1/2025 luglio

Rivista di diritto dei media

ISSN 2532-9146

DIRETTORE RESPONSABILE
EDITOR-IN-CHIEF
Oreste Pollicino (Università Bocconi)

DIRETTORI
EDITORS
Giulio Enea Vigevani (Università di Milano - Bicocca)
Carlo Melzi d'Eril (Avvocato in Milano)
Marina Castellaneta (Università di Bari)
Marco Bassini (Tilburg University)

VICEDIRETTORI
VICE-EDITORS
Marco Cuniberti (Università di Milano)
Giovanni Maria Riccio (Università di Salerno)
Marco Orofino (Università di Milano)
Ernesto Apa (Avvocato in Roma)

REDAZIONE
EDITORIAL BOARD
Coordinatore: Marco Bassini (Tilburg University)
Segreteria: Martina Cazzaniga (Università di Milano-Bicocca)
Giulia Napoli (Università di Milano-Bicocca)
Redazione di Bari
Teresa Catalano, Giuseppe Gallo, Stefania Rutigliano
Redazione di Milano-Bicocca
Marco Cecili, Maria Galbusera, Giacomo Mingardo
Redazione di Milano-Bocconi
Flavia Bavetta, Claudia Massa, Matteo Monti, Giuseppe Muto, Federica Paolucci

SEDE
CONTACTS
Studio legale Melzi d'Eril Vigevani
Via San Barnaba 32 - 20122 Milano

Università Bocconi - Dipartimento di Studi Giuridici
Via Roentgen 1 - 20136 Milano
e-mail: redazione@rivistadidirittodeimedia.it

COMITATO SCIENTIFICO - STEERING COMMITTEE

Shulamit Almog *(University of Haifa),* Fabio Basile *(Università di Milano),* Mirzia Bianca *(La Sapienza – Università di Roma),* Elda Brogi *(European University Institute),* Giuseppe Busia *(Autorità Nazionale Anticorruzione),* Licia Califano *(Università di Urbino, già Garante per la protezione dei dati personali),* Angelo Marcello Cardani *(Università Bocconi, già Autorità per le garanzie nelle comunicazioni),* Marta Cartabia *(Università Bocconi, Presidente emerito della Corte costituzionale),* Massimo Ceresa-Gastaldo *(Università Bocconi),* Pasquale Costanzo *(Università di Genova),* Marilisa D'Amico *(Università di Milano),* Filippo Donati *(Università di Firenze),* Mario Esposito *(Università del Salento),* Giusella Finocchiaro *(Università di Bologna)*, Tommaso Edoardo Frosini *(Università Suor Orsola Benincasa),* Maurizio Fumo *(già Suprema Corte di Cassazione),* Alberto Maria Gambino *(Università Europea – Roma),* Michale Geist *(University of Ottawa),* Glauco Giostra *(La Sapienza – Università di Roma),* Enrico Grosso *(Università di Torino),* Uta Kohl *(University of Southampton),* Krystyna Kowalik-Bańczyk *(Tribunale dell'Unione europea),* Simone Lonati *(Università Bocconi),* Fiona Macmillan *(University of London),* Enrico Maria Mancuso *(Università Cattolica),* Vittorio Manes *(Università di Bologna),* Michela Manetti *(Università di Siena),* Christopher Marsden *(Monash University),* Manuel D. Masseno *(Instituto Politécnico de Beja),* Roberto Mastroianni *(Tribunale UE),* Luigi Montuori *(Garante per la protezione dei dati personali),* Antonio Nicita *(LUMSA, già Autorità per le garanzie nelle comunicazioni),* Monica Palmirani *(Università di Bologna)*, Miquel Pequera *(Universitat Oberta de Catalunya),* Vincenzo Pezzella *(Suprema Corte di Cassazione),* Laura Pineschi *(Università di Parma),* Giovanni Pitruzzella *(Corte costituzionale),* Francesco Pizzetti *(Università di Torino),* Andrea Pugiotto *(Università di Ferrara),* Margherita Ramajoli *(Università di Milano),* Gianpaolo Maria Ruotolo *(Università di Foggia),* Sergio Seminara *(Università di Pavia),* Salvatore Sica *(Consiglio di Presidenza della Giustizia Amministrativa),* Pietro Sirena *(Università Bocconi),* Francesco Viganò *(Corte costituzionale),* Luciano Violante *(Futuri Probabili)*, Lorenza Violini *(Università di Milano),* Roberto Zaccaria *(Università di Firenze),* Nicolò Zanon *(Università di Milano),* Vincenzo Zeno-Zencovich *(Università di Roma Tre)*

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE - ADVISORY BOARD

Maria Romana Allegri, Giulio Allevato, Benedetta Barbisan, Marco Bellezza, Daniela Bifulco, Elena Bindi, Carlo Blengino, Monica Bonini, Manfredi Bontempelli, Fernando Bruno, Daniele Butturini, Irene Calboli, Simone Calzolaio, Quirino Camerlengo, Gianluca Campus, Nicola Canzian, Marina Caporale, Andrea Cardone, Corrado Caruso, Stefano Catalano, Adolfo Ceretti, Francesco Clementi, Roberto Cornelli, Giovanna Corrias Lucente, Filippo Danovi, Monica Delsignore, Giovanni De Gregorio, Giovanna De Minico, Gabriele Della Morte, Marius Dragomir, Fernanda Faini, Fabio Ferrari, Roberto Flor, Federico Furlan, Giovanni Battista Gallus, Marco Gambaro, Gianluca Gardini, Ottavio Grandinetti, Antonino Gullo, Erik Longo, Valerio Lubello, Federico Lubian, Nicola Lupo, Paola Marsocci, Claudio Martinelli, Alberto Mattiacci, Alessandro Melchionda, Massimiliano Mezzanotte, Francesco Paolo Micozzi, Donatella Morana, Piergiuseppe Otranto, Omar Makimov Pallotta, Anna Papa, Paolo Passaglia, Irene Pellizzone, Sabrina Peron, Bilyana Petkova, Davide Petrini, Marina Pietrangelo, Federico Gustavo Pizzetti, Augusto Preta, Giorgio Resta, Federico Riboldi, Francesca Rosa, Andrej Savin, Salvatore Scuto, Monica Alessia Senor, Silvio Sonnati, Stefania Stefanelli, Giulia Tiberi, Bruno Tonoletti, Emilio Tosi, Lara Trucco, Luca Vanoni, Gianluca Varraso, Silvia Vimercati, Thomas Wischmeyer, Paolo Zicchittu

ANNO 2025 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

I contributi sono scritti e ceduti a titolo gratuito e senza oneri per gli autori. Essi sono attribuiti dagli autori con licenza Creative Commons "Attribuzione – Non commerciale 3.0" Italia (CC BY-NC 3.0 IT). Sono fatte salve, per gli aspetti non espressamente regolati da tale licenza, le garanzie previste dalla disciplina in tema di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (l. 633/1941).

Il lettore può utilizzare i contenuti della rivista con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons "Attribuzione – Non commerciale 3.0 Italia" (CC BY-NC 3.0 IT), in particolare menzionando la fonte e, laddove necessario a seconda dell'uso, conservando il logo e il formato grafico originale.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (rivista.medialaws.eu). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione comparata"), "Cronache e commenti" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache e commenti" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. A discrezione della direzione, i saggi di autori di particolare autorevolezza o richiesti dalla direzione possono essere pubblicati senza essere sottoposti alla procedura di referaggio a doppio cieco ovvero essere sottoposti a mero referaggio anonimo, previa segnalazione in nota.

Sezione monografica
"Le transizioni digitali"
a cura di Federica De Simone, Luca Di Majo, Marianna Russo

11 Le transizioni digitali
Federica De Simone, Luca Di Majo, Marianna Russo

36 Il rischio di decisioni automatizzate in materia di inammissibilità delle impugnazioni penali
Aldo Franceschini

63 L'IA nel procedimento penale: tra riconoscimento facciale e finalità investigative
Christian Pallante

84 Tra Neuromanti e pecore elettriche: Metaverso e tutela dei dati personali e della *privacy*
Alessandro Rosanò

106 Diritto alla protezione dei dati personali e dignità umana: "Profili di una pregnante correlazione"
Antonio Vertuccio

127 Dal principio del consenso informato al *Trust-Based Consent*, una possibile traiettoria evolutiva
Isabella de Vivo

162 Riflessioni sull'impatto dell'intelligenza artificiale sul rispetto del diritto internazionale umanitario e il ruolo del principio di umanità
Alice Civitella

Altri saggi

188 La regolazione dei videogiochi: tra opere audiovisive e digitali, cultura e mercato
Marina Caporale

210 The EU Legal Framework on Personal Data Flows to Third Countries and its Interplay with EU International Commitments in the Field of Trade Law
Gabriele Rugani

237 *Regulatory Sandboxes.* Spazi di sperimentazione normativa per l'intelligenza artificiale
Eugenia Perrone

Note a sentenza

271 Diritto di cronaca e limiti alla pubblicazione della corrispondenza telematica: note a margine del provvedimento del Garante per la protezione dei dati personali del 12 febbraio 2025
Pietro Villaschi

287 Un ulteriore tassello nella ricostruzione interpretativa del GDPR: la Corte di giustizia amplia oltremisura il potere discrezionale delle autorità di controllo?
Giovanna De Carne

300 Il segreto professionale del giornalista alla prova del sequestro: la Cassazione tra libertà di informazione e funzione del processo penale
Amalia Mariana Buzura

Cronache

312 The Cybersecurity and AI Nexus in the EU Digital Acquis
Irene Kamara, Marco Bassini

327 The Legal Challenges of AI Literacy Between Enforcement and Compliance
Ludovica Paseri, Massimo Durante, Ugo Pagallo

Indice

345 Navigating the Twin Transition: Digital and Ecological Transformations in the European Union
Tobia Eugenio Boaro

359 *Data protection* e immigrazione irregolare: quali tutele (in)esistenti?
Filomena Pisconti

378 I *cloud computing services*: nuove prospettive regolatorie per un'innovazione digitale sostenibile
Fabiana Magnolo

392 Minori e social media, tra norme e violazioni: i risultati di una ricerca empirica
Mario D'Avino

Focus
"The digital transition"
edited by Federica De Simone, Luca Di Majo, Marianna Russo

11 The digital transition
Federica De Simone, Luca Di Majo, Marianna Russo

36 The Risk of Automated Decisions on the Inadmissibility of Criminal Appeals
Aldo Franceschini

63 The Use of AI in Criminal Proceedings: Between Facial Recognition Technologies and Investigative Purposes
Christian Pallante

84 Between Neuromancers and Electric Sheep: The Metaverse and the Protection of Personal Data and Privacy
Alessandro Rosanò

106 Right to Data Protection and Human Dignity: "Profiles of a Meaningful Correlation"
Antonio Vertuccio

127 From the Principle of Informed Consent to Trust-Based Consent: A Possible Evolutionary Trajectory
Isabella de Vivo

162 The Digital Transition in Armed Conflicts. Some Considerations on the Impact of Artificial Intelligence for the Respect of International Humanitarian Law and the Principle of Humanity
Alice Civitella

Other essays

188 The Regulation of Video Games: Between Audiovisual and Digital Works, Culture and Market
Marina Caporale

210 The EU Legal Framework on Personal Data Flows to Third Countries and its Interplay with EU International Commitments in the Field of Trade Law
Gabriele Rugani

237 AI Regulatory Sandboxes
Eugenia Perrone

Case notes

271 The Right to Report and the Limits on the Publication of Electronic Correspondence: Reflections on the Decision of the Italian Data Protection Authority of 12 February 2025
Pietro Villaschi

287 A Step Further in the Interpretative Reconstruction of the GDPR: Does the Court of Justice of the European Union Over-Extende the Discretionary Power of Supervisory Authorities?
Giovanna De Carne

300 Journalistic Professional Secrecy: The Italian Supreme Court Between Freedom of Information and Criminal Justice
Amalia Mariana Buzura

Comments

312 The Cybersecurity and AI Nexus in the EU Digital Acquis
Irene Kamara, Marco Bassini

327 The Legal Challenges of AI Literacy Between Enforcement and Compliance
Ludovica Paseri, Massimo Durante, Ugo Pagallo

345 Navigating the Twin Transition: Digital and Ecological Transformations in the European Union
Tobia Eugenio Boaro

359 Data Protection and Illegal Immigration: What (In)Existent Protections?
Filomena Pisconti

378 Cloud Computing Services: New Regulatory Perspectives for Sustainable Digital Innovation
Fabiana Magnolo

392 Minors and Social Media: an Empirical Research
Mario D'Avino

Sono stati sottoposti a referaggio anonimo a doppio cieco i saggi di Marina Caporale, Alice Civitella, Isabella de Vivo, Aldo Franceschini, Christian Pallante, Eugenia Perrone, Alessandrò Rosanò, Gabriele Rugani, Antonio Vertuccio e le cronache di Irene Kamara-Marco Bassini e Ludovica Paseri-Massimo Durante-Ugo Pagallo. Sono stati sottoposti a referaggio anonimo i contributi di Tobia Eugenio Boaro, Amalia Mariana Buzura, Mario D'Avino, Giovanna De Carne, Federica De Simone-Luca Di Majo-Marianna Russo, Fabiana Magnolo, Filomena Pisconti, Pietro Villaschi.

Saggi

Sezione monografica

“Le transizioni digitali”

a cura di Federica De Simone, Luca Di Majo, Marianna Russo

Le transizioni digitali*

Federica De Simone, Luca Di Majo, Marianna Russo

Sommario

1. I Conferenza LA.NE.T.: obiettivi e approccio metodologico. – 2. Dalle antiche credenze alla persona *in rete*. – 2.1. Primo problema: la deterritorializzazione e l'assenza delle garanzie statuali. – 2.2. Secondo problema: la metamorfosi della persona nella dimensione digitale. – 2.3. Terzo problema: l'autodeterminazione della persona nell'ecosistema digitale. – 2.4. Quarto problema: la *platforms economy*. – 3. Diritto e tecnoscienza: dal *nomos* analogico al *nomos* digitale. – 4. L'impatto delle nuove tecnologie sul sistema penale. – 4.1. Transizione digitale e diritto penale: alcune coordinate tematiche. – 5. La transizione digitale del lavoro tra prospettive giuridiche e nuove frontiere tecnologiche. – 6. Riflessioni non conclusive.

1. I Conferenza LA.NE.T.: obiettivi e approccio metodologico

«Milioni di persone hanno visto cadere una mela, ma solo Newton si è chiesto "perché?"»[1].

Il "motore" della ricerca[2] consiste nel porsi sempre nuovi interrogativi per cercare di decifrare la realtà circostante e rinvenire risposte adeguate, al fine di apportare il proprio contributo all'ampliamento della *scientia*.

Questo è stato l'obiettivo perseguito dalla I Conferenza La.Ne.T., che, in due giornate dal ritmo serrato, ha coinvolto numerosi giovani studiosi in un ampio e variegato confronto sulle prospettive giuridiche delle transizioni digitali, offrendo spunti di riflessione e sollevando nuovi interrogativi su una questione particolarmente sfidante.

La prima sfida da affrontare è rappresentata proprio dalla scelta del tema, che, *prima facie*, sembrerebbe esulare dalle competenze prettamente giu-

* Il presente contributo trae origine dalla relazione conclusiva tenuta in occasione della I Conferenza La.Ne.T. "Transizioni Digitali: Prospettive Giuridiche e Nuove Frontiere Tecnologiche", svoltasi presso il Dipartimento di Giurisprudenza dell'Università della Campania Luigi Vanvitelli il 21 e 22 novembre 2024.

Pur essendo il frutto di una riflessione condivisa dei tre Autori, i paragrafi 1 e 5 vanno attribuiti a Marianna Russo; 2, 2.1, 2.2., 2.3 e 2.4 a Luca Di Majo; 3, 4 e 4.1. a Federica De Simone. Il paragrafo 6 a tutti.

Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista.

[1] B. Baruch, *New York Post*, 1965.

[2] Ricorrendo all'etimologia, è suggestivo rilevare come il sostantivo "ricerca" derivi dal verbo latino tardo «*circare*» – che significa letteralmente «circoscrivere, delimitare con un cerchio» – a cui si aggiunge il prefisso rafforzativo «*ri*», che indica l'intensità, l'insistenza e la perseveranza. Il ricercatore è colui che non si ferma e non si accontenta: sceglie un settore in cui convogliare curiosità e impegno e, con determinazione e costanza, cerca di contribuire all'accrescimento del sapere di tutti.

ridiche, generalmente considerate poco innovative e relegate nella *turris eburnea* di un autoreferenziale *latinorum* di manzoniana memoria[3]. L'indagine sulle nuove frontiere tecnologiche risulterebbe appannaggio esclusivo delle discipline c.d. STEM[4], che concretamente potrebbero concorrere al progresso e all'innovazione. Eppure, l'irruzione della digitalizzazione in ogni ambito della quotidianità ha un notevole impatto giuridico e sollecita un'attenta regolamentazione per evitare che, dietro la trasmissione di ogni sequenza di *bit*, si celino potenziali lesioni dei diritti fondamentali degli individui[5].

Al contempo, la riflessione giuridica sulla trasformazione digitale in atto può contribuire ad individuare e promuovere le inedite potenzialità inclusive delle nuove tecnologie.

Anche se la convinzione della imprescindibilità del diritto per garantire la convivenza civile affonda le sue radici in epoca romanistica («*Ubi homo, ibi ius*»[6]), le disposizioni normative non sono cristallizzate nel tempo, "respirano" la realtà in cui sono immerse, dialogano tra di loro ed evolvono per adattarsi concretamente al progresso e allo sviluppo della tecnica e dei costumi, in modo da rispondere ad istanze sempre nuove, in un incessante e delicato bilanciamento tra valori da tutelare. Senza un'approfondita analisi giuridica sui temi di frontiera si incorrerebbe nel rischio di impantanarsi in scelte politiche – e, di conseguenza, nell'emanazione di leggi – completamente anacronistiche e inadeguate, nonché in una giurisprudenza debole e ondivaga, sprovvista di bussole e di àncore salde[7].

