960/15, Judgment, 13 September 2018.

context of secret surveillance, in particular the right to respect for private and family life (Article 8), freedom of thought, conscience, and religion (Article 9), and freedom of expression (Article 10).

During the implementation of special investigative measures, these rights are most at risk of being inappropriately restricted, as the rules governing such limitations may not be sufficiently fulfilled. Contemporary scholarship increasingly emphasizes that traditional frameworks based solely on the right to privacy and personal data protection are no longer sufficient to regulate highly intrusive digital investigative measures. As Flor and Panattoni argue, modern digital investigations – particularly those involving advanced technological tools – may compromise not only individual privacy, but also the security, integrity, and reliability of digital systems themselves. Therefore, the authors propose that cybersecurity should be recognized as an autonomous interest that must be balanced alongside public safety and fundamental rights, especially when law enforcement authorities gain covert access to private devices and communication infrastructures³³.

In this regard, concerning the right to respect for private and family life, the ECHR stipulates that public authorities cannot interfere with the exercise of this right except to the extent provided by law and when necessary in a democratic society, in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others³⁴. Similarly, regarding freedom of thought, conscience, and religion, the ECHR provides for the possibility of limiting this right, as it stipulates that the freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health, or morals, or for the protection of the rights and freedoms of others³⁵. Furthermore, freedom of expression also provides for the possibility of limiting this right, as the exercise of these freedoms, which carries duties and responsibilities,

may be subject to such formalities, conditions, restrictions, or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity, or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of confidential information, or for maintaining the authority and impartiality of the judiciary³⁶.

All these rights are also guaranteed by the Constitution of the Republic of Kosovo, specifically: The right to privacy (Article 36), freedom of belief, conscience, and religion (Article 38), freedom of expression (Article 40), and freedom of the media (Article 42).

Article 55 of the Constitution of the Republic of Kosovo provides for the possibility of limiting these rights under conditions specified by the Constitution itself. In this regard, even when the principle of implementing special investigative measures applies, fulfilling one of the fundamental conditions set by the Constitution is necessary, but not sufficient unless other constitutional conditions are also met. The Constitution outlines specific criteria for how constitutionally guaranteed rights can be restricted. Human rights and fundamental freedoms may be limited by law only if such limitation is permitted by the Constitution, but in most cases, the Constitution delegates this authority to the law. These rights and freedoms can only be restricted for purposes allowed by the Constitution and to the extent necessary to achieve the constitutional purpose of the restriction in an open and democratic society. What is particularly important to emphasize is that such limitations must not affect the essence of the guaranteed right. All state bodies, especially the courts, are obligated to ensure the preservation of the essence of the rights or freedoms being limited. Additionally, these bodies must consider the importance of the purpose of the limitation, the nature and extent of the limitation, the relationship between the limitation and its purpose, and, in

33. FLOR-PANATTONI 2023.

34. Art. 8 ECHR.

35. Art. 9 ECHR.

36. Art. 10 ECHR.

particular, whether the purpose of the limitation can be achieved through less restrictive means³⁷.

In this regard, to fulfill the conditions that ensure the restriction is in accordance with the Constitution, the following criteria must be met collectively in every situation:

- a right can only be restricted if it is explicitly defined by law;
- a right can only be restricted to the extent necessary to achieve the purpose for which the restriction is allowed, in an open and democratic society;
- the restriction of a right cannot be made for purposes other than those for which it has been defined;
- when restricting human rights and interpreting such limitations, all public authorities, especially the courts, are obliged to pay attention to the essence of the right being restricted, the importance of the purpose of the restriction, the nature and extent of the restriction, the relationship between the restriction and the intended purpose, and to examine whether the purpose can be achieved through a less restrictive means; and
- the restriction of rights and freedoms guaranteed by this Constitution must in no way deny the essence of the guaranteed right³⁸.

8. The strategic combination of special investigative measures in criminal investigations

Given the complexity involved in proving criminal offences for which special investigative measures are applied, it is recommended that these measures be combined with one another in order to establish a functional and complementary linkage, thereby enabling the collection of the widest possible range of evidence supporting suspicions of criminal conduct. In this context, the measures of metering of telephone calls and interception of telecommuni-

cations may be combined with other special investigative measures, which are authorized either by the State Prosecutor or by the pre-trial judge, in accordance with the competencies defined by the Criminal Procedure Code.