La scelta di affrontare il tema delle transizioni digitali con i tipici strumenti giuridici è stata, però, arricchita dal dialogo con le discipline sociali, economiche, scientifiche. L'approccio interdisciplinare è stato, infatti, il filo conduttore della conferenza La.Ne.T.: dall'individuazione del titolo – ampio, trasversale, onnicomprensivo – all'organizzazione dei lavori in panel non suddivisi per settore scientifico-disciplinare, bensì per linee di ricerca affini. Il confronto tra discipline si è rivelato prezioso e stimolante, confermando la complementarità delle conoscenze e spronando al superamento della frammentarietà e dell'isolamento a cui l'attività di studio e ricerca rischia di condurre. D'altronde, la complessità della realtà che ci circonda esige il coinvolgimento di quanti più strumenti possibile per poterla indagare efficacemente e riuscire a cogliere la policromia del mosaico generale, pur valorizzando la specialità di ciascun tassello.

Un altro aspetto che ha caratterizzato la conferenza è stata la partecipazione di studiosi ad ogni stadio del percorso accademico, in un dialogo sereno e costruttivo tra chi sta muovendo i primi passi nell'attività di ricerca e chi ha intrapreso quella strada già da molti anni. Inoltre, la condivisione

---

[3] A. Manzoni, *I promessi sposi*, cap. 2.

[4] *Science, Technology, Engineering* e *Mathematics*.

[5] Basti pensare alla violazione del diritto alla riservatezza e alla protezione dei dati personali, alle insidiose discriminazioni algoritmiche, ai rischi psicosociali connessi all'uso smodato degli strumenti tecnologici.

[6] La nota locuzione latina è ampiamente commentata in A. Levi, *Saggi di teoria del diritto*, Bologna, 1924.

[7] Sul punto, v. M. Russo, *Per "riveder le stelle" serve la ricerca giuslavoristica? Riflessioni sul lavoro tra vaccino anti-Covid e green pass*, in *Lavoro Diritti Europa*, 2021, 4, 3.

di idee e spunti di riflessione non è rimasta racchiusa soltanto tra le mura universitarie, come attestano i molteplici interventi di professionisti e rappresentanti delle istituzioni.
Infine, è doveroso sottolineare il respiro ampio e internazionale dell'iniziativa, che ha attirato studiosi da ogni regione d'Italia e anche dall'estero, confermando la rilevanza, trasversalità e globalità del tema.
I lavori hanno consentito di individuare e mettere a sistema molteplici profili giuridici delle transizioni digitali, avviando un confronto aperto e stimolante che rappresenta un valido punto di partenza per riflessioni future.

2. Dalle antiche credenze alla persona *in rete*

Le nuove tecnologie attraggono il diritto in una serie di questioni controverse che riguardano ora la natura umana[8], ora la condizione di vulnerabilità ontologica dell'«immigrato digitale»[9], ora i profili concernenti lo sfruttamento del valore economico dei dati condivisi con la rete[10].
Dal dopoguerra (almeno) i transumanisti[11] si interrogano su quanto resisterà quella logica darwininana che ha condotto la naturale evoluzione antropologica[12]ad arretrare dinanzi alla pervasività *disruptive* della tecnologia.
Fino a quanto il «palinsesto della vita»[13] era regolato dal diritto, il *paradosso di Zenone* non rappresentava uno scenario attagliato alla regolazione del naturale dispiegarsi dell'evoluzione sociale ed economica.
Ma quando, sin dal 1950[14], il diritto iniziava a confrontarsi con scenari, per così dire, di frontiera, all'orizzonte iniziavano a profilarsi i primi interrogativi attorno «l'uomo antiquato»[15].
Certo, le infrastrutture di silicio rappresentavano mondi lontani e, anzi, gli universi paralleli neanche si profilavano come scenari realizzabili tra i più ottimisti post-umanisti, tra i quali l'idea di una "vita immersiva" regolata non tanto dal diritto, quanto dai sovrani digitali, veniva considerata una

[8] Hanno affrontato tali questioni S. Rodotà, *L'uso umano degli esseri umani*, in *Micromega*, 8, 2015, N. Wiener, *Introduzione alla cibernetica. L'uso umano degli esseri umani*, tr. it. a cura di D. Persiani, Torino, 1970.

[9] L'espressione è di L. Floridi*, The Onlife Manifesto. Being Human in a Hyperconnected Era, Berlin.Heidelberg, 2018*. Per quanto concerne l'idea della vulnerabilità ontologica in rede della persona, cfr. L. Di Majo, *La vulnerabilità degli utenti in rete*, in *BioLaw – Rivista di BioDiritto*, spec. 1, 2024.

[10] Cfr., su questi temi, L. Di Majo – G. Frezza (a cura di), *Il Metaverso: Profili strutturali, sociologici, economici e giuridici*, Milano, 2025.

[11] N. Bostrom, *Transhumanist Values*, in *Journal of Philosophical Research*, 30 (Supplement), 2015, and N. Bostrom, *A history of transhumanist thought*, in *Journal of Evolution and Technology*, 14, 2005.

[12] A. Huxley, *Brave new World,* 1931.

[13] L'espressione è di S. Jasanoff, *Introduction: Rewriting Life, Reframing Rights*, in Id. (a cura di), *Reframing Rights. Biocostitutionalism in the Genetic Age*, Mit Press, Cambridge, Mass., 2011, 1, ma anche di S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012.

[14] A. Touring, *Computing machinery and intelligence*, in Mind, 236, 1950, 433.

[15] G. Anders, *L'uomo è antiquato. Considerazioni sull'anima nell'epoca della seconda rivoluzione industriale*, trad. it. a cura di L. Dallapiccola, Torino, 2007.

condizione probabilmente irrealizzabile.
Tuttavia, la prospettiva che anima investimenti pari a porzioni significative di PIL dei Paesi più avanzati, induce a ritenere che il diritto si stia muovendo già troppo tardi rispetto ad una *Strategia dell'UE per guidare il web 4.0 e i mondi virtuali: muoversi in anticipo verso la nuova transizione tecnologica* che approccia attraverso una modalità difensiva, legata certamente all'idea di fondo del *pacchetto digitale* eurounionale teso ad una massimizzazione dei diritti, a fronte, tuttavia, di un modello tipico della piattaforme digitali fondato su una massimizzazione del solo profitto, su un'attività di continua, e a tratti anche subdola, di apprensione di dati e fidelizzazione dell'*avatar*, attraendo la persona nella rete e in nuove dinamiche relazionali.
Si tratta di questioni attinenti al ruolo dei proprietari delle molteplici *Big Tech* della *silicon valley*, in cui la persona si muove inconsapevole del livello di violenza che subisce il corpo, di come, in una tale dimensione – e ancora maggiormente negli ambienti paralleli del Metaverso[16] – l'*habeas corpus* diventa un ossimoro rispetto agli spazi di manovra acquisiti dai nuovi sovrani, proprio per il potere economico e culturale esercitato sulla persona in una dimensione che rifugge da ogni controllo eteronormante da parte dell'autorità statuale.

2.1. Primo problema: la deterritorializzazione e l'assenza delle garanzie statuali

Una delle questioni maggiormente gravide di problemi è l'assenza di un'autorità statale nella dimensione tecnologica, a fronte di sovrani digitali ontologicamente e morfologicamente antitetici rispetto alla forma storica di organizzazione del potere[17].
Il costituzionalismo ha avuto certamente il pregio di limitare il potere statuale attraverso la contrapposizione dei diritti fondamentali della persona umana nelle Costituzioni. L'uomo è forte nei confronti del potere statuale quanto più il livello di garanzia dei suoi diritti nelle Costituzioni è «lungo, largo e profondo»[18].
È la Costituzione il luogo in cui lo Stato incontra i propri limiti nell'esercizio della sovranità su una comunità stanziata entro confini certi, naturali o politici, ma ben definiti. Allo stesso tempo, lo Stato assume talvolta impegni, talaltra obblighi che non si arrestano al riconoscimento delle tradizionali libertà liberaldemocratiche, ma si estendono all'accoglimento delle pretese del popolo, dai diritti sociali ai nuovi diritti.
È questa probabilmente la caratteristica principale dell'ultima evoluzione dello Stato moderno, il quale è chiamato ad esercitare la forza "sul popolo per il popolo" che ne riconosce la funzione di arbitro, garante, anche fustigatore, se necessaria a garantire l'interesse collettivo all'ordine pubblico,

[16] Su cui, si consenta un rinvio a L. Di Majo – G. Frezza (a cura di), *Il Metaverso: aspetti strutturali, sociologici, economici e giuridici*, Milano, 2025.

[17] F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Torino, 2022.

[18] E. Mounier, *Rivoluzione personalista e comunitaria*, Milano, 2022, 90 ss.

ma sempre nel prisma dei limiti sanciti dalle Costituzioni.
Insomma, le Costituzioni governano il potere statuale che, a partire dalle democrazie liberali, diventa uno strumento di garanzia e non di persecuzione del popolo, benché la disciplina del territorio sul quale esercitare tale potere si collochi al di fuori del testo, nei trattati e nelle convenzioni internazionali. Tra l'altro, i confini territoriali non sono nella libera disponibilità degli Stati, salvo la rottura degli equilibri mondiali dovuta alle invasioni unilaterali, alle guerre.
Gli equilibri territoriali sono invero sconosciuti alla rete: la *persona upload* si colloca infatti nell'ambito di una nuova dimensione slegata da ogni «legame territoriale o di sangue»[19].
Le piattaforme digitali hanno accentuato quel fenomeno erosivo della sovranità statuale, già in atto con la globalizzazione, e dovuto dall'intreccio di relazioni tra soggetti posti in essere non solo al di là di ogni confine, ma a prescindere dai confini naturali o artificiali. Dopotutto si discute di dissoluzione dello Stato da molto prima di *internet*, perché la questione del rapporto tra politica ed economia è posta in anticipo rispetto alla rivoluzione portata dalle tecnologie artificialmente intelligenti, da un'economia che rifugge dai limiti che la politica pone, ed esorbita oltre i confini nazionali non soltanto attraverso *internet*.
La deterritorializzazione delle relazioni digitali è probabilmente un elemento sintomatico ulteriore dello «scoronamento»[20] dell'istituzione statuale, certo maggiormente accentuato nella dimensione digitale rispetto a quanto lo è stato nella globalizzazione, tanto da essere surrogata dai sovrani di silicio che hanno raccolto un'eredità niente affatto scomoda per il solo fatto di aver mutato quel paradigma tradizionale, che fondava sul legame territorio-cittadinanza-sovranità, non solo la limitazione del potere statuale, quanto le garanzie ai diritti fondamentali concretizzati nel patto tra Stato e popolo: le Costituzioni.
Quanti elementi costitutivi di tale patto ci sono nella dimensione digitale? Probabilmente pochi, almeno se volgiamo lo sguardo a quegli elementi strutturali propri di ogni entità statuale, senza i quali lo Stato non è tale: oltre ai confini, come detto, un sistema di giustizia coerente con i principi costituzionali di un giudice terzo ed imparziale, con il contraddittorio, con il diritto di difesa; la sovranità monetaria; una comunità ben definita.
Se l'*Oversight board* di *Meta* è un modo alternativo di governare i conflitti tra privati, se i *Zuck Bucks* potrebbero rappresentare il *token* alternativo alla moneta statuale, se l'esternalizzazione di servizi essenziali a grandi società (*Palantir Technologies*) diventa un modo alternativo di cessione della sovranità statale a soggetti privati che, di fatto, si inoculano all'interno dello Stato, privatizzandone le logiche, non è remota l'idea di un processo di abdicazione dello Stato a quelle funzioni tradizionali che, da un lato, gli hanno riservato un livello di ascendenza più o meno significativa sulla comunità, dall'altro, di attuare una serie di politiche strutturali che le Costituzioni gli assegnano costantemente in funzione della tutela dei diritti fondamentali.

[19] S. Rodotà, R*elazione 2002. Discorso del Presidente Stefano Rodotà, Roma, Garante per la protezione dei dati personali*, 2003, 7.

[20] S. Capograssi, *Saggio sullo Stato*, Torino, 1918.

La sovranità si dirada, il popolo si dirada, i principi costituzionali lasciano il posto alle clausole negoziali unilaterali accettate dal migrante digitale senza alcuna possibilità di contrattazione. In assenza del potere statuale, il *click* di assenso è il patto che lega la persona ad una dimensione territoriale altra, governata da un sovrano diverso dall'entità statuale che impone la propria disciplina, detta le condizioni, modifica i contenuti degli accordi e sottomette – al pari di uno Stato assoluto – l'*avatar* alle proprie regole che, se non condivise, comportano l'estromissione senza appello dalla comunità virtuale.
Il "non territorio" della rete riconosce la posizione primaria di anti sovrani che operano in una dimensione profondamente diversa da quella analogica, nella quale le individualità scompaiono, tutti i soggetti sono apparentemente uguali davanti alle regole imposte (ma accettate), certo, ma a prescindere delle peculiarità di ciascuno che le Costituzioni del dopoguerra riconoscono e tutelano in forza di quel principio di eguaglianza sostanziale di cui i sovrani digitali smentiscono alla radice: ogni corpo digitale è uguale, perché è la fonte dalla quale trarre il profitto, ed è diverso dai sui simili soltanto per la capacità di produrre profitto, a prescindere dall'indirizzo *ip*.
Quanto è vulnerabile la persona in un contesto deterritorializzato è chiaramente percepibile nella misura in cui quelle garanzie costituzionali – parte del patto tra lo Stato e il popolo – vengono meno per il venir meno del patto stesso, nel quale il sovrano incontra i suoi limiti, certo, ma è sottoposto a precisi obblighi di tutela della persona stanziata sul proprio territorio, anzi anche di chi non è legato alla cittadinanza, per il solo fatto che i diritti umani sono tali a prescindere dal legame di sangue con lo Stato.

2.2. Secondo problema: la metamorfosi della persona nella dimensione digitale

La progressiva erosione della sovranità statuale dimostra come il ruolo delle piattaforme digitali non può essere inquadrato esclusivamente scrutando il versante gnoseologico del *body swapping*, ma per il modo in cui il la persona entra in relazione con gli altri e con l'ambiente all'interno del quale si trova a vivere.
Non è soltanto la mutazione genetica della persona umana dall'analogico al virtuale che rileva, ma anche ad una modifica poliedrica dei suoi rapporti con il mondo esterno e con il fatto che si entra in relazione, in modo pressoché irreversibile, con la tecnologia.
Non si tratta di considerare le singole piattaforme come uno spazi artificialmente intelligenti solo per la ragione di prospettare un'esistenza *smart* dal punto di vista relazionale, lavorativo, economico, piuttosto di capire come l'intelligenza viene adoperata, perché tale ambiente è munito di un prisma di strumenti tecnologici che consentono un continuo e penetrante monitoraggio di immigrati digitali.
Nel momento in cui tutto questo accade, qual è il ruolo riservato dalle piattaforme digitali alla persona, rispetto a quel percorso di emancipazione dalla società degli *status* feudali, dal quale iniziava la germinazione della società dell'eguaglianza, nella quale le persone venivano considerate eguali,

facendo astrazione della dimensione naturale nella quale si trovavano?
Anzi, proprio sul terreno del ripensamento delle categorie giuridiche, uno dei dati più significativi è stato il percorso di emancipazione della persona nella prospettiva della costituzionalizzazione di essa e dei diritti fondamentali.
Nella Costituzione il termine persona ricorre non tanto nella logica del compromesso costituzionale e quale concessione a quella parte del pensiero cattolico personalista di Maritain e Mounier, piuttosto nella prospettiva di una grande operazione culturale, che trova probabilmente l'acme nella versione finale della CEDU, dove l'«individuo» è stato sostituito dalla «persona».
Questa prospettiva oggi rischia di essere surrogata dalla corsa sregolata verso un progresso tecnologico che riguarda la modifica del corpo e delle relazioni, collocate in una nuova esperienza extrasomatica. Non tanto una logica trasformativa di un corpo invaso da oggetti meccanici; non tanto una "esomatizzazione" nelle banche dati dei gameti, del sangue, delle cellule staminali; piuttosto una mutazione genetica, immaginata dai transumanisti, di un corpo proiettato nella *virtual reality* delle piattaforme digitali, in una inusuale visione di prospettive che mostrano come le nuove tecnologie siano sensibili a ciò che le stesse possono determinare per il futuro della specie umana, probabilmente destinata ad essere catalogata in singole *personalità upload*, attraverso il trasferimento ad una macchina delle informazioni incamerate nel cervello.
Un «passaggio epocale»[21], per il fatto che le nuove tecnologie tendono a conformare il corpo della persona non soltanto nella sfera più direttamente percepibile della fisicità, ma anche nei processi cerebrali e nelle modalità di comunicazione «*onlife*»[22].
L'interazione tra corpo e tecnologia è continua: l'uomo proietta sé stesso al di là dei propri confini fisici ed entra in relazione con il mondo attraverso reti, *blend machine intarfaces*, impianti neuronali, visori, che mettono in relazione cervello e piattaforme, con il primo, per così dire, "riprogrammato" sulla base di parametri posti dall'intelligenza artificiale, a lui certamente sconosciuti, così come è ignota la condizione trascendentale di qualsiasi elemento connesso ad uno spazio indefinito e ad un tempo incalcolabile.
L'intelligenza artificiale, di cui si nutrono le piattaforme digitali, contribuisce alla costruzione di un'artificialità sociale, determinando l'immaginario della persona, ne delinea il modo con cui si mostra e percepisce sé stessa attraverso un'esperienza dominata dall'alto, costruendo il nesso identità-esperienza non sulla libertà di autodeterminazione, piuttosto governandone bisogni, passioni, impulsi.
Nuda è la persona, spogliata nella sua più intima essenza perché non più collocata al centro dei diritti fondamentali, ma bersaglio di logiche concorrenziali che la utilizzano come strumento volto alla massimizzazione del profitto, sfruttando la propensione degli algoritmi a costruire l'individualità come il risultato di un legame anfibio, e probabilmente irreversibile, con una massa indotta da chi detiene il potere di condizionamento economico,

[21] E. Mazzarella, *Contro Metaverso. Salvare la presenza*, Sesto San Giovanni, 2022, 109.

[22] L. Floridi, *The Onlife Manifesto Being Human in a Hyperconnected Era*, Edinburgh, 2014.

sociale e culturale.
Nella terza dimensione antropologica si percepisce una fortissima pulsione «tecnognostica»[23] che diffonde un'idea sprezzante del corpo umano a vantaggio di un *avatar* asintomatico al dolore, alle delusioni, ai sentimenti, perdendo di vista il fattore umano come metacriterio, superato dall'oggettività digitale.
Se questo è attualmente lo stato dell'arte, possiamo chiederci se siamo animali, macchine, o se stiamo diventando «schiavi felici delle macchine»[24]; insomma, quale può essere il limite alle forme di interventi sulla mente umana, quale è il grado di autonomia che consente di attribuire e di imputare determinati atti alla libera scelta della persona.

2.3. Terzo problema: l'autodeterminazione della persona nell'ecosistema digitale

Nel momento in cui tutto questo accade, qual è il ruolo riservato dalle piattaforme digitali alla persona?
Nel momento in cui la persona umana si colloca sulle piattaforme digitali, diventa ostaggio dei *cookies* volti a tracciare i profili individuali, di gruppo, collettivi, che incasellano la persona in logiche in grado di ricavare, con un elevato livello di certezza, quali saranno i comportamenti futuri. Sono proprio gli studi della psicografia biometrica a mettere in luce come la raccolta e l'utilizzo di dati biologici funzionali a rilevare dettagli intimi su simpatie, antipatie, preferenze, interessi di un utente, possono condurre a metodi ancora più opachi e invadenti di profilare, categorizzare, manipolare gruppi vulnerabili al di là di ogni relazione umana[25].
Si tratta, a ben vedere, di un metodo standard di profilazione intrusiva, di perdita del controllo di un corpo virtuale soggetto continuamente ad attività di *marketing* digitale aggressivo e di sorveglianza capillare.
Il diritto deve prendere atto di tali cambiamenti e governare le situazioni in cui la decisione e la scelta sono ancora possibili, salvaguardando quell'autodeterminazione che i Costituenti incastonarono a chiare lettere nell'ultimo comma dell'art. 32 Cost., dove la Carta probabilmente manifesta la massima presbiopia. La legge può intervenire solo per garantire l'effettiva libertà dell'autodeterminazione, che ha nell'autonomia un fattore protettivo, autoimmunizzante verso l'esposizione agli altri. La categoria dell'autonomia declinata come autodeterminazione assume, in questo contesto, un valore fondativo ed è un punto sul quale la discussione è tutt'oggi molto aperta e sottoposta in continua fibrillazione dal mondo in silicio.
Diverse sono le questioni poste al diritto, come la fuga millenaristica legata alle trasformazioni possibili della tecnologia[26]: il *doppio standard*, una società

[23] E. Davis, *Techgnosis. Mito magia e misticismo nell'era dell'informazione*, trad. it. a cura di F. Massarenti, Roma, 2023.

[24] W. James, *We are Automata?*, Moscow, 1956.

[25] S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004.

[26] J. Offray de La Mettrie, *L'uomo macchina*, trad. it. a cura di F. Polidori, Sesto San

costruita intorno a funzioni diverse attribuite alle persone, non attraverso una decisione politica o sociale, ma attraverso il condizionamento biologico[27], la misurazione dei diritti al futuro e l'incertezza con la quale si muove il diritto sulle continue novità del progresso[28].

Quando si discute attorno alle caratteristiche di una società democratica, resta ferma l'idea per cui i diritti fondamentali delle persone devono essere rispettati in tutte le situazioni create dal mutamento tecnologico. La democrazia, insomma, non prescinde dai diritti fondamentali delle persone, anche in una quotidianità plasmata, nei suoi tratti essenziali, dall'intelligenza artificiale.

Limitare il potere, garantire i diritti e legittimare i moti di cambiamento, entro una cornice che pone al tempo stesso doveri e obblighi, costituisce, sin dall'art. 16 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789, il tratto essenziale del costituzionalismo[29], che mira a definire le condizioni di un progetto di emancipazione sociale, muovendo entro un equilibrio complessivo di poteri e diritti[30].

In questo senso, le Costituzioni moderne non sono solo «un testo giuridico o un armamentario di regole normative, ma anche l'espressione di uno stadio evolutivo culturale, un mezzo di autorappresentazione culturale del popolo, lo specchio di un patrimonio culturale e fondamento delle sue speranze»[31] e, come tali, «rappresentano gli atti del limite al e ai poteri per eccellenza, funzionali alla convivenza attraverso la preservazione di princípi storicamente e materialmente indisponibili ai poteri stessi»[32].

Il potere pubblico, cosí circoscritto e limitato, è chiamato a predisporre garanzie per il pieno e libero godimento di diritti e libertà, proteggendo l'azione umana anche dall'agire di nuovi soggetti: il costituzionalismo dei diritti, soprattutto nell'àmbito della cornice di giustizia sociale che connota le Costituzioni europee del secondo dopoguerra – e tra queste, quella italiana –, è infatti tenuto non solo a limitare il potere politico, ma estende la sua funzione anche nei confronti degli altri poteri[33].

E lo fa orientando la propria azione a precise coordinate teoriche: tra queste, in primo luogo, la teoria dell'effetto orizzontale dei diritti fondamentali nei rapporti inter privati.

I diritti fondamentali previsti dalle Carte costituzionali europee, quali garanzie normative poste alla base della convivenza politica, si presentano infatti come indissolubilmente legati agli aspetti sociali che ne stanno alla base e pertanto hanno un effetto diretto tanto nella dimensione verticale (nella contrapposizione tra autorità e libertà) quanto in quella orizzontale

---

Giovanni, 2015, H. Jonas, *Dalla fede antica all'uomo tecnologico. Saggi filosofici*, Bologna, 2001.

[27] A. Huxley, *op. ult. cit.*

[28] Si tratta di riflessioni emerse in S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Milano, 2006.

[29] M. Dogliani, *Introduzione al diritto costituzionale*, Bologna, 1994, 201.

[30] C.H. McIlwain, *Costituzionalismo antico e moderno*, Bologna, 1990, 159.

[31] P. Häberle, *Costituzione e identità culturalre*, Milano, 2006, 11.

[32] F. Paruzzo, *op. ult. cit.*

[33] L. Di Majo – F. Paruzzo, *Nuovi aspetti del potere nel Metaverso*, in M. Calamo Specchia (a cura di), *Processi politici e nuove tecnologie*, Torino, 2024.

nei rapporti tra privati[34], tanto in una situazione dominante-dominato[35], quanto nella dimensione paritaria dell'autonomia negoziale.
Dal momento che il nostro ordinamento, nel ribadire il riconoscimento e la tutela dei diritti dell'uomo, «non indica la direzione verso cui tali diritti devono essere garantiti, non è alla natura pubblica o privata del potere che bisogna guardare per tutelare il sistema democratico o la dignità del singolo, ma ai suoi effetti, al fine di evitare abusi derivanti da una combinazione di forze che si avvalgono di una libertà a discapito di altre»[36].
Dignità, solidarietà ed eguaglianza rappresentano le barriere davanti le quali il potere deve arrestarsi in nome di una Costituzione (non solo italiana) dichiaratamente fondata – come non è nemmeno il caso di precisare – sul personalismo e sulla nozione cruciale della dignità umana, strettamente legata alla pari dignità sociale di ogni persona, uguaglianza come non discriminazione nella vita di relazione e diritto all'identità personale.
Ebbene, proprio rispetto alle questioni poste da un utilizzo smodato della persona nella rete, unitamente all'assenza di ogni garanzia collocata nel patto costituzionale tra lo Stato e la comunità, non è remoto il rischio di una espropriazione di una identità plasmata dai sovrani digitali che non per forza (anzi, quasi mai) corrisponde all'effettiva identità personale.
Il punto centrale è essere giudicati fuori dal contesto: si costruisce una identità virtuale incoerente a quella umana, proiettando una costruzione dell'umano attraverso logiche e tecniche completamente diverse.
Si tratta di un tema capitale perché investe una serie di situazioni che non possiamo continuare a leggere con i criteri pretecnologici in riferimento alla persona calata nell'*on life reality*, che non esclude l'idea che tale nuova condizione materiale diventi strumento di discriminazione.
Ed allora, in uno scenario del genere, vale ancora di più quell'*alert* consegnatoci da chi ha assegnato un ruolo chiave al costituzionalismo moderno, chiamato, «nell'universo dei diritti fondamentali [ad] occuparsi più ampiamente, con la del resto ovvia avvertenza che esso è venuto, nel corso del tempo, a farsi notoriamente sempre più complesso, dopo la rivoluzione copernicana del tardo XVIII secolo, che intese svincolarli da appartenenze "comunitaristiche": innanzitutto i diritti della tradizione liberale, poi quelli detti "sociali" e "politici", infine i 'nuovi diritti'. Giacché questi ultimi sono in molti casi l'effetto delle acquisizioni scientifiche e tecnologiche, nessuna meraviglia che la discussione bioetica ne sia investita in pieno»[37] .
I valori di riferimento risiedono in quelle espressioni semantiche che «hanno nutrito nei secoli il dibattito filosofico e filologico, denotandone valori-pietre miliari, indicandone 'concetti strategici della tradizione etica e politica', o anche 'eulogici', come sono stati definiti, i quali si sono quindi tradotti, nella complessità mai troppo riducibile della loro articolazione semantica, anche in princîpi giuridici, ormai solitamente enunciati in testi

[34] R. Alexy, *Teoria dei diritti fondamentali*, Bologna, 2012, 570-571.

[35] L. Ferri, *Nozione giuridica di autonomia privata*, in *Rivista trimestrale di diritto e procedura civile*, 1947, 129.

[36] P. Rescigno*, L'abuso del diritto*, in *Rivista di diritto civile*, I, 1965, 289.

[37] S. Prisco, *La musica della vita. Quaderno di biopolitica e bioetica di un giurista*, Napoli, 2015, 71.

costituzionali»[38] .
Dignità, solidarietà, eguaglianza. C'è molto di vecchio in questi principi oppure la continuità di grandi valori, nati da una lunga elaborazione di Carte e Corti, mantengono la loro persistenza in una diversa e inusuale dimensione, con caratteristiche che sono legate alla novità della situazione, mantenendo alto il livello di preoccupazione sui profili di vulnerabilità della persona?
Il riferimento all'art. 32 Cost. è probabilmente l'elemento più significativo attorno al quale impostare la riflessione sulla re-ontologizzazione della persona: «la legge non può in nessun modo e in nessun caso violare i limiti imposti dal rispetto della persona umana». Questo è un grandissimo tema dove si innesta la questione dell'autodeterminazione. La regolazione, a prescindere dalla fonte utilizzata (meglio *soft*), può intervenire solo per garantire l'effettiva libertà dell'autodeterminazione, ma non si può sostituire alla scelta: si tratta, insomma, di riconoscere e rivalutare il limite del rispetto alla persona umana.
La categoria dell'autonomia declinata come autodeterminazione assume, in questo contesto, un valore fondativo ed è un punto sul quale la discussione sull'«apocalisse culturale»[39] è tuttora molto aperta, così come lo è stata in passato per quei passaggi di mondo dove la fase di transizione culturale ha comportato la sostituzione di vecchi valori con nuovi valori.
Se queste sono le premesse, il diritto ha il compito di costruire un contesto normativo coerente con la novità dei tempi, dove i valori e principi inviolabili del costituzionalismo, primi tra tutti, la dignità e l'eguaglianza, non possono non tracciare il perimetro di una riflessione non più procrastinabile rispetto a cosa il diritto può fare, cosa il diritto deve fare e cosa, invece, deve astenersi dal fare[40], pur governando i rischi congeniti insiti nella tecnologia[41] di una persona virtuale molto più vulnerabile della persona analogica.

2.4. Quarto problema: la *platforms economy*

Chi immaginava di funzionalizzare la rete all'umanità, ha dovuto fare presto i conti con comunità disintegrate, pregiudizi, odio e disinformazione.
Eppure, lo spirito originario della rete, prima ancora dell'era algoritmica, era improntato ad una esaltazione della libertà individuale[42], materializzatosi come uno spazio di libertà senza confini[43].
La rete è diventata ben presto una realtà plasmata originariamente dagli utenti, a loro uso e consumo, integrando uno spazio che riusciva a raccogliere anche i contributi "di nicchia", a dare riscontro a quegli interessi

[38] S. Prisco, *La dignità nel dibattito biogiuridico e biopolitico. Linee ricostruttive,* in *BioLaw Journal – Giornale di BioDiritto*, spec. 2, 2019, 61.

[39] E. De Martino, *La fine del mondo. Contributo all'analisi delle apocalissi culturali*, Torino, 2016.

[40] S. Rodotà, *La vita e le regole. Tra diritto e non diritto*, Milano, 2009.

[41] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 82.

[42] T. Detti – G. Lauricella, *Le origini di Internet*, Milano, 2013.

[43] M. Castells, *Comunicazione e potere*, Milano, 2009.

all'apparenza *naif*. Uno spazio per gli utenti e degli utenti.
Era il periodo in cui stava maturando la svolta del *web 2.0*, un nuovo modo di concepire l'*agorà* digitale come contesto di partecipazione e produzione di contenuti personali.
L'avvento del *web 2.0* ha rafforzato l'accesso alla rete, ha prodotto la nascita di una cultura partecipativa[44], ha incrementato una *peer production*, ha rappresentato la capitalizzazione di una massa collettiva scaturita dalla partecipazione degli utenti, per un verso indistinta, per altro verso connotata da individualismi, ognuno dei quali portatori di un capitale umano ben presto trasformatosi in capitale economico a favore di coloro i quali diventeranno «i sovrani dalla corona di silicio»[45] .
Su questo terreno sono stati piantati i semi del capitalismo digitale, portato alle estreme conseguenze da chi ha proposto, invero già nel XX secolo, una idea di prosumerismo[46] come annullamento tra utenti e padroni, tra consumatori e produttori che vide, nel 1980, una prima fase di un fenomeno invero preconizzato da Alvin Toffler[47], per cui non esisteva qualcosa di pari alla pura produzione senza almeno un certo consumo e, per converso, non esisteva un puro consumo senza una determinata produzione di beni.
I due processi si compenetrano: l'azienda è chiamata a svolgere attività di impresa, e diventa essa stessa attore sociale, unitamente a chi, in passato, aveva contribuito a formare il popolo della rete: l'utente-consumatore[48].
L'evoluzione di tale processo, a partire dall'evoluzione di una società probabilmente non ancora totalmente robotica, ma quantomeno "algoritmica" perché fondata sulle aspirazioni meccanizzanti dell'Intelligenza Artificiale (*web 3.0*), lasciava intravedere un'altra dimensione che sembra ispirare la logica attorno a cui si sta sviluppando attualmente il progetto Metaverso.
Non perché la figura del produttore e quella del consumatore, l'atto della produzione e quello del consumo si stiano allontanando; né può essere considerata una novità che la produzione culturale egemonica sia sempre stata strettamente connessa al potere economico, tanto da riflettersi, conseguentemente, sull'immaginario collettivo stesso.
Anzi, era prevedibile come anche la cultura partecipativa, alla lunga, finisse con l'assumere sembianze sempre più commerciali[49], tanto che la vera innovazione è consistita piuttosto nell'inserimento tra l'azione dei produttori e dei consumatori, di terzi soggetti: le piattaforme digitali.
Il riferimento alle piattaforme è soprattutto il riferimento ad un nuovo modello di *business* introdotto nell'era della c.d. *platform economy*[50], non basa-

---

[44] H. Jenkins – R. Purushotma – M. Weigel – K. Clinton – A.J. Robison, *Culture partecipative e competenze digitali. Media education per il XXI secolo*, Milano, 2010.

[45] A. Venanzoni, *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in *Rivista Italiana di Informatica e Diritto*, 1, 2020.

[46] G. Fabris, *Customer Knowledge Marketing*, in *Consumatori, Diritti e Mercato*, 1, 2008.

[47] A. Toffler, *The Third Wave*, London, 1980.

[48] Spiega bene questo modello M. Centorrino, *L'era del Metaverso. Perché non sarà un Internet 3.0*, in L. Di Majo – G. Frezza (a cura di), *Il Metaverso*, cit., 101 ss.

[49] B.E. Duffu – D.B. Nieborg – T. Poell – M. Fax, *Platforms and Cultural Production*, New Jersey, 2022.

[50] A. Gawer, *Platforms, Markets and Innovation*, Northampton, Massachusetts, 2010.

ta sui prodotti (perché la piattaforma non possiede i mezzi di produzione), piuttosto sulla fornitura di servizi e sul controllo dei mezzi di comunicazione.

Dopotutto, cos'è una piattaforma se non un nuovo modello di *business* che «crea valore»[51], governando gli scambi tra gruppi di persone e aziende?

Le piattaforme si sono guardate bene dall'inserirsi nelle dinamiche del prosumerismo, assumendo tuttavia un ruolo di mediazione che in passato era svolto da altri soggetti in modalità molto meno pervicace perché, per l'appunto, le piattaforme non distribuiscono merci, piuttosto forniscono i mezzi (servizi) di connessione e controllano il flusso del *web*.

Lo spazio della rete, inizialmente configurato libero da un gruppo di ricercatori e messo da essi stessi a disposizione della comunità mondiale, si articolò in una cultura di internet caratterizzata da una struttura a quattro strati[52]: meritocratico, hacker, comunitario/virtuale e imprenditoriale. Questi strati, insieme, hanno contribuito alla formazione di un modello di libertà largamente diffusa nel mondo di internet, senza mettere in conto lo sviluppo di un inusuale modello capitalistico e oligopolistico, incentrato sullo sfruttamento dei dati più intimi della persona.

A venti anni di distanza si ha contezza del mutamento di tali equilibri per la comparsa di nuovi soggetti di mediazione, cioè le piattaforme digitali.

Ciò che si prefigura è un cambiamento dell'ambiente in cui queste relazioni si svolgeranno: il Metaverso è un progetto che si sta sviluppando esclusivamente in una dimensione aziendale. Le espressioni utilizzate da Mattew Ball rappresentano già oggi un segnale di ciò che potrà essere un domani: si combatteranno molte guerre per avere la supremazia nel Metaverso e nel suo interno; i giganti della tecnologia si scontreranno con *startup* rivoluzionarie, usando come armi *hacker*, strumenti, requisiti tecnici, contenuti e portafogli digitali[53].

L'internet 2.0 e 3.0 – quello della grande comunità globalizzata e quello degli scambi commerciali *peer to peer* – ha fatto comprendere come l'attenzione oggi riservata agli sviluppi dell'intelligenza artificiale e alla logica algoritmica sarà estesa anche al Metaverso, con il rischio che poche aziende controlleranno mondi virtuali e *avatar* con più poteri di quelli che regolano l'economia digitale per come è conosciuta oggi. Un orizzonte diverso che guarda ad una palingenesi complessiva di un mondo ricreato in una dimensione post-umana, rideterminando il rapporto tra la fisicità e il virtuale, tra l'esperienza e il simbolismo, oltre la vita, anzi che crea l'*alpha* e l'*omega* della vita sociale/virtuale, dentro la logica organizzativa di un mondo rigido e racchiuso in un codice binario.