Depending on the nature of the criminal offense being investigated through these special investigative measures, the measures should be combined to ensure that the offense under investigation is proven through multiple methods. The management of a criminal case during the investigation phase of criminal offenses is the responsibility of the State Prosecutor, who leads the investigation of criminal offenses. This responsibility is grounded in the powers derived from the Constitution of the Republic of Kosovo³⁹, the Criminal Procedure Code of Kosovo, the Law on the State Prosecutor⁴⁰, and the Law on the Special Prosecution of the Republic of Kosovo⁴¹.

This approach is also consistent with the standards of the Council of Europe on the use of special investigative measures, which emphasize that the combination of covert investigative techniques should form part of a coordinated investigative strategy, based on reasonable suspicion, proportionality, and the use of less intrusive means whenever such measures are sufficient to achieve the investigative objective⁴².

9. The role and impact of measures of interception and metering of telephone calls on public safety

The measures of metering of telephone calls and interception of telecommunications play a significant role in strengthening public safety, particularly in the prevention, detection, and prosecution of serious criminal offences such as organized crime, terrorism, drug trafficking, and corruption. In these forms of criminality, the complexity of criminal activity and the closed structure of criminal

37. HASANI-ČUKALOVIĆ 2013.

38. Art. 55, Constitution of The Republic of Kosovo.

39. *Ivi*, Art. 109.

40. Law on State Prosecutor, Official Gazette of the Republic of Kosovo, No. 11/2023, 17 May 2023, Law No. 08/L-167.

41. Law on The Special Prosecution Office of the Republic of Kosovo, Official Gazette of the Republic of Kosovo, No. 27/2008, 3 June 2008, Law No. 03/L-052.

42. Council of Europe, Committee of Ministers *Recommendation CM/Rec (2017)6 to member States on “special investigation techniques” in relation to serious crimes including acts of terrorism*, adopted on 5 July 2017.

networks often make the use of covert investigative measures indispensable, as they enable the collection of evidence and the identification of criminal links and networks.

However, the impact of these measures on public safety is also accompanied by serious challenges. Interference with individual privacy, the covert nature of interception, and the potential for selective or politically motivated use pose genuine risks to democracy and to the protection of human rights. In this context, European standards have consistently emphasized the need for robust legal and procedural safeguards in order to prevent arbitrary and abusive practices in the application of special investigative measures⁴³. In this regard, the jurisprudence of the European Court of Human Rights has emphasized that even when interception and recording measures are aimed at combating serious crime, interference with privacy must not only pursue a legitimate aim but must also be “in accordance with the law”, which requires the existence of a clear, accessible legal basis accompanied by safeguards against arbitrary interference. In *Khan v. the United Kingdom*, the Court found a violation of Article 8 precisely due to the absence of a statutory legal framework governing the use of covert listening devices, holding that a non-binding and not directly accessible guideline was insufficient to meet the “in accordance with the law” standard. The Court further found a violation of Article 13 on account of the lack of an effective and independent remedy against abuse of this form of interference⁴⁴. These standards reinforce the necessity of judicial control and institutional oversight as essential conditions for maintaining the balance between public safety and fundamental rights. This approach is also consistent with United Nations guidelines on criminal investigations, which emphasize that the use of intrusive measures by law enforcement authorities must be necessary, proportionate, and accompanied by effective safeguards for the protection of human rights, in order for investigations to remain legitimate in a democratic society⁴⁵.

For this reason, the implementation of interception measures and the metering of telephone

calls must be grounded in the principles of proportionality and necessity, and limited exclusively to cases in which such measures are indispensable for achieving a legitimate public safety objective and where less intrusive means are insufficient. Effective judicial oversight and robust institutional supervision constitute essential guarantees for preserving the balance between security interests and the protection of individual freedoms and fundamental rights, ensuring that these measures are applied lawfully and proportionately within a democratic society.