Siamo distanti da quegli elementi caratterizzanti la modernità, dove la visione antropocentrica dell'uomo si contrapponeva alle visioni trascendenti transumane.

Questo mondo delle nuove tecnologie conduce ad una frattura, pone un passaggio dall'antropocentrismo al datocentrismo: tutto si datifica, tutto

---

[51] M. Pedemonte, *Piattaforme digitali: la dittatura vorace che piace*, in *DigitCult*, 3, 2017, 9-14.

[52] M. Castells, *Comunicazione e potere*, Milano, 2009.

[53] M. Ball, *MetaVerso. Cosa significa, chi lo controllerà e perché sta rivoluzionando le nostre vite*, trad. it. di G. Mancuso, Milano, 2022.

è dato.
Attraverso questa esperienza di riduzione al dato, l'uomo si divide tra opportunità e riduzionismo all'uno platoniano, al principio-motore aristotelico individuato nel codice binario 0-1.
Vi è però un elemento nuovo: anche i capitalisti di internet chiedono all'utente di accedere liberamente. Lo stesso *Google* consente all'utente di utilizzare il motore di ricerca in maniera apparentemente gratuita. L'estrazione di valore avviene dall'utilizzo: più l'utente è immerso nella rete, più diventa produttore.
L'utente è diventato un "consumatore al quadrato" (più che *prosumer*). Il rapporto è biunivoco: l'utente è consumatore delle piattaforme e consumato dalle piattaforme che sfruttano i percorsi individuali per acquistare e rivendere gusti, abitudini e aspirazioni al mercato digitale.
La politica e, conseguentemente, il diritto non possono rimanere indifferenti davanti ad uno scenario impervio, dove i diritti fondamentali restano ingabbiati in logiche profittevoli ben lontane dall'idea di un *world wide web* come bene comune, invece forgiati da una logica capitalistica di estrazione di valori dietro l'apparente gratuità di internet.

3. Diritto e tecnoscienza: dal *nomos* analogico al *nomos* digitale

L'inarrestabilità del progresso tecnologico e la velocità con cui si susseguono i mutamenti che ne conseguono non hanno, con ogni probabilità, precedenti analoghi nella storia dell'umanità. Le innovazioni tecnologiche hanno investito ogni aspetto della vita sociale, dando luogo a trasformazioni talmente rapide da non raggiungere una unanimità di vedute rispetto alla determinazione della fase che il genere umano sta attraversando.
Terminata la terza rivoluzione industriale (prima rivoluzione digitale), ci troviamo nel pieno della quarta[54] o si intravedono già gli albori della quinta rivoluzione industriale[55]? E la seconda rivoluzione digitale in quale delle due si inserisce?
La questione, i cui termini non sono affrontabili in questa sede, non è di poco conto e non rappresenta un mero esercizio di stile. La comprensione dei diversi momenti evolutivi, infatti, costituisce il fondamento da cui il diritto trae il suo compito interpretativo della realtà sociale, per adeguare efficacemente la regolamentazione normativa ai nuovi scenari.

[54] L. Floridi, *Pensare l'infosfera. La filosofia come design concettuale*, Milano 2020, secondo cui la quarta rivoluzione (detta anche Industria 4.0) coinciderebbe con l'affermazione dell'infosfera, a cui si deve la fusione tra il mondo fisico, digitale e biologico. L'introduzione di tecnologie come l'IoT, l'AI, la robotica avanzata, la stampa 3D e il *cloud computing*, starebbe apportando significativi mutamenti nella società. La Quinta Rivoluzione Industriale, invece, pur prendendo le mosse dalla Quarta, pone maggiore enfasi sulla collaborazione tra uomo e macchina, sulla personalizzazione di massa, sulla sostenibilità e sulla capacità di adattamento.

[55] T. Groppi, *Alle frontiere dello stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in *Consulta online*, 2020, 3, 675 ss. La quinta rivoluzione industriale costituirebbe una evoluzione della quarta, incentrandosi maggiormente sulla relazione tra uomo e macchina, sulla personalizzazione di massa, sulla sostenibilità e sulla capacità di adattamento.

Questa la ragione principale di un interesse giuridico per simili temi, da cui prende le mosse l'attività di ricerca del gruppo *Law and New Technologies* (La.Ne.T.) del Dipartimento di Giurisprudenza dell'Università della Campania Luigi Vanvitelli, con la finalità di indagare le sfide dommatiche, fornire spunti di riflessione in merito alle esigenze di adeguamento normativo e offrire prospettive giuridiche evolute ed evolutive, con un approccio che predilige l'interdisciplinarietà.

Il giurista è naturalmente portato a risolvere le innovazioni classificando e regolamentando; tuttavia, si avverte anche nel mondo del diritto l'inadeguatezza degli strumenti ordinari e l'inopportunità di una visione ristretta alle categorie tradizionali, nella consapevolezza che da una corretta regolamentazione di tali strumenti dipende la tenuta stessa dell'ordinamento. Cionondimeno, l'evoluzione del quadro giuridico nell'ottica dell'accoglienza delle innovazioni tecnologiche non può tramutarsi – ad avviso di chi scrive – in un ridimensionamento del ruolo dei principi fondamentali dell'ordinamento. Questi, infatti, si rivelano ancor più irrinunciabili, dando luogo all'*ubi consistam* della tutela dei diritti fondamentali in particolare e della coerenza del sistema in generale.

In primis, il principio di legalità, che svolgendo un ruolo di primazia in tema di tutela dei diritti fondamentali, potrebbe trarre una rinnovata vitalità proprio dallo sviluppo delle nuove tecnologie, per le quali la certezza del diritto e la determinatezza della regolamentazione assurgono a indispensabile canone interpretativo[56]. La disciplina normativa, dunque, fornisce un limite necessario per garantire la tutela dei diritti fondamentali e per far sì che i nuovi strumenti assicurino il rispetto della persona umana. Tuttavia, al potere legislativo è richiesto anche uno sforzo in termini di velocità di adeguamento e, al contempo, di superamento sia delle logiche emergenziali sia della frammentarietà della tecnica, dovendo individuare una regolamentazione ponderata, che sia capace di offrire risposte efficaci alle svariate questioni che si pongono con l'implementazione delle nuove tecnologie.

Al principio della separazione dei poteri, poi, si riconosce anche il compito di assicurare che le scelte normative non siano condizionate in larga misura dai poteri economici e che tendano, piuttosto, a bilanciare gli interessi pubblici e della collettività rispetto a quelli dei privati.

Invero, queste brevi riflessioni riguardano solo alcuni dei principi fondamentali, ma lo sviluppo della robotica, l'evoluzione dei sistemi di intelligenza artificiale, l'adozione di strumenti come la *blockchain* e le monete virtuali, li coinvolgono tutti e proprio questa direttrice di indagine, unitamente all'esigenza di non imbrigliare eccessivamente l'innovazione, costituisce il più ampio punto di ricerca del gruppo La.Ne.T., a cui seguono

[56] Il contributo dei sistemi di intelligenza artificiale al rispetto del principio di legalità potrebbe consistere nella loro grande capacità di analisi computazionale che, permettendo di esaminare una mole considerevole di testi e dati, renderebbe le norme più coerenti rispetto all'impianto legislativo nel suo complesso (magari evidenziando lacune o contraddizioni con altre disposizioni), più trasparenti e anche più efficaci, potendo fornire un'analisi dell'impatto nella realtà concreta in cui sono chiamate ad operare. Cfr. M. Zalnieriute – L. Burton (*et al.*), *From Rule of Law to Statute Drafting: Legal Issues for Algorithms in Government Decision-Making*, in *Cambridge Handbook on the Law of Algorithms*, Cambridge University Press, 2019.

tematiche specifiche. In particolare, costituiscono oggetto di indagine i casi di *E-governance* in relazione alla partecipazione digitale, i profili della responsabilità per i casi di violazione della regolamentazione e conseguenti lesioni dei diritti coinvolti, le fattispecie implicate nei fenomeni del *cybercrime* e della *cybersecurity*.

4. L'impatto delle nuove tecnologie sul sistema penale

Tra tutti gli ambiti del diritto, quello penale rappresenta probabilmente il settore in cui l'impatto delle nuove tecnologie si manifesta in modo ambivalente.

Sotto un primo profilo, emergono evidenti criticità in merito al rispetto dei principi fondamentali, nonché all'effettività delle garanzie su cui si misura la coerenza dell'ordinamento, a cominciare dal principio di legalità, per il quale si colgono delle tensioni intrinseche. Le scelte di politica criminale e gli interventi normativi, infatti, non riescono a seguire in maniera diacronica lo sviluppo tecnologico, costringendo il legislatore penale a fare ricorso a tecniche di normazione spesso di tipo emergenziale, che non riescono a soddisfare le esigenze di tutela dei beni giuridici e di regolamentazione dei nuovi fenomeni. La rapida obsolescenza tecnologica spinge il legislatore ad adottare o norme carenti sotto il profilo della tassatività e determinatezza, o che sono già superate al momento della loro entrata in vigore, con il rischio di vuoti di tutela, arbitrarietà interpretativa o eccesso di incriminazione. Non solo, si impone una riflessione anche sul principio di responsabilità penale e sul principio di colpevolezza per i fatti commessi ad esempio dall'intelligenza artificiale, per i quali sarebbe opportuno prendere in considerazione l'idea di introdurre una forma di responsabilità della persona elettronica, come già tentato in alcuni Paesi. L'Estonia, ad esempio, discute da tempo la proposta di introdurre una forma di responsabilità giuridica limitata per i sistemi di intelligenza artificiale più avanzati, inseriti in registri per "agenti autonomi" e dotati anche di una limitata capacità giuridica, pur sufficiente a stipulare *smart contracts*[57]. Certo il discorso è ben più articolato e coinvolge categorie dommatiche fondamentali, come la capacità di intendere e di volere, l'imputabilità e l'elemento soggettivo del reato e forse proprio questa complessità ha fatto sì che il dibattito subisca una battuta d'arresto, anche in considerazione delle determinazioni raggiunte a livello sovranazionale, la cui recentissima normativa esclude una simile possibilità[58]. Finanche il principio di proporzionalità della risposta

[57] Cfr. L.A. Kuklińska, *Establishing liability for the actions of Artificial Intelligence. Recommendation for the European Commission*, in *InstytutNowejEuropy*, 6 September 2021; A. Grigoryan, *Estonia: il governo pubblica un rapport sull'intelligenza artificiale*.

[58] Il 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) n. 2018/858, (UE) n. 2018/1139 e n. (UE) 2019/2144 e le direttive n. 2014/90/UE, (UE) n. 2016/797 e n. (UE) 2020/1828 (regolamento sull'intelligenza artificiale), meglio noto come AI ACT, esclude espressamente questa possibilità, affermando che le responsabilità giuridiche

punitiva rispetto a fatti nuovi e anche molto diversi tra loro solleva degli interrogativi di natura sostanziale. L'eterogeneità delle ipotesi criminose nell'ecosistema digitale, la necessità di recepire le istanze sovranazionali e il carattere spesso transnazionale delle fattispecie sono tutti fattori che possono determinare delle difficoltà nel bilanciamento delle sanzioni e, dunque, della loro adeguatezza ed efficacia. Non è da sottovalutare, poi, il rischio che una violazione del principio di proporzionalità sia la conseguenza di un effetto distorsivo dovuto a un'attenzione normativa selettiva sul tema. Basti pensare al caso dell'estorsione tradizionale (art. 629 c.p.) e della cosiddetta *cyberestorsione* (art. 629, co. 3 c.p.) di recente introduzione, ipotesi per le quali facilmente si può determinare una disparità di trattamento sanzionatorio a fronte di condotte molto simili[59].

L'evidenza del rischio di un conflitto tra l'impiego dei nuovi strumenti e i principi fondamentali sembra possa trarsi ulteriormente anche dal ricorso agli strumenti di giustizia predittiva. La prevenzione, infatti, è un altro tema spinoso che solleva non poche perplessità *ex se*, ponendo in discussione i caratteri propri del diritto penale fattuale e della sua funzione repressiva. La complessità della questione diventa particolarmente evidente dinnanzi a strumenti tecnologici avanzati, impiegati per prevenire i reati e anticipare la tutela penale, come accade nel caso degli algoritmi predittivi o dei sistemi di riconoscimento facciale, che quand'anche non si atteggino a vere e proprie misure di prevenzione, comportano comunque il rischio di una sorveglianza di massa[60].

Fin qui i nodi più critici. Sotto un secondo profilo, invece, occorre osservare la centralità del ruolo regolatorio del diritto penale: la tipizzazione di nuove fattispecie concorre non solo a contrastare l'emersione dei nuovi fenomeni criminosi, ma anche a orientare la collettività e a definire i limiti entro cui è possibile utilizzare i nuovi strumenti. L'importanza di tale funzione nell'ambito delle tematiche proprie del *cyberspazio* è emersa gradualmente, considerando che un primo intervento organico risale al 1993, quando la legge n. 547 ha sanzionato l'uso illecito dei sistemi informatici, introducendo nuove fattispecie e modificando quelle esistenti[61]. Il quadro

devono ricadere su persone fisiche o giuridiche (aziende, sviluppatori, fornitori di servizi), poiché non si ritiene sostenibile il rischio di deresponsabilizzazione che una simile scelta potrebbe comportare. Si vedano, ad esempio, gli articoli 14, 16 e 26.

[59] La nuova ipotesi è stata introdotta dalla già citata legge n. 90/2024 (art. 16, lett. *m)*, n. 2). Si può concretizzare la disposizione facendo l'esempio in cui l'estorsione coinvolga l'accesso non autorizzato al database di un ente pubblico, minacciando la divulgazione di dati sensibili. Sebbene la pena massima in presenza di circostanze aggravanti sia allineata a ventidue anni di reclusione sia nell'estorsione tradizionale sia in quella cibernetica, quest'ultima sembra connotata da maggiore gravità in virtù delle fattispecie presupposte per le quali opera e ciò potrebbe dare luogo a una maggiore probabilità di applicazione della pena massima rispetto a quanto avverrebbe per la casistica classica. Pur a voler giustificare un simile risultato, facendo leva sulla maggiore natura lesiva della minaccia cibernetica, resta la considerazione di fondo secondo cui il diritto penale italiano deve necessariamente guardare al fatto.

[60] Sia consentito rinviare a F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Arch pen. web*, 2, 2023, 1-36.

[61] Legge n. 547/1993 contenente *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, finalizzata a punire le aggressioni alla riservatezza, all'integrità e alla disponibilità dei dati e delle comunicazioni informatiche,

normativo delineato in tema di *cybersicurezza* nazionale e criminalità informatica è stato successivamente modificato; in particolare, con l'intervento della legge n. 48 del 2008[62] il legislatore ha provveduto ad adeguare la normativa nazionale a quanto previsto dalla Convenzione di Budapest del 2001 e, recentemente, con la legge n. 90/2024 ha introdotto nuove ipotesi di reato[63], inasprito le sanzioni di quelle già previste e rafforzato il ruolo della Agenzia per la Cybersicurezza Nazionale.

4.1. Transizione digitale e diritto penale: alcune coordinate tematiche

Da queste premesse hanno preso le mosse gli interventi afferenti all'area penalistica durante la I Conferenza La.Ne.T. e dalle quale emerge come le nuove tecnologie rappresentino talvolta un Giano bifronte, potendo assumere la duplice veste di strumenti deputati ora alla commissione di reati, ora alla loro prevenzione e repressione.
È quanto accade, ad esempio, con le questioni connesse alle condotte di *cyberbullismo*. Da un lato, infatti, il *web* e le applicazioni digitali costituiscono un ambiente favorevole alla proliferazione dei casi di bullismo, che seppure non godano ancora di un'autonoma fattispecie di reato[64], rappresentano purtuttavia un rischio rilevante soprattutto per la tutela dei minori. Le condotte di molestie, diffamazioni e minacce sono amplificate dal contesto tecnologico e soprattutto agevolate dall'anonimato, senza considerare la velocità di diffusione delle stesse, che contribuisce ad aggravare la lesione del bene tutelato. Dall'altro, invece, *software* di monitoraggio, filtri, piattaforme di segnalazione e strumenti di indagine forense digitali sono regolarmente impiegati per sensibilizzare con finalità preventiva la collettività sul tema, ma anche come strumento di supporto alle vittime, oltre che di

nonché le condotte di falso e di frode commesse attraverso l'uso di tecnologie informatiche

[62] Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.

[63] La legge n. 90/2024 contenente *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*,ha introdotto l'ipotesi dell'estorsione commessa mediante la commissione di un reato informatico e, al contempo, una circostanza attenuante per i casi di lieve entità di estorsione informatica e di danneggiamento di sistemi informatici. Il provvedimento interviene anche sulla responsabilità amministrativa degli enti per i reati informatici, modificando l'articolo 24-*bis*, d. lgs. n. 231/2001.