10. Conclusion

This paper has comprehensively addressed the measures of metering of telephone calls and interception of telecommunications in Kosovo, analyzing the legal aspects and the impact these measures have on human rights and public safety. The research has identified a range of challenges in balancing the need for security with the respect for privacy and the fundamental freedoms of citizens.

Kosovo’s legislation, including the Criminal Procedure Code and the Law on Electronic Interceptions, provides a legal basis for the implementation of special investigative measures. However, gaps exist in compliance with international human rights standards, particularly with the European Convention on Human Rights and the jurisprudence of the European Court of Human Rights. One of the key challenges identified is the lack of strong judicial oversight and institutional transparency during the implementation of these measures. This creates room for potential abuses and violations of citizens’ rights, especially if these measures are used outside the context of investigative necessity.

The implementation of metering and interception measures should be based on the principle of proportionality, being used only when less intrusive alternatives do not exist. Their use must be justified by a real threat to public safety and not as a routine investigative tool. The interception and metering of calls expose several fundamental rights to risk, including the right to privacy (Arti-

43. *Ibidem*.

44. European Court of Human Rights, *Khan v. the United Kingdom*, No. 35394/97, Judgment, 12 May 2000.

45. United Nations Office of the High Commissioner for Human Rights, *Manual on Human Rights for Law Enforcement Officials*, Professional Training Series No. 5/Rev.1, United Nations, 2025.

cle 8 of the ECHR), and freedom of thought and expression (Articles 9 and 10 of the ECHR). The restriction of these rights must always be justified and supported by law.

While these measures contribute to strengthening public safety and combating organized crime, their uncontrolled use can undermine citizens' trust in state institutions. Balancing security and freedom are essential for maintaining a democratic society.

To avoid abuses and ensure the protection of human rights, it is recommended to strengthen ju-

dicial oversight mechanisms, improve institutional transparency, and further align legislation with international standards. Additionally, it is important to develop training programs for relevant authorities to ensure the fair and proportional implementation of these measures.

In conclusion, building an effective legal framework and respecting fundamental human rights are essential for maintaining the balance between the need for security and the protection of individual freedoms in Kosovo.

References

- I. ARMADA (2015), *The European Investigation Order and the lack of European standards for gathering evidence: is a fundamental rights-based refusal the solution?*, in "New Journal of European Criminal Law", vol. 6, 2015, n. 1
- J. BARBOSA E SILVA (2019), *The speciality rule in cross-border evidence gathering and in the European Investigation Order – let's clear the air*, in "Era Forum", vol. 19, 2019, n. 3
- A. CONTE (2010), *Special Investigative Techniques and Rules of Criminal Procedure*, in "Human Rights in the Prevention and Punishment of Terrorism", Springer, 2010
- C. DEVERY (2010), *Criminal Profiling and Criminal Investigation*, in "Journal of Contemporary Criminal Justice", vol. 26, 2010, n. 4
- R. FLOR, B. PANATTONI (2023), *Digital criminal investigations in Italy. The intersection between data protection and cybersecurity*, in "New Journal of European Criminal Law", vol. 14, 2023, n. 4
- E. HASANI, I. ČUKALOVIĆ (2013), *Commentary: Constitution of the Republic of Kosovo*, GIZ, 2013
- C. HEARD, D. MANSELL (2011), *The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases*, in "New Journal of European Criminal Law", vol. 2, 2011, n. 4
- B. KEENAN (2025), *From interception to integration: encryption, bulk data, and the investigatory powers regime*, in "King's Law Journal", vol 36, 2025, n. 3
- E.R. MAGUIRE, W.R. KING (2013), *Transferring criminal investigation methods from developed to developing nations*, in "Policing and Society", vol. 23, 2013, n. 3
- E. SAHITI, R. MURATI, XH. ELSHANI (2014), *Commentary on the Criminal Procedure Code*, GIZ, 2014
- N. SELVADURAI, N. KISSWANI, Y. KHALAILEH, (2016), *The proportionality principle in telecommunications interception and access law in an environment of heightened security and technological convergence*, in "Information & Communications Technology Law", vol. 25, 2016, n. 3