[64] Il legislatore ha provveduto a introdurre una prima definizione di *cyberbullismo* già nel 2017 con la legge n. 71/2017 recante *Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo*, poi aggiornata con la legge n. 70/2024, recante *Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e cyberbullismo*, con l'intento di ampliare l'intervento legislativo. Cionondimeno, ancora non si dispone di una fattispecie autonoma, dovendosi piuttosto fare riferimento di volta in volta ai diversi reati previsti nel codice penale a seconda del contesto di riferimento. È pur vero, però, che si tratta di un caso in cui dalla disciplina di un fenomeno cibernetico si addiviene alla regolamentazione di un fenomeno sociale non digitale, laddove il recente intervento normativo coglie l'occasione per estendere la tutela anche alle ipotesi di bullismo, senza considerare che misure rieducative anche incisive possono essere disposte nei confronti del minore di anni diciotto che sia stato autore di tali atti.

identificazione degli autori.
Ancora, in tema di *cybersicurezza*, l'intelligenza artificiale è spesso impiegata per prevenire i crimini informatici, rilevando, identificando e segnalando i casi che possono mettere a rischio la sicurezza dei sistemi digitali, ma – al tempo stesso – può essere utilizzata per manipolare i dati, con particolari rischi per quelli sensibili.
Analoga duplice funzione si rinviene anche nell'ambito della cosiddetta criminalità economico-finanziaria, in cui la dematerializzazione degli affari, la velocità degli scambi e anche l'assenza di intermediari, favoriscono la commissione di reati in generale e la criminalità organizzata nello specifico. Al contempo, i nuovi strumenti sono indispensabili per la repressione di simili ipotesi, rivelandosi particolarmente utili soprattutto per il tracciamento dei beni di provenienza illecita, a cui potrebbero far seguito i provvedimenti di congelamento sequestro e confisca nelle diverse forme previste[65]. La tecnologia *blockchain*, l'analisi dei *big data* e la *digital forensics*, infatti, ben si prestano a essere impiegati nelle attività di recupero di beni, ma ciò richiede l'adeguamento della disciplina normativa alle potenzialità delle tecnologie avanzate, affinché ne sia regolamentato l'uso e – aspetto non di poco conto – garantita la validità probatoria. La recente direttiva (UE) 2024/1260, pur costituendo un apprezzabile tentativo di armonizzazione delle discipline adottate dai singoli paesi in tema di recupero e confisca dei beni illeciti, nonché di rafforzamento della cooperazione transfrontaliera, non dedica un'ampia trattazione ai nuovi strumenti. L'unico riferimento al tema si rinviene, infatti, in occasione dell'individuazione dei beni che possono essere oggetto di recupero, tra i quali sono state inserite anche le criptovalute. Un'occasione persa, dunque, che non solo contribuisce a rendere superato il provvedimento appena adottato a fronte di una criminalità sempre più avvezza all'utilizzo delle nuove risorse, ma che soprattutto fallisce nell'intento stesso di armonizzazione, lasciando ai singoli Stati la scelta se adottare o meno tali strumenti[66].
Nonostante l'AI Act adottato nel 2024 sia tra i primi strumenti regolatori dei sistemi di intelligenza artificiale[67], la stessa Unione europea mostra una

---

[65] Sull'istituto della confisca molto si è scritto, trattandosi di uno strumento *proteiforme*, particolarmente discusso in riferimento soprattutto ad alcune sue forme. *Ex multis*, si veda A.M. Maugeri, *Voce* c*onfische: definizioni, questioni problematiche e prospettive*, in C. Piergallini – G. Mannozzi (*et al.*), *Studi in onore di Carlo Enrico Paliero. Politica criminale e teoria della pena*, Milano 2022, 425 ss.; Id., *La direttiva 2014/42/UE come strumento di armonizzazione della disciplina della confisca nel diritto comparato*, in *La legislazione penale*, 15.07.2021, pp. 1 ss.; Id*., La nozione di profitto confiscabile e la natura della confisca: due inestricabili e sempre irrisolte questioni*, in *La legislazione penale*, 17.1.2023, 1 ss.; A. Costantini, *La confisca nel diritto della prevenzione*, Torino, 2022; A. Esposito, *La confisca urbanistica. Una storia a più voci*, Torino, 2020; E. Nicosia, *La confisca*, *le confische*, Torino, 2012.

[66] Il tema della formazione degli operatori e delle forze armate rispetto all'impiego delle nuove tecnologie è stato ampiamente trattato dal CEPOL, l'agenzia dell'Unione europea che promuove, attraverso la formazione, la cooperazione internazionale nell'attività di contrasto. Sul punto si veda il report *Operational training needsanalysis – criminalfinances, money laundering and asset recovery*, che sembra evidenziare proprio la lacuna della direttiva UE sopra citata.

[67] Si tratta 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) n. 2018/858,

certa cautela nel regolamentare l'uso dei nuovi sistemi. A ulteriore riprova di ciò si consideri anche la direttiva (UE) 2019/1937 Parlamento Europeo e del Consiglio[68] che, in tema di *whistleblowing*, annovera genericamente tra gli strumenti di segnalazione le piattaforme *online*, non facendo alcun esplicito riferimento ai più avanzati sistemi automatizzati di *whistlebot*[69].

Non va meglio a livello nazionale. Sovente il legislatore italiano tende a risolvere le criticità connesse alla diffusione dei nuovi fenomeni (siano essi sociali, tecnologici, economici o altro) con scelte di politica criminale che hanno come risultato finale un eccesso di criminalizzazione. È quanto potrebbe accadere anche nell'ipotesi in cui il disegno di legge presentato per recepire e armonizzare l'AI ACT dovesse essere approvato in via definitiva[70]. Il provvedimento contiene una esplicita disciplina penale per i casi in cui il reato commesso sia stato perpetrato impiegando a diverso titolo sistemi di intelligenza artificiale; un ulteriore aggravamento di pena è previsto per la commissione di reati contro i diritti politici dei cittadini. Infine, una nuova fattispecie di reato viene introdotta per le ipotesi di condivisione di *deepfake* che cagionino un danno ingiusto, quando manca il consenso della persona ritratta.

A una prima lettura emergono già alcuni rilievi critici in relazione al rispetto dei principi fondamentali. Il riferimento ai sistemi di intelligenza artificiale in termini di "insidiosità" pone una prima questione di vaghezza e conseguente indeterminatezza, oltre che di colpevolezza: cosa rende insidioso un simile strumento ai fini dell'operatività dell'aggravante? Il carattere insidioso è ontologicamente ascrivibile al sistema, ovvero è il suo uso a renderlo tale? Neanche vanno tralasciate, poi, le difficoltà probatorie relative all'aver ostacolato la pubblica o la privata difesa o, anche, all'aver aggravato le conseguenze del reato.

(UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive n. 2014/90/UE, (UE) n. 2016/797 e (UE) n. 2020/1828 (regolamento sull'intelligenza artificiale), meglio noto come AI Act o legge europea sull'intelligenza artificiale, entrata in vigore il 1 agosto 2024. Da più parti il provvedimento è ritenuto il primo del suo genere, ma tale convinzione non tiene in debito conto il Regolamento cinese del 13 luglio 2023. L'Ufficio Nazionale per l'Informazione su Internet e altri dipartimenti hanno emanato congiuntamente le *Misure provvisorie per l'amministrazione dei servizi di intelligenza artificiale generativa ("Misure")*, entrate in vigore il 15 agosto 2023, e che propongono requisiti dettagliati di conformità in termini di contenuti, dati e algoritmi. Si tratta in particolare del primo documento normativo per i contenuti generati dall'intelligenza artificiale ("AIGC") in Cina.

[68] Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 *riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*.

[69] È altresì vero, però, che questi ultimi, pur garantendo maggiore efficienza nei controlli aziendali interni e assicurando l'anonimato, non sono scevri da rischi di errori e *bias*, che ben possono causare danni reputazionali anche importanti e accuse ingiuste.

[70] Risale al 20 marzo 2025 l'approvazione al Senato del disegno di legge in materia di intelligenza artificiale (DDL AI), finalizzato ad armonizzare la normativa italiana alle disposizioni del regolamento (UE) 2024/1689 (AI ACT). Per le modifiche in materia penale si veda l'art. 25 e, in particolare, il co. 1 che così recita: «1. Al codice penale sono apportate le seguenti modificazioni: a) all'articolo 61, primo comma, dopo il numero 11-novies) è aggiunto il seguente: 11-decies) l'avere commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato».

Le nuove tecnologie impongono una riflessione anche sul non meno rilevante tema della cosiddetta "tecnologia giudiziaria", in riferimento ai casi in cui il ricorso ai nuovi strumenti porti sempre più nella direzione dell'automazione dei processi decisionali. Ciò comporta il prevalere di un formalismo sempre più imperante (come sembra evidenziarsi nei processi telematici), ma con il paradossale risultato di una semplificazione delle procedure proprio per favorire l'automazione stessa, dando luogo così a un corto circuito del sistema giudiziario.

Da questo quadro appena accennato, emerge una realtà dinamica e complessa, in cui le innovazioni tecnologico-digitali incidono sugli equilibri classici delle funzioni proprie del diritto penale, alterando la relazione tra prevenzione, repressione e garanzie e generando aporie di sistema nel bilanciamento tra le esigenze di efficienza e le necessità di tutela. Si tratta di scenari inediti che impongono una riflessione profonda non più rinviabile sul ruolo e sugli strumenti del diritto penale, a cui far fronte con un approccio normativo che, pur tenendo conto della rapidità dei mutamenti, non deroghi ai principi fondamentali dell'ordinamento, riconoscendone la funzione di baluardo a tutela dei diritti fondamentali.

In una società sempre più tecnologicamente avanzata, infatti, diviene concreto il rischio di una progressiva compromissione di tali diritti e ciò rende necessaria una capacità di adattamento costante delle coordinate giuridiche. Cionondimeno, questo non deve tradursi in una tendenza alla regolamentazione eccessiva o mal fatta, pena il rischio di svuotare di significato la norma penale, addivenendo a un inefficace diritto penale simbolico.

5. La transizione digitale del lavoro tra prospettive giuridiche e nuove frontiere tecnologiche

All'interno della variegata cornice delle transizioni digitali si collocano i quattro panel dedicati alla riflessione sul delicato e controverso binomio "lavoro e nuove tecnologie".

Com'è noto, l'innovazione tecnologica costituisce una preziosa occasione per introdurre «nuovi prodotti e nuovi processi, che consentono di ridurre i costi e di accrescere la produttività»[71], nonché di creare forme inedite di organizzazione lavorativa e di opportunità occupazionali[72], anche agevolando la conciliazione tra vita professionale e personale. D'altro canto, però, la digitalizzazione del lavoro è foriera di preoccupazioni relative ai rischi psicosociali, al godimento dei diritti da parte dei lavoratori[73]

[71] P. Sylos Labini, *Nuove tecnologie e disoccupazione*, Bari, 1989, 44.

[72] V. Van Roy – D. Vértesy – M. Vivarelli, *Technology and employment: Mass unemployment or job creation? Empirical evidence from European patenting firms*, in *Research Policy*, 47, 2018, 1762.

[73] Sul rapporto tra tecnologia e relazioni sindacali, v. M. Marazza, *Social, relazioni industriali e (nuovi percorsi di) formazione della volontà collettiva*, in *Riv. it. dir. lav.*, 1, 57, 2019; V. Aniballi, *Diritti e libertà sindacali nell'ecosistema digitale*, Napoli, 2022; T. Treu, *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *Federalismi*, 9, 190, 2022; M. Russo, *L'attività sindacale nel prisma della transizione tecnologica: il punto sulla giurisprudenza*, in *Arg. Dir. Lav.*, 5, 2023, 1087.Sull'impatto delle nuove tecnologie sul sistema di sicurezza sociale, v. P. Sandulli,

e alla incombente "spada di Damocle" della disoccupazione tecnologica[74], in quanto «provoca un'incessante redistribuzione delle risorse, umane e materiali, una redistribuzione che coinvolge non solo le nuove leve di lavoratori, ma anche quelle già attive»[75], comportando l'espansione di certe attività, ma anche il declino di altre.

L'intreccio tra innovazione tecnologica e lavoro apre quotidianamente scenari inesplorati, che reclamano soluzioni giuridiche adeguate, perché «le tecnologie sfidano i vecchi diritti e ne esigono impetuosamente di nuovi»[76]. La trasformazione è ormai in atto da decenni[77] e il suo ritmo aumenta in maniera esponenziale, investendo sia le strategie aziendali che la stessa regolamentazione del lavoro[78], attraverso l'introduzione di nuovi strumenti[79] e l'implementazione delle disposizioni normative in materia[80].

Il lavoro stesso è in transizione, perché sta attraversando un cambiamento[81] innescato dal dilagante ricorso alla digitalizzazione. Considerato che l'attuale connessione ad Internet si avvale esclusivamente di segnali di tipo digitale[82], tutte le prestazioni lavorative svolte mediante dispositivi elettronici connessi alla rete possono essere pacificamente considerate "digitali", a prescindere dalla qualificazione giuridica del rapporto – subordinato o autonomo – e dalla natura pubblica o privata del datore di lavoro[83].

Digitalizzazione e sicurezza sociale, in *Federalismi*, 9, 2022, 180.

74 V. M. R. Ford, *Rise of the robots: technology and the threat of a jobless future*, New York, 2015; J. Kaplan, *Humans Need not Apply: A Guide to Wealth and Work in the Age of Artificial Intelligence*, New Haven, 2015; A. McAfee – E. Brynjolfsson, *The Second Machine Age: Work, Progress, and Prosperity in a time of brilliant technologies*, New York, 2016; OECD, *Automation and independent work in a digital economy*, in *www.oecd.org*, 2016; R. Campa, *Technological unemployment. A Brief history of an idea*, in *Orbis Idearum*, 6, 2, 2018, 57; A. Perulli – V. Speziale, *Dieci tesi sul diritto del lavoro*,, Bologna, 2022, p. 143; D. Susskind, *Un mondo senza lavoro*, Milano, 2022. Di recente, v. World Economic Forum, *Future of Jobs Report 2025*, Ginevra, 2025, 10, sulle previsioni dell'impatto della transizione digitale nel mercato del lavoro nel prossimo quinquennio.

75 P. Sylos Labini, *Nuove tecnologie*, cit., VII.

76 S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 15.

77 Cfr. G. Vardaro, *Tecnica, tecnologia e ideologia della tecnica nel diritto del lavoro*, in *Politica del diritto* 1,, 1986, 75; S. Simitis, *Juridification of labor relations*, in G. Teubner (a cura di), *Juridification of social spheres: a comparative analysis in the areas of labor, corporate, antitrust and social welfare law*, Firenze, 1987, 150.

78 V. M. Weiss, *Digitalizzazione: sfide e prospettive per il diritto del lavoro*, in *Dir. rel. ind.*, 3, 2016, 651; P. Ichino, *Le conseguenze dell'innovazione tecnologica sul diritto del lavoro*, in *Riv. it. dir. lav.*, 4, 2017, 525.

79 Basti pensare, per quanto concerne l'Italia, al lavoro agile (art. 18 ss. della l. 22 maggio 2017, n. 81) e al lavoro tramite piattaforme digitali (art. 47 *bis* ss. d. lgs. n. 81/2015, così come modificato dal d.l. n. 101/2019, convertito dalla legge n. 128/2019).

80 V., ad es., il regolamento (UE) 2024/1689 sull'intelligenza artificiale.

81 Transizione deriva dal latino «*trans - ire*», che significa andare attraverso, passare.

82 Trasmessi in forma binaria e non in forma continua, come avviene nella tecnologia analogica.

83 Sul punto, v. la Risoluzione del Parlamento europeo del 21 gennaio 2021 in materia di disconnessione: secondo il considerando 11 della proposta di direttiva UE allegata alla risoluzione, «il diritto alla disconnessione dovrebbe applicarsi a tutti i lavoratori e a tutti i settori, sia pubblici che privati».

Innumerevoli e variegate sono le applicazioni della digitalizzazione all'organizzazione ed esecuzione della prestazione di lavoro: dal tradizionale telelavoro al più recente e dinamico lavoro agile o *smart working*, dal lavoro ibrido[84] al lavoro mediante piattaforme digitali (i c.d. *riders*)[85], dall'attività e-sportiva esercitata in via professionale dal *pro-player*[86] alle prestazioni di lavoro svolte mediante metaverso[87]… E il ricorso alla digitalizzazione del lavoro non investe soltanto le attività intellettuali, come dimostra il diffuso utilizzo di dispositivi elettronici indossabili (c.d. *wearable technologies*) per lo svolgimento di mansioni manuali e l'impiego di tecnologia 5G per pilotare a distanza veicoli automatizzati nel settore logistico, manifatturiero ed edilizio.

D'altronde, la corsa alla digitalizzazione del lavoro è inarrestabile e, al tempo stesso, irresistibile dal punto di vista imprenditoriale, in quanto strumenti sempre più sofisticati possono rendere la prestazione lavorativa maggiormente efficace, rapida e conveniente. L'altro lato della medaglia, però, è rappresentato dai numerosi rischi psicosociali[88] già segnalati nel 2017 da Eurofound e OIL[89], dal mancato riconoscimento di un effettivo diritto alla disconnessione, dalle insidiose discriminazioni algoritmiche, nonché dalle subdole violazioni del diritto alla riservatezza dei dati personali, tutte criticità emerse dall'ampio dibattito nei panel dedicati.

Il lavoro è in transizione a causa della (o grazie alla) digitalizzazione, ma il cardine resta la sua tutela in tutte le forme ed applicazioni[90], anche digitali, affinché sia «dignitoso»[91], ossia garantisca alle lavoratrici e ai lavoratori condizioni di libertà, equità, salute e sicurezza.

---

[84] Conosciuto internazionalmente come *hybrid work*, è regolamentato da *policies* aziendali ed è caratterizzato da un'ampia possibilità di modulazione della flessibilità di tempo e di luogo, valorizzando il ricorso alla digitalizzazione, in modo da rispondere di volta in volta alle esigenze organizzativo-produttive: v. I. De Clerq, *Hybrid work. A Manifesto*, Brugge, 2021; AA.VV., *Hybridworkplace*, Boston 2022.

[85] *Ex multis*, A. Donini, *Il lavoro attraverso le piattaforme digitali*, Bologna, 2019; V. Maio, *Il lavoro per le piattaforme digitali tra qualificazione del rapporto e tutele*, in *Arg. dir. lav*., 582, 2019; M. Biasi, *Nuove tecnologie e crisi della subordinazione: il caso riders - le (in)attese ricadute di un approccio rimediale al lavoro tramite piattaforma digitale*, in *Giur. it*., 1797, 2020; D. Garofalo, *La prima disciplina del lavoro su piattaforma*, in *Lav. giur*., 2020, 5; G. Santoro Passarelli, *Il lavoro mediante piattaforme digitali e la vicenda processuale dei riders* in *Dir. rel. ind*., 2021, 111.

[86] Per una panoramica sul tema mi sia consentito di rinviare a M. Russo, *Se gli e-Sports non sono (soltanto) un gioco. Qualche riflessione sull'inquadramento giuslavoristico del pro-player*, in *Media Laws*, 2024, 3.

[87] Sul lavoro nel metaverso, v. A. Donini – M. Novella – M.L. Vallauri, *Prime riflessioni sul lavoro nel metaverso*, in *Labour &Law Issues*, 2022; M. Martone, *Prime riflessioni su lavoro e metaverso*, in *Argomenti di Diritto del Lavoro*, 2022, 1131; M. Biasi, *Il decent work e la dimensione virtuale: spunti di riflessione sulla regolazione del lavoro nel Metaverso*, in *Lavoro Diritti Europa*, 2023; M. Russo, *Le sfide nella regolamentazione del lavoro tecnologico: dal lavoro agile al metaverso*, in A. Fuccillo – V. Nuzzo – M. Rubino De Ritis (a cura di), *Diritto e universi paralleli. I diritti costituzionali nel metaverso*, Napoli, 2023, 82.

[88] Dal rischio di isolamento al *burnout*, dall'*overworking* allo stress lavoro-correlato.

[89] Eurofound-OIL, *Working anytime anywhere: the effects on the world of work*, Ginevra, 2017.

[90] Art. 35 Cost.

[91] Il «lavoro dignitoso» è l'obiettivo n. 8 dell'Agenda 2030 dell'OIL.

6. Riflessioni non conclusive

L'avvio della discussione della *Strategia 4.0.* fortemente voluta dal legislatore unionale rappresenta un importante passo in avanti verso temi in continuo sviluppo: un approccio proporzionale e rispettoso di quella che è l'iniziativa privata che, ovviamente, deve essere canalizzata e ben individuata sia sotto il profilo soggettivo che sotto il profilo oggettivo.
Il criterio della proporzionalità, unitamente ad una disciplina *soft*, può definirsi un buon modo di legiferare il progresso tecnologico, fermo restando lo sviluppo delle piattaforme "metaversanti" che, allo stato attuale, è ben lontano dal potersi dire definitivo e concluso, anzi spesso celato nelle sue potenzialità dalle stesse piattaforme timorose di essere strette in lacci e lacciuoli volti a moderare lo sregolato profitto a danno degli utenti e dei diritti fondamentali custoditi nelle Carte.
Cosa potrà, in futuro, la regolazione, fermo restando che resta oggettivamente perdente di fronte alla iper-accelerazione della tecnologia?
Si tratta di problematiche che, al netto della diversità del *medium* tecnico, si traslano in seno agli spazi digitali.
Insomma, non ragionare esclusivamente sul fattore umano, come la naturale e ontologica posizione di vulnerabilità della popolazione digitale che fa fatica ad entrare nell'immaginario collettivo delle grandi piattaforme, piuttosto sul ruolo assunto dalle *Corporation* del capitalismo transazionale, in relazione al nucleo centrale dell'attività di impresa che sta tutta nel rapporto mercato-investimento-guadagno.
Non è solo la semplice somma vettoriale dell'interesse di lucro sulle persone che compongono i nuovi mondi: la regolazione delle grandi piattaforme, se da un lato deve essere eteronormante, in uno spirito quasi escludente – come traspare dal *DSA* e dal *DMA* –, dall'altro lato deve comunque "educare" al valore dei diritti fondamentali e delle libertà costituzionalmente garantite, a prescindere dalla condizione soggettiva di vulnerabilità della persona dentro l'ecosistema digitale e delle difese apprestate dalla regolazione eurounionale.
Il canone di differenziazione a-territoriale dentro i singoli frammenti spaziali, come l'Europa, consente di applicare in ogni caso i principi di ordine costituzionale trasfusi nel nucleo duro dei Trattati, nei regolamenti e nella giurisprudenza delle Corti, da concretizzare, semmai, nella strategia 4.0 in corso di studio da parte della Commissione.
Il percorso è certamente impervio, ma se ne intravede la direzione che non può che essere quella europea: l'adattamento del pacchetto digitale alle nuove sfide poste anche dai "multiversi", o di un intervento regolativo del tutto nuovo, ma sempre volto a realizzare i tratti caratterizzanti della democrazia, anche digitale.

Abstract

L'era delle transizioni digitali si sta affermando con una rapidità tale da incidere su ogni aspetto della società e impone agli studiosi del diritto la necessità di interrogarsi sull'opportunità e sulle modalità di una regolamentazione delle nuove tecnologie. L'erosione delle tradizionali garanzie statuali in un ambiente digitale dematerializzato e la tutela dei diritti fondamentali, il tema dell'autodeterminazione nell'ecosistema di dati, le questioni connesse alla prevenzione e repressione dei reati, le trasformazioni del mondo del lavoro, sono alcuni degli argomenti affrontati nell'ambito della prima Conferenza internazionale La.Ne.T. Le riflessioni interdisciplinari che ne sono scaturite hanno evidenziato l'importanza di individuare un *nomos digitale*, capace di elaborare nuove categorie giuridiche o adattare quelle note ai complessi mutamenti in atto, preservando i principi fondamentali.

The era of digital transitions is asserting itself with such speed that it's impacting every aspect of society. This rapid evolution requires legal scholars to consider the advisability and methods of regulating new technologies. The erosion of traditional state guarantees in a dematerialized digital environment, the protection of fundamental rights, the issue of self-determination within the data ecosystem, questions related to crime prevention and suppression, and transformations in the world of work are some of the topics addressed at the first La.Ne.T. International Conference. The interdisciplinary discussions that emerged highlighted the importance of identifying a *digital nomos* capable of developing new legal categories or adapting existing ones to the complex ongoing changes, all while preserving fundamental principles.

Keywords

costituzionalismo digitale - diritto digitale - regolazione - tecnologia - transizione digitale

Il rischio di decisioni automatizzate in materia di inammissibilità delle impugnazioni penali*

Aldo Franceschini

"[…] lo sviluppo dell'AI fino ad oggi non è andato tanto nella direzione dell'emulazione o del superamento dell'intelligenza umana, quanto verso lo sviluppo di sistemi in grado di convincere noi umani che le macchine sono intelligenti. L'IA, di conseguenza, è intelligente nella misura in cui la consideriamo tale. E il sogno di creare delle macchine intelligenti ha valore nella misura in cui seguitiamo a crederci"

Simone Natale, *Macchine ingannevoli. Comunicazione, tecnologia, intelligenza artificiale*, Einaudi, 2022

Sommario

1. A mo' di premessa (poco tecnologica). - 2. Tendenze normative e paranormative. - 2.1. La proliferazione delle inammissibilità, all'insegna del formalismo e dell'efficientismo. - 2.2. La deprocessualizzazione delle decisioni di inammissibilità. - 2.3. La delega del vaglio preliminare sulle impugnazioni. - 2.4. Il formante giurisprudenziale e la "cultura della inammissibilità". - 2.5. Direttive redazionali, tra formante "protocollare" e limiti dimensionali. - 3. Il processo penale telematico e la digitalizzazione degli atti. - 4. Le risorse tecnologiche al servizio del giudice. - 5. L'intelligenza artificiale generativa e l'esplosione del *Natural Language Processing*. - 6. La futuribile (ma non troppo) automazione delle decisioni in materia di inammissibilità delle impugnazioni. - 7. La "preferenza per l'umano". - 8. L'intollerabile abuso del processo penale come luogo di sperimentazione tecnologica.

1. A mo' di premessa (poco tecnologica)

Correndo il rischio di deludere il lettore, chiarisco subito che nella prima parte del mio contributo non ragionerò di intelligenza artificiale. Nulla di tecnologico, dunque. Questo perché, dal mio punto di vista, per immaginare traiettorie future, è necessario inquadrare prima il contesto attuale e, in particolare, i *trends* che si registrano nelle linee di politica normativa e negli orientamenti espressi dal formante giurisprudenziale[1]. Questa inda-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

[1] Proprio in questa prospettiva di indagine si muovono le autorevoli riflessioni di O.

gine, ovviamente, prescinde del tutto dagli algoritmi e dal loro possibile utilizzo in ambito giudiziario.
D'altra parte, come ha di recente osservato autorevole dottrina, tra le domande urgenti da porsi riflettendo sulla prospettiva della «sostituzione della macchina all'uomo nel campo della giurisdizione» vanno incluse quelle «su come si sia potuti arrivare alle soglie di questo mutamento di paradigma; su quali fattori hanno preparato il terreno perché attecchisse anche solo l'idea di una amministrazione della giustizia "artificiale"»[2].
Secondo avvertimento. Il campo di indagine di questo lavoro afferisce alla giustizia penale ed è circoscritto al tema dell'inammissibilità delle impugnazioni, con una speciale attenzione a quelle ordinarie dell'appello e del ricorso per cassazione.
Nella seconda parte, invece, proverò a "maneggiare" alcune nozioni di matrice tecnologica, limitatamente a quelle che attengono ai congegni potenzialmente impiegabili in materia di inammissibilità. L'attenzione verrà così riservata all'intelligenza artificiale generativa e ai modelli di sviluppo del linguaggio naturale.

2. Tendenze normative e paranormative

Ebbene, osservando le direttrici seguite, negli ultimi anni, dal sistema delle impugnazioni penali, non è difficile rilevare alcune tendenze piuttosto marcate: 1) l'incremento delle fattispecie di inammissibilità; 2) la deprocessualizzazione delle decisioni dichiarative di tale sanzione; 3) la delega del vaglio preliminare sulle impugnazioni; 4) la tendenza della giurisprudenza a favorire esiti di inammissibilità delle impugnazioni; 5) l'introduzione, anche con strumenti di *soft law*, di criteri redazionali e limiti dimensionali per gli atti impugnatori.
Può essere molto proficuo soffermarsi brevemente su ciascuna di esse, anche al fine di comprendere se siano animate da un denominatore comune.

Mazza, *Distopia del processo artificiale*, in ***archiviopenale.it***, 7 gennaio 2025, 6, il quale segnala che «l'avvento della AI nel processo penale è stato largamente favorito e, in qualche misura, anticipato da un modello di giurisdizione penale da tempo coltivato in giurisprudenza e avallato dalla dottrina maggioritaria. Concetti come la formalizzazione e la prevedibilità delle decisioni o la stessa efficienza del sistema giudiziario, intesa quale semplificazione e riduzione dei tempi processuali, ma anche la dimensione oracolistica della prova scientifica, rappresentano la base teorica e il substrato culturale della gestione artificiale del processo». L'Autore più avanti prosegue: «Manca, anzitutto, la consapevolezza del fatto che il fondamento della giustizia artificiale risiede proprio in quegli pseudo valori che ci sono stati imposti a partire dall'inizio del nuovo secolo: il processo breve, di preferenza scritto, digitale e non partecipato, il vincolo dei precedenti della giurisprudenza di legittimità e la prevedibilità delle decisioni, la sinteticità degli atti e le limitazioni ai giudizi di impugnazione, la formalizzazione del decidere e la verticizzazione della giurisdizione».

[2] V. Manes, *Giustizia artificiale. Siamo davvero disposti ad essere giudicati da un algoritmo?*, in *dirittodidifesa.eu*, 3 dicembre 2024, 3, ora anche in *Diritto di Difesa*, 3-4, 2023, 627 ss.

2.1. La proliferazione delle inammissibilità, all'insegna del formalismo e dell'efficientismo

Si registra, innanzitutto, una significativa proliferazione delle ipotesi di inammissibilità. Prima di approfondire il tema, sia consentito gettare un breve sguardo periferico a un profilo critico di carattere generale. Proprio il campo delle impugnazioni consente, infatti, di fare affiorare in modo efficace quel circolo vizioso che si è da tempo instaurato tra il formante legislativo e quello giurisprudenziale[3]: in un numero crescente di casi, quest'ultimo genera e plasma nuove figure, che il primo si limita, a distanza di qualche tempo, a "convalidare", così finendo però per certificare la matrice creativa della soluzione inventata dalla giurisprudenza[4].

E sì, perché una delle più significative fattispecie di inammissibilità di nuovo conio nasce dal laboratorio giurisprudenziale per essere poi recepita supinamente dal nostro legislatore. Il riferimento è all'aspecificità[5] estrinseca dell'atto di appello, prima forgiata nel 2016 nella fucina delle Sezioni unite[6], e poi – dopo il fallito tentativo della riforma Orlando del 2017[7] – disciplinata nor-

[3] Su questo argomento sono magistrali le pagine di P. Ferrua, *L'inammissibilità del ricorso: a proposito dei rapporti tra diritto "vigente" e diritto "vivente"*, in *Cassazione Penale*, 9, 2017, 3006 ss.; Id., *Soggezione del giudice alla sola legge e disfunzioni del legislatore: il corto circuito della riforma Orlando*, in *Diritto penale e processo*, 2017, 1265 ss.; Id., *Il contraddittorio tra declino della legge e tirannia del diritto vivente*, in D. Negri – R. Orlando (a cura di), *Le erosioni silenziose del contraddittorio*, Torino, 2017, 3 ss.

[4] In tal senso, esplicitamente, B. Nacar, *Natura cognitiva della sentenza di patteggiamento e rimedi impugnatori*, Padova, 2022, 273, che denuncia la «positivizzazione degli approdi giurisprudenziali» e che finisce per palesare «la natura creativa delle interpretazioni del diritto vivente».

[5] Per un'analisi molto accurata del concetto di aspecificità, sia pure sviluppata in tema di ricorso per cassazione, si vedano le pagine di F.M. Iacoviello, *La Cassazione penale. Fatto, diritto e motivazione*, Milano, 2013, 757 ss., il quale individua e descrive cinque forme di aspecificità: assenza di critica o ripetizione di argomenti già confutati (il motivo di ricorso apparente); genericità per mancanza di informazioni (motivo carente) o per mancanza di argomenti (motivo apodittico); caoticità (motivo di ricorso confuso); la manifesta illogicità del motivo di ricorso (il motivo di ricorso perplesso); incompletezza (il motivo di ricorso insufficiente).

[6] Il riferimento è a Cass. pen., sez. un., 27 ottobre 2016 (dep. 2017), n. 8825, Galtelli, Pres. Canzio, Rel. Andronio, CED 268822, secondo cui «L'appello, al pari del ricorso per cassazione, è inammissibile per difetto di specificità dei motivi quando non risultano esplicitamente enunciati e argomentati i rilievi critici rispetto alle ragioni di fatto o di diritto poste a fondamento della decisione impugnata, fermo restando che tale onere di specificità, a carico dell'impugnante, è direttamente proporzionale alla specificità con cui le predette ragioni sono state esposte nel provvedimento impugnato». Prese di posizione molto critiche nei confronti dell'arresto delle Sezioni unite si trovano in A. Pulvirenti, *La specificità estrinseca dei motivi di appello come requisito di ammissibilità dell'appello: la fine del* favor impugnationis, in *Processo penale e giustizia*, 4, 2017, 698 ss.; L. Zilletti, *Sezioni Unite e specificità dell'appello*: pròfasis, aitìa, archè, in *Parola alla difesa*, 3, 2017, 257 ss. Attente analisi della pronuncia si leggono, tra gli altri, anche in H. Belluta, *Inammissibilità dell'appello per genericità dei motivi: le Sezioni unite tra l'ovvio e il rivoluzionario*, in *Diritto penale contemporaneo*, 2, 2017, 137 ss.; A. Muscella, *Ammissibilità dell'atto di appello e difetto di specificità dei relativi motivi*, in *Archivio Penale*, 1, 2017, 351 ss.

[7] Il riferimento è all'interpolazione, ad opera della l. 23 giugno 2017, n. 103, degli artt. 546 e 581 c.p.p., la quale, tuttavia, in assenza di una esplicita descrizione della c.d. specificità estrinseca come requisito dell'atto di impugnazione, non ha consentito

mativamente dalla riforma Cartabia nel 2022 (art. 581, co. 1-*bis* c.p.p.)[8].
Parallelamente il legislatore si è anche preoccupato di gravare il sistema delle impugnazioni di sterili formalismi[9], cui fanno da *pendant* altrettante ipotesi di inammissibilità. È il caso, ad esempio, degli oneri di allegazione all'atto di impugnazione della dichiarazione o elezione di domicilio (art. 581 co. 1-*ter* c.p.p.) e del mandato specifico a impugnare per l'imputato nei cui confronti si sia proceduto in assenza (art. 581 co. 1-*quater* c.p.p.), introdotti dalla riforma Cartabia del 2022[10]. Stante il carattere marcatamente defatigante di tali incombenze, difficile scacciare il sospetto che l'obiettivo della riforma fosse quello di porre ostacoli alle impugnazioni in chiave efficientista[11] per incidere in modo drastico sul segmento processuale esposto alle maggiori criticità in termini di durata e *performance*, ossia il giudizio di appello (da molti icasticamente definito il "collo di bottiglia" del sistema).
Sebbene la legge Nordio di agosto 2024[12] abbia cercato di porre rimedio a una deriva formalistica, l'operazione di rimuovere i congegni meramente deflativi introdotti nel 2022 è riuscita solo in parte: è stato eliminato l'incombente della dichiarazione o elezione di domicilio, mentre quello relativo al mandato specifico a impugnare è stato ricalibrato lasciandolo solo per il difensore di ufficio. Sagomatura chirurgica che, tuttavia, risulta inaccettabile, perché proprio quest'ultima figura soffre la conclamata difficoltà di entrare in contatto con il proprio assistito: nella maggior parte dei casi, dunque, nonostante la valutazione di opportunità, sarà preclusa al difensore d'ufficio la possibilità di proporre impugnazione avverso la sentenza di primo grado, a scapito del

di reputare implementata la sanzione dell'inammissibilità in caso di suo difetto. Sulla sostanziale "inefficacia", *in parte qua*, della riforma, si veda A. Pulvirenti, *La "nuova" specificità e il pericolo di nuovi spazi concessi all'inammissibilità dell'appello*, in *archiviopenale.it*, 22 marzo 2023, 4-5.

[8] Il d.lgs. 10 ottobre 2022 n. 150 ha introdotto il c. 1-*bis* dell'art. 581 c.p.p., a mente del quale: «L'appello è inammissibile per mancanza di specificità dei motivi quando, per ogni richiesta, non sono enunciati in forma puntuale ed esplicita i rilievi critici in relazione alle ragioni di fatto o di diritto espresse nel provvedimento impugnato, con riferimento ai capi e punti della decisione ai quali si riferisce l'impugnazione».

[9] Sul concetto di formalismo non può non ricordarsi il fondamentale saggio di S. Satta, *Il formalismo nel processo*, (1958), ora in Id., *Il mistero del processo*, Adelphi, 1994, 100 ss.

[10] D.lgs. 10 ottobre 2022 n. 150, attuazione della legge 27 settembre 2021 n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari.

[11] Il tema dell'efficientismo, ad onta del carattere cacofonico del termine, presenta grande attualità e meriterebbe di essere tematizzato in dottrina. Parla espressamente di *efficientismo processuale*, a proposito dell'ideologia che ispira la recente riforma Cartabia, O. Mazza, *L'efficientismo del processo post-accusatorio*, in *Archivio della nuova procedura penale*, 6, 2022, 498 ss., spec. 499-501. Per una abbozzata definizione di efficientismo, si veda, volendo, L. Cricrì – F. De Maria – A. Franceschini, *L'ufficio per il processo: tra vocazione efficientista e salvaguardia della funzione giurisdizionale*, in G. Colaiacovo – F. Delvecchio – W. Nocerino (a cura di), *Gli snodi problematici della riforma Cartabia con uno sguardo al futuro*, Bari, 2023, 263 ss., spec. 265-266. Interessanti le riflessioni di G. Caneschi, *L'imputato*, Milano, 2021, 70 ss., che denuncia la natura tensiva della visione efficientista rispetto alla presunzione di innocenza.

[12] L. 9 agosto 2024 n. 114, recante *Modifiche al codice penale, al codice di procedura penale, all'ordinamento giudiziario e al codice dell'ordinamento militare*. L'art. 2, c. 1, lett. *o)*, ha abrogato il c. 1-*ter* dell'art. 581 c.p.p. che prevedeva l'onere di allegare la dichiarazione o l'elezione di domicilio all'atto di impugnazione.

cittadino. E d'altra parte non può sfuggire che questo ostacolo[13] all'esercizio del diritto di impugnare il provvedimento di merito produrrà un impatto estremamente significativo dal punto di vista del carico di lavoro delle corti d'appello.

I formalismi, purtroppo, appaiono destinati a crescere esponenzialmente a seguito dell'entrata a regime del processo penale telematico. Al riguardo parte della dottrina, già parla espressamente di «formalismo digitale»[14].

Propensione che è iniziata ad affiorare durante il periodo emergenziale Covid, che si è rivelato un "formidabile" laboratorio di soluzioni dal taglio efficientista. Basti qui ricordare le ipotesi di inammissibilità introdotte dalla l. n. 176 del 2020, aggiuntive rispetto a quelle classiche previste dall'art. 591 c.p.p. e imperniate sul rispetto di canoni digitali[15]. Per giunta con la eccentrica soluzione di attribuire al giudice del provvedimento impugnato il potere-dovere di verificare la sussistenza di tali situazioni di inammissibilità[16].

In questa cornice normativa, la giurisprudenza, ancora una volta, sta giocando un ruolo determinante: una vasta frangia, animata dall'intento di potenziare gli strumenti deflativi, si impegna infatti nel tirar fuori dalle norme il maggior numero di situazioni capaci di espellere dal sistema una parte del carico di lavoro. Così, ad esempio, si spiega la recente decisione del Giudice di legittimità con cui è stata validata l'interpretazione in virtù della quale sarebbe inammissibile l'impugnazione trasmessa, a mezzo posta elettronica certificata, ad un indirizzo risultante dall'elenco "ufficiale" a suo tempo diramato dalla Direzione generale dei servizi informativi automatizzati, ma non corrispondente a quello associato, nell'ambito dell'ufficio giudiziario di riferimento, all'organo destinatario dell'atto[17]. Oppure le

---

[13] Con riferimento a questi formalismi introdotti dalla riforma Cartabia, parla espressamente di ostacolo, F. Compagna, *L'appello dell'imputato assente: un diritto costituzionale sottoposto a nuovi ostacoli*, in *penaledp.it*, 9 giugno 2023.

[14] L. Tavassi, *Formalismi giurisprudenziali e forme tecnologiche nel giusto processo digitale*, in *archiviopenale.it*, 1 marzo 2024, 23; Ead., *Il labirinto telematico per la trasmissione degli atti*, in *dirittodidifesa.eu*, 8 gennaio 2025, 6, 11, 19.

[15] L'art. 24, c. 6-*sexies*, della l. n. 176 del 2020 prevedeva infatti l'inammissibilità dell'atto di impugnazione nelle seguenti ipotesi: a) quando l'atto di impugnazione non è sottoscritto digitalmente dal difensore; b) quando le copie informatiche per immagine di cui al c. 6-*bis* non sono sottoscritte digitalmente dal difensore per conformità all'originale; c) quando l'atto è trasmesso da un indirizzo di posta elettronica certificata che non è presente nel Registro generale degli indirizzi certificati di cui al c. 4; d) quando l'atto è trasmesso da un indirizzo di posta elettronica certificata che non è intestato al difensore; e) quando l'atto è trasmesso a un indirizzo di posta elettronica certificata diverso da quello indicato per l'ufficio che ha emesso il provvedimento impugnato dal provvedimento del Direttore generale dei sistemi informativi e automatizzati di cui al c. 4 o, nel caso di richiesta di riesame o di appello contro ordinanze in materia di misure cautelari personali e reali, a un indirizzo di posta elettronica certificata diverso da quello indicato per il tribunale di cui all'art. 309, c. 7, c.p.p. dal provvedimento del Direttore generale dei sistemi informativi e automatizzati di cui al c. 4.

[16] Cfr. art. 24, c. 6-*septies*, l. n. 176 del 2020.

[17] Cfr. Cass. pen., sez. I, 29 novembre 2024, n. 47557, Pres. Santalucia, Rel. Masi, CED 287294-01, ove si legge «In tema di impugnazioni, è inammissibile il ricorso per cassazione depositato telematicamente presso un indirizzo di posta elettronica certificata diverso da quello indicato nel decreto del Direttore generale per i sistemi informativi automatizzati di

decisioni che censurano la mancanza della firma digitale, pur non essendo dubbia la provenienza del deposito dell'atto[18].
Poi ci sono le ipotesi di inammissibilità gemmate dalla sforbiciata all'impugnabilità oggettiva delle sentenze di patteggiamento[19], su cui ha lavorato la riforma Orlando con l'art. 448, c. 5-*bis*, c.p.p. Dalla rigida perimetrazione dei margini di ricorribilità (motivi attinenti all'espressione della volontà dell'imputato, al difetto di correlazione tra la richiesta e la sentenza, all'erronea qualificazione giuridica del fatto e all'illegalità della pena o della misura di sicurezza) discende la speculare implementazione della sanzione processuale destinata a colpire le impugnazioni che vadano "fuori bersaglio".
Insomma, una tendenza generalizzata ispirata ad un approccio che frustra il tradizionale principio del *favor impugnationis*[20] e della c.d. conservazione degli atti. Principio, quest'ultimo, che – per inciso – la giurisprudenza non lesina di evocare ogniqualvolta si tratti di "salvare" un atto o un provvedimento del giudice.

2.2. La deprocessualizzazione delle decisioni di inammissibilità

Altro fattore rilevante consiste nella semplificazione delle procedure che

cui all'art. 87-bis, c. 1, d.lgs. 10 ottobre 2022, n. 150. (In motivazione, la Corte ha precisato che la "ratio" sottesa alla citata disposizione, di semplificazione delle comunicazioni tra parti e uffici giudiziari e di accelerazione degli adempimenti di cancelleria, non ammette interpretazioni che attenuino il rigore delle cause di inammissibilità previste dalla legge, nemmeno valorizzando l'idoneità della notifica al "raggiungimento dello scopo")».

[18] Cfr. Cass. pen., sez. IV, 25 ottobre 2023, n. 48545, CED 285571-01, secondo cui: «è inammissibile l'impugnazione proposta dal difensore con atto in formato digitale privo di sottoscrizione digitale, trasmesso a mezzo di posta elettronica certificata (Fattispecie relativa al deposito dell'atto di appello da parte del difensore in formato "smime,p7c", inviato da un indirizzo di posta elettronica riconducibile al predetto, in cui la Corte ha precisato che l'utilizzo di tale estensione del file, in assenza di sottoscrizione digitale, non è sufficiente a provarne l'attribuibilità al professionista legittimato)».

[19] B. Nacar, *Natura cognitiva della sentenza di patteggiamento e rimedi impugnatori*, Padova, 2022, 267 ss.

[20] Sulla sterzata del sistema in una direzione opposta al *favor impugnationis* e per una decisa critica di questa tendenza, si vedano, tra gli altri, M. Ceresa Gastaldo, *La riforma dell'appello, tra malinteso garantismo e spinte deflative*, in *Diritto penale contemporaneo*, 3, 2017, 170, il quale lamenta che «l'idea che sembra dominare la logica dell'irrigidimento dei requisiti formali dell'atto è che valga in materia una presunzione di strumentalità dell'iniziativa impugnatoria della parte, rispetto alla quale il *favor impugnationis* non è altro che un segno della decadenza dei "costumi" processuali, un sintomo dell'atteggiamento colpevolmente lassista del giudice che ammette controlli non dovuti, ritardando l'esecuzione della sentenza. Un'idea tanto discutibile sul piano esegetico, quanto pericolosa nella prospettiva de iure condendo. Il *favor impugnationis*, infatti, è innanzitutto, un ineludibile canone interpretativo delle norme che sacrificano l'interesse (non solo del singolo, ma prima di tutto) pubblico alla giustizia sostanziale della decisione penale a favore dell'esigenza di certezza del diritto, ossia di relativa economicità e tempestività dell'intervento giurisdizionale». In argomento si veda anche F. Talamo, *Il mutamento giurisprudenziale su una norma processuale sfavorevole ma prevedibile*, in *dirittodidifesa.eu*, 27 gennaio 2022, 8-9, il quale stigmatizza «una costante azione di offuscamento del principio del *favor impugnationis* nel processo penale, in virtù di un efficientismo giudiziario elevato illegittimamente a valore costituzionale».

disciplinano il vaglio di ammissibilità. Si pensi al modulo «senza formalità di procedura» per la dichiarazione di inammissibilità[21], in alcuni casi, del ricorso per cassazione[22], plasmato all'insegna di un'autentica deprocessualizzazione[23] di tale tipologia di decisioni. Si tratta del congegno disciplinato dall'art. 610, c. 5-*bis*, c.p.p., introdotto dalla riforma Orlando[24]. Una procedura iper-semplificata[25], che finisce inoltre per propiziare, ineluttabilmente, la monocratizzazione della decisione, accentrandola nelle figure del consigliere "spogliatore" o di quello relatore, e facendo così evaporare del tutto la collegialità.

Si tenga conto che le situazioni attratte in questa sorta di insondabile "buco nero" non sono poche e non sono (ad eccezione di qualche caso) affatto marginali. Vi rientrano, infatti, le ipotesi di: 1) difetto di legittimazione (art. 591, c. 1, lett. a) c.p.p.); 2) non impugnabilità del provvedimento (art. 591, c. 1, lett. b) c.p.p.); 3) inosservanza delle disposizioni in materia di presentazione dell'atto impugnatorio, di termini e di impugnazione di ordinanze dibattimentali (art. 591, c. 1, lett. c) c.p.p.); 4) rinuncia all"impugnazione (art. 591, c. 1, lett. d) c.p.p.); 5) inammissibilità del ricorso avverso le sentenze di patteggiamento; 4) inammissibilità del ricorso avverso le sentenze pronunziate all'esito del c.d. concordato in appello.

L'assoluta inadeguatezza di tale modello deliberativo per la decisione sulla sorte degli atti di impugnazione appare in modo plastico se solo si pensi al fatto che esso, nell'impianto originario del codice di rito, era destinato a regolamentare il momento decisorio di procedure con oggetto "semplice" e, in ogni caso, diverso dalla *res iudicanda* principale. Tre, in particolare, sono le fattispecie processuali che vengono in rilievo.

La prima che balza all'attenzione è quella che ospita il prototipo del procedimento *de plano*, regolamentato dall'art. 667, co. 4, c.p.p. («il giudice provvede in ogni caso senza formalità»)[26]. Questo modulo è riservato alle decisioni del giudice dell'esecuzione in ordine a: 1) dubbio sull'identità fisica della persona detenuta (art. 667 c.p.p.); 2) applicazione dell'amnistia e dell'indulto (art. 672 c.p.p.); 3) estinzione del reato dopo la condanna e della pena, pene accessorie, confisca o restituzione di cose sequestrate (art. 676 c.p.p.); 4) sequestro e confisca in casi particolari previsti dall'art.

---

[21] In argomento si vedano C. Scaccianoce, *Sull'inammissibilità del ricorso straordinario: procedura* de plano *o contraddittorio cartolare?*, in *Archivio penale*, 3, 2017, 1033 ss.; F. Tribisonna, *L'inammissibilità "de plano" del ricorso per cassazione privo di uno specifico mandato ad impugnare: una lettura estensiva non priva di insidie*, in *Processo penale e giustizia*, 3, 2024, 698 ss.

[22] B. Nacar, *Natura cognitiva della sentenza di patteggiamento e rimedi impugnatori*, Padova, 2022, 280, parla di «rigido controllo di inammissibilità», richiamando il 610 c. 5-*bis* c.p.p.

[23] Parla di deprocessualizzazione, O. Mazza, *L'efficientismo del processo post-accusatorio*, in *Archivio della nuova procedura penale*, 6, 2022, 498, e O. Mazza, *Distopia del processo artificiale*, in *archiviopenale.it*., 7 gennaio 2025, 3.

[24] Per un'analisi critica di tale innovazione si veda, volendo, A. Franceschini, *Rito non partecipato in appello, scoria del periodo emergenziale tra efficientismo e delegificazione*, in *Diritto di Difesa*, 2, 2022, 363 ss.

[25] Con questo sintagma lo denotavo in A. Franceschini, *Rito non partecipato in appello, scoria del periodo emergenziale tra efficientismo e delegificazione*, cit., 363. Nello stesso lavoro utilizzo anche l'espressione ancora più "radicale" di «non-procedura» (364)

[26] In argomento si veda F. Caprioli – D. Vicoli, *Procedura penale dell'esecuzione*, II ed., Torino, 2011, 358 ss.

240-*bis* c.p. (e da altre disposizioni che ad esso rinviano) dopo l'irrevocabilità della sentenza (art. 183-*quater* disp. att. c.p.p.)[27]. A questo schema semplificato rinviano poi diverse disposizioni in tema di competenze della magistratura di sorveglianza (art. 678, co. 1 e 1-*bis*, c.p.p.)[28]. Va però rammentato che tale fattispecie ha natura eventualmente complessa, nel senso che i soggetti interessati conservano la facoltà potestativa di promuovere opposizione contro il provvedimento *de plano*, provocando l'innesco di una procedura in contraddittorio dinanzi allo stesso giudice.

La seconda fattispecie è quella ospitata nel c. 9 dell'art. 127 c.p.p., secondo cui l'inammissibilità dell'atto introduttivo del procedimento camerale è dichiarata dal giudice con ordinanza «anche senza formalità di procedura, salvo che sia altrimenti stabilito»[29]. In particolare, al di là del facile rilievo che fa perno sulla estrema versatilità del modulo camerale, va segnalato che, da tempo, la dottrina più sensibile al tema delle garanzie guarda con severo occhio critico alla previsione normativa contenuta in tale disposizione, assegnandole carattere residuale ed eccezionale, specie a seguito della costituzionalizzazione del principio del contraddittorio nell'art. 111, co. II, Cost.[30].

In realtà – ed ecco il richiamo normativo che mi pare più significativo per profilare la caratura delle decisioni che il legislatore del 1988 ha stimato compatibili con la totale assenza di forme –, se si fruga con zelo il codice, ci si imbatte in una fattispecie che presenta un'assoluta identità, in termini di enunciato normativo, rispetto al disposto contenuto nell'art. 610, co. 5-*bis*, c.p.p. Si scopre così che il modulo iper-semplificato ispira il segmento conclusivo del procedimento di astensione, quello in cui il capo dell'ufficio giudiziario (*ergo*, un organo monocratico) deve decidere se accogliere o meno una *dichiarazione* formulata da un giudice del suo ufficio. Si legge, nel corpo dell'art. 36, co. 4, c.p.p., che il presidente della corte o del tribunale «decide con decreto senza formalità di procedura», con formula del tutto sovrapponibile a quella che compare nell'art. 610, c. 5-*bis* c.p.p. Difficile non rimanere perplessi, tenuto conto della siderale differenza tra

[27] L'utilizzo del modulo semplificato per le decisioni in materia di sequestro e confisca è stato introdotto nel 2018 (l. 1 marzo 2018 n. 21) e si inserisce nel solco normativo che ne favorisce la diffusione per la sua agilità e attitudine semplificativa, parallelamente percorso anche sul versante delle decisioni di competenza del magistrato di sorveglianza (si veda, in particolare, il c. 1-bis dell'art. 678 c.p.p., introdotto dal d.l. 23 dicembre 2013 n. 146).

[28] La Riforma Orlando, nell'incidere in modo significativo sul recupero delle pene pecuniarie, si affida proprio al procedimento de plano per regolamentare alcuni snodi decisori, come ad esempio quello relativo alla rateizzazione del pagamento (art. 660, c. 3, c.p.p.) e alla conversione della pena pecuniaria (art. 660, c. 8, c.p.p.).

[29] Per una scrupolosa analisi dell'istituto, per tutti, si veda G. Di Chiara, *Il contraddittorio nei riti camerali*, Milano, 1994, spec. 187 ss. Il lavoro offre anche un'utile indagine storica sulle procedure *de plano* nel codice di rito del 1930 (19 ss.)

[30] R. Fonti, *Il procedimento in camera di consiglio*, in G. Spangher (a cura di), *Trattato di procedura penale*, Vol. 1, tomo II, Torino, 2008, 62 ss.; F. Porcu, sub *Art. 127 c.p.p.*, in A. Giarda – G. Spangher (a cura di), *Codice di procedura commentato*, V ed., Vicenza, 2017, 1286 ss. Parlava già di «residuale categoria» G. Di Chiara, *Il contraddittorio nei riti camerali*, Milano, 1994, 188, secondo cui «i provvedimenti *de plano*, pur certamente continuando a godere pieno diritto di cittadinanza nel sistema, costituiscono, tuttavia, l'eccezione e non – come erroneamente si sostiene – la regola».

l'oggetto delle eterogenee decisioni: da un lato l'esito del giudizio di impugnazione sulla pronuncia in ordine alla responsabilità penale del cittadino, dall'altro la dichiarazione di astensione di un giudice.
D'altra parte sembra che il c.d. diritto vivente brighi ormai per espandere l'area operativa della procedura iper-semplificata, cercando di superare i confini applicativi tratteggiati nella disposizione. Così, ad esempio, nonostante l'art. 610, co. 5-*bis*, c.p.p. espressamente escluda, dalla sua sfera d'azione, le situazioni riconducibili all'inosservanza delle disposizioni dettate dall'art. 581 c.p.p., la Corte di cassazione, di recente, ha ritenuto che vada seguito il modulo «senza formalità di procedura» anche nell'ipotesi di mancanza di specifico mandato a impugnare, facendo leva sul richiamo (contenuto nella disposizione) al difetto di legittimazione di cui all'art. 591, co. 1, lett. a) c.p.p., risolvendo così su (asserite) basi sistematiche[31] la (predicata) aporia tra disposizioni normative[32].
Ma non è tutto. A seguito dello sdoganamento della (non)procedura *de plano* per assumere decisioni sul tema principale del giudizio penale, in alcune pronunce si cerca di attribuire *vis espansiva* al modello iper-semplificato, come se fosse un archetipo decisorio di carattere generale[33], in evidente controtendenza rispetto all'orientamento della dottrina poc'anzi ricordato.

2.3. La delega del vaglio preliminare sulle impugnazioni

Altro fenomeno riguarda la sfera organizzativa, con il sostanziale "declassamento" delle attività preliminari in punto di ammissibilità dell'atto impugnatorio, che in alcuni uffici giudiziari sono affidate alle risorse dell'ufficio per il processo. Così in Cassazione per lo "spoglio" dei ricorsi e presso la

[31] Sul carattere potenzialmente strumentale del metodo interpretativo sistematico, si vedano le "affilate" critiche di C. Valentini, *Norme processuali e interpretazione*, in *Cassazione Penale*, 9, 2019, 3396 ss.

[32] Cfr. Cass. pen., sez. II, 15 gennaio 2024, n. 4800, ord., Pres. Petruzzellis, Rel. Messini D'Agostini , CED 285927-01, secondo cui: «Nel caso di ricorso per cassazione proposto, in violazione dell'art. 581, comma 1-*quater*, cod. proc. pen., da difensore privo di specifico mandato a impugnare rilasciato successivamente alla pronunzia della sentenza, è possibile dichiarare l'inammissibilità dell'impugnazione con procedimento "de plano" ex art. 610, comma 5-*bis*, cod. proc. pen., posto che il contrasto tra la disposizione che prevede l'anzidetta procedura non partecipata anche per i ricorsi proposti da soggetto non legittimato e quella, egualmente contenuta in tale norma, che la esclude in caso di inosservanza delle previsioni di cui all'art. 581 cod. proc. pen. deve essere risolto accordando la prevalenza alla prima, potendosi ritenere che il riferimento a tale articolo, nella sua interezza, sia rimasto invariato per un difetto di coordinamento».

[33] Cfr. Cass. pen., sez. II, 8 febbraio 2022, n. 23244, Pres. Rago, Rel. Beltrani, CED 283441-02, la quale ha ritenuto legittimo l'impiego, da parte del Tribunale di Napoli, della procedura de plano, «ovvero senza formalità», per decidere sulla domanda di sospendere l'esecutività dell'ordinanza che, accogliendo l'appello cautelare del pubblico ministero, aveva disposto il sequestro dei beni, in quanto, «considerato che l'istanza dei ricorrenti non era disciplinata dal vigente codice di rito, che non ne contempla l'ammissibilità e/o la proponibilità, difettava un richiamo alla necessità di procedere con rito camerale partecipato, ai sensi dell'art. 127 cod. proc. pen.».

Settima Sezione; ma anche presso diverse corti di appello[34].
In realtà la direttrice di una significativa delega delle funzioni di filtro preliminare sulle impugnazioni è stata preceduta, con riguardo alla Corte di cassazione, da una tendenza comunque attinente a profili di organizzazione del lavoro giudiziario.
Mi riferisco alla concentrazione di tali attività, con l'istituzione di una sezione dedicata (la famigerata "Settima") e la creazione della figura del magistrato addetto allo spoglio[35]. Opzioni che, all'evidenza, non possono considerarsi neutre rispetto alle concrete modalità di svolgimento di tali mansioni e al volume delle inammissibilità: un conto è che la valutazione di inammissibilità sia per così dire diffusa tra tutti i giudici che compongono il collegio; discorso ben diverso è che via sia un magistrato dedicato all'esercizio di una funzione selettiva e che abbia, tra l'altro, la *mission* di "scovare" le inammissibilità al fine di instradarle su di un binario processuale "privilegiato".
Ma questa è una scelta che ormai appartiene al passato[36]. L'attualità è rappresentata dalla tendenziale delegazione delle attività di filtro sull'*input* dei giudizi di legittimità alle risorse dell'ufficio per il processo[37] nella "prima lettura" dell'atto impugnatorio e nella redazione di una scheda riassunti-

[34] A. Franceschini, *Gli uffici per il processo penale e l'esercizio della funzione giurisdizionale: per un approccio esternalista*, in *archiviopenale.it*, 14 luglio 2023, 28 ss.

[35] Si tratta di un argomento poco esplorato in dottrina. Per un approccio ad esso, si vedano A. Bassi, *La gestione operativa della funzione nomofilattica della Corte suprema di cassazione*, in *Sistema Penale*, 3, 2020, 69 ss.; A. Remelli, *L'imparzialità del magistrato "spogliatore" che componga il collegio della sezione-filtro: una soluzione interpretativa nel solco della giurisprudenza costituzionale*, in *archiviopenale.it*, 2, 2016.

[36] Vale la pena segnalare il tentativo del Consiglio superiore della magistratura di suggerire la sostanziale "esportazione" di questo modello organizzativo caratterizzato dalla centralizzazione dell'esame preliminare degli atti introduttivi. Nelle *Linee guida in materia di esame preliminare delle impugnazioni e modalità stilistiche di redazione dei provvedimenti* (delibera 5 luglio 2017), si propone, per favorire la «valutazione attenta di eventuali profili di inammissibilità» e una «proficua organizzazione del lavoro», la creazione, nelle corti di piccole-medie dimensioni, di un unico ufficio "spoglio" centralizzato e, nelle corti di maggiori dimensioni, di uffici "spoglio" sezionali. A questo progetto è stato dato seguito con il successivo invito, rivolto ai dirigenti degli uffici giudiziari di secondo grado, di «introdurre, mediante le opportune previsioni tabellari, la struttura deputata all'esame preliminare delle impugnazioni secondo modelli flessibili in rapporto alle singole realtà territoriali» (cfr. CSM, *Esame preliminare delle impugnazioni e tecniche di redazione degli atti del giudizio d'appello: cooperazione tra il Consiglio superiore della magistratura ed il Consiglio nazionale forense per l'attuazione pratica delle linee guida*, delibera 22 novembre 2017). Le *Linee guida* del 2017 sono analizzate in modo approfondito da D. Cavallini, *Linee guida* e best practices *in materia organizzativa e processuale: le nuove frontiere del Csm*, in *archiviopenale.it*, 10 novembre 2020, 9 ss., la quale (5) considera emblematica degli interventi del Consiglio superiore della magistratura che presentano «implicazioni anche sul piano ordinamentale e processuale» proprio «la delibera in materia di esame preliminare delle impugnazioni che arriva a suggerire l'adozione di un "filtro" in appello in materia penale, nonostante non via sia alcuna previsione legislativa che lo contempli espressamente» (l'Autrice ritorna poi sull'argomento anche in seguito, 13).

[37] D'altra parte alcuni studiosi già segnalano come l'ufficio per il processo possa essere «sede per lo sviluppo dei sistemi di intelligenza artificiale». Così P. Bonini, *Le coordinate costituzionali per un sistema di intelligenza artificiale al servizio della funzione giurisdizionale*, in V. Maffeo – A. Romano – P. Troncone, *Intelligenza artificiale e processo*, Torino, 2024, 23 ss.

va[38]. Discorso simile vale per i giudizi di appello: anche qui ai funzionari addetti all'ufficio per il processo vengono affidate mansioni che, a ben vedere, intaccano il nucleo della funzione giurisdizionale[39].

2.4. Il formante giurisprudenziale e la "cultura della inammissibilità"

Da tempo si denuncia una spinta tendenza della giurisprudenza ad abusare della sanzione processuale che inibisce l'esame nel merito dell'atto impugnatorio. Parte della dottrina parla, apertamente, di una vera e propria "cultura della inammissibilità"[40].
Basti guardare ai numeri che si registrano in Corte di cassazione: nel 2023 questo epilogo ha colpito circa il 71,2% dei ricorsi[41].
Non è, quindi, meramente suggestiva la testé ricordata espressione, coniata proprio per denotare un conclamato fenomeno di autentico favore per l'inammissibilità. Per inciso, vale a questo proposito osservare che la "cultura della inammissibilità" rappresenta uno degli aspetti del più complesso concetto di "cultura della giurisdizione", sintagma piuttosto abusato specie quando si discorre del divisivo (e oggi quanto mai attuale) tema della separazione delle carriere[42]. Ebbene, se con questa espressione intendiamo

[38] Si tratta di funzioni espressamente attribuite dalla legge ai funzionari addetti all'ufficio per il processo istituito presso la Corte di cassazione. In effetti, ai sensi del n. 1) e del n. 3) dell'art. 8, c. 1, lett. *b)* d.lgs. n. 151 del 2022, ad essi vengono attribuiti anche i seguenti compiti: la compilazione della scheda del ricorso, corredata delle informazioni pertinenti quali la materia, la sintesi dei motivi e l'esistenza di precedenti specifici; l'assistenza nella fase preliminare dello spoglio dei ricorsi, anche attraverso l'individuazione di tematiche seriali.

[39] Con riferimento al giudizio di appello, si veda, a titolo esemplificativo, la *Relazione sull'Amministrazione della Giustizia nel Distretto nell'Anno Giudiziario 2024*, presentata il 25 gennaio 2025 dal Presidente della Corte di appello di Napoli, ove si legge (14, nel paragrafo dedicato a *Gli addetti all'ufficio per il processo*): «il modello organizzativo prevalentemente adottato in tutti i Settori della Corte di Appello è stato caratterizzato dall'assegnazione dei singoli Addetti alle diverse Sezioni, all'interno delle quali ciascuno coadiuva il magistrato di riferimento, di solito con criterio di rotazione, nelle attività preparatorie dell'udienza, nella compilazione di schede riassuntive dei procedimenti trattati, nello studio e approfondimento delle questioni giuridiche affrontate e nella funale predisposizione di bozze di provvedimenti». Dalla Relazione emerge pure che al Settore penale della Corte è stato assegnato il contingente più cospicuo di funzionari, ben 107 unità (a fronte dei 70 nel Settore civile) distribuiti tra sette sezioni penali. Dato, questo, che lascia desumere il coinvolgimento di tali funzionari in una rilevante aliquota di affari giudiziari, anche in considerazione di un altro aspetto di cui pure si dà conto nella Relazione, ossia la graduale riduzione del loro «apporto alle attività di tipo amministrativo e di supporto alla cancelleria».

[40] O. Mazza, *La nuova cultura dell'inammissibilità fra paradossi e finzioni legislative*, in *Cassazione Penale*, 10, 2017, 3472 ss.

[41] Cfr. Cass. Uff. statistica, *La Cassazione penale. Annuario statistico 2023*, Tab. 5.4: *Procedimenti definiti: classificazione per esito*. Dal raffronto diacronico con i numeri delle annualità precedenti, emerge anche una crescita delle inammissibilità di oltre dieci punti dal 2013. Nella sezione *Statistiche* del sito istituzionale della Corte di cassazione sono consultabili anche altri *report*.

[42] Sul significato della locuzione si sofferma, di recente, con grande autorevolezza T.

l'insieme dei valori espressi, in un dato momento storico, dai protagonisti della giurisdizione in senso stretto (*id est*, i giudici) nell'esercizio della loro funzione e, in particolare, nei provvedimenti che rappresentano il prodotto di tale attività, anche una spiccata tendenza a favorire esiti di inammissibilità costituisce un momento sintomatico di tale cultura.
Così come non può essere privo di significato che la percentuale di inammissibilità sia marcatamente asimmetrica tra ricorsi presentati dal pubblico ministero e quelli interposti dalle parti private: nel 2023, i primi non vanno oltre il 34,1% di tutte le inammissibilità, mentre i secondi sfondano la quota del 72,8% sul totale di tali esiti, mostrando un assestamento, rispetto all'anno precedente, di tale tendenza[43].
Favore per l'inammissibilità che, nel giudizio di legittimità[44], si esalta soprattutto sul terreno della manifesta infondatezza, una categoria concettuale dai contorni fumosi, che il nostro ordinamento, ispirato alla legalità processuale (art. 111, c. I, Cost.), avrebbe dovuto "rigettare" per evidente indeterminatezza della fattispecie[45]. Un costrutto giuridico praticamente insondabile nelle sue declinazioni pratiche[46].

2.5. Direttive redazionali, tra formante "protocollare" e limiti dimensionali

Va poi segnalato il tentativo di introdurre, anche con strumenti di *soft law*, parametri redazionali per il confezionamento degli atti di impugnazione. Il pensiero corre, anzitutto, al famigerato protocollo del 2015 tra Corte di cassazione e Consiglio nazionale forense per la redazione dei ricorsi penali[47] (e al suo omologo per la stesura dei ricorsi in materia civile e tributaria[48]).

Padovani, *Separare le carriere? La domanda è: perché mai sono unite?*, su *L'Unità*, 3 febbraio 2025, 5.

43 I dati riportati nel testo, di recente, sono stati segnalati da A. De Caro, *Ricorso per cassazione e clausole di inammissibilità non formali*, relazione tenuta all'ultimo convegno annuale dell'Associazione tra gli Studiosi del Processo Penale, dal titolo *Dove va la giustizia penale*, svoltosi presso l'Università degli Studi di Milano, 12-14 dicembre 2024.

44 Sul tema, ormai da diversi lustri molto spigoloso, resta centrale il lavoro di L. Marafioti, *Selezione dei ricorsi penali e verifica d'inammissibilità*, Torino, 2004.

45 In tal senso, e anche per la denuncia di indeterminatezza della fattispecie, si veda la relazione di A. De Caro, *Ricorso per cassazione e clausole di inammissibilità non formali*, cit.

46 Sul carattere oscuro della formula si vedano le suggestive pagine di F.M. Iacoviello, *La Cassazione penale. Fatto, diritto e motivazione*, Milano, 2013, 809, che definisce la manifesta infondatezza come «un territorio senza legge», considerandola, senza giri di parola, «l'arma – poco affilata – della pur temuta 7 sezione penale della Cassazione, che serve per stoppare un gran numero di ricorsi». L'Autore lamenta che «la Cassazione evita accuratamente di motivare le proprie scelte: lo stesso ricorso anche all'interno della medesima Sezione, per uno è rigetto per un altro è inammissibilità» e conclude che «è l'epistemologia privata del giudice – rigorosamente celata ad occhi estranei – che decide se un ricorso è inammissibile o da rigettare, se la prescrizione funziona o è congelata».

47 Cfr. *Protocollo d'intesa tra la Corte di cassazione e il Consiglio nazionale forense sulle regole redazionali dei motivi di ricorso in materia penale*.

48 Cfr. *Protocollo d'intesa tra la Corte di cassazione e il Consiglio nazionale forense in merito alle regole*

Si tratta di parametri, anche di natura grafica (tipo carattere, dimensione, spaziature, etc.), volti, evidentemente, a favorirne (anche) la possibile lettura automatizzata[49]. Parametri che, in assenza di espresso recepimento in sede normativa, non dovrebbero rivestire alcuna rilevanza in punto di ammissibilità del ricorso[50]. Ma, evidentemente, non tutti sono d'accordo sul punto, se si annoverano decisioni della Suprema Corte che hanno finito per attribuirvi, sia pure indirettamente, rilievo per decretare la inammissibilità di alcuni ricorsi[51].

Per inciso, anche il formante "protocollare"[52] agita interrogativi di portata generale e, in particolare, quello sulle nuove fonti della procedura penale[53] e sulla evidente crisi in cui versa il codice di procedura penale come sua sorgente principale[54].

---

redazionali dei motivi di ricorso in materia civile e tributaria.

[49] Segnala il rischio di «una riduzione degli atti processuali in semplici moduli riconoscibili dai lettori ottici, con campi e spazi predeterminati, magari ispirati a un draconiano principio di sinteticità, che favoriscano la loro gestione automatizzata, per finire con i codici a barre già in uso presso la Corte europea dei diritti dell'uomo», L. Tavassi, *Il labirinto telematico per la trasmissione degli atti*, in ***dirittodidifesa.eu***, 8 gennaio 2025, 6.

[50] G. Romeo, *Note sparse a margine del protocollo d'intesa tra Corte suprema di cassazione e Consiglio nazionale forense sulle regole redazionali dei motivi di ricorso penale*, in ***dirittopenalecontemporaneo.it***, 12 gennaio 2016, § 3.

[51] Cfr. Cass. pen., sez. II, 19 giugno 2019, n. 42052, Pres. Cervadoro, Rel. Beltrani, non massimata sul punto. Per una sintetica scheda illustrativa di tale decisione, si veda, volendo A. Franceschini, *L'inammissibilità del ricorso per cassazione per inosservanza dei parametri "protocollari"*, in *Rassegna Penale*, 4, 2019, 104-106. La pronuncia richiama precedenti arresti di analogo tenore: Cass. pen., sez. II, 20 settembre 2018, n. 57737, CED 274471-01, secondo cui «è inammissibile, per genericità dei motivi, il ricorso per cassazione che renda le ragioni dell'impugnazione incomprensibili a causa della tecnica espositiva, caratterizzata da una pluralità di questioni eccentriche, tali da rendere l'illustrazione dei motivi ridondante e caotica (In motivazione, la Corte ha precisato che, al fine della valutazione dell'ammissibilità dei motivi di ricorso, va considerato quale strumento esplicativo del dato normativo dettato dall'art. 606 cod. proc. pen. il "Protocollo d'intesa tra Corte di cassazione e Consiglio Nazionale Forense sulle regole redazionali dei motivi di ricorso in materia penale». In senso conforme anche Cass. pen., sez. VI, 9 novembre 2017, n. 57224, CED 271725-01. Ma la tendenza sembra trasversale, abbracciando anche il comparto civile. Si veda, in tal senso, Cass. civ., sez. I, 24 aprile 2018, n. 10112, che sposa la stessa lettura con riferimento al Protocollo siglato il 17 dicembre 2015 tra Corte di cassazione e Consiglio nazionale forense in merito alle regole redazionali dei motivi di ricorso in materia civile e tributaria.

[52] Il tema della *soft-law* come fonte della procedura penale è diffusamente approfondito in F. Trapella, *Fondamenti e limiti della fonte protocollare nella gestione dell'emergenza*, in Id. (a cura di), *La rivoluzione digitale*, cit., 363 ss.

[53] Per qualche considerazione critica su questa deriva della disciplina, si veda, volendo, A. Franceschini, *Rito non partecipato in appello, scoria del periodo emergenziale tra efficientismo e delegificazione*, in *Diritto di Difesa*, 2, 2022, 384 ss., in cui parlo di «sistema multilivello e ramificato», individuando, al netto delle fonti sovranazionali e di quella costituzionale, almeno cinque livelli disciplinari: 1) legge ordinaria; 2) decreto ministeriale; 3) provvedimento direttoriale; 4) circolari capi uffici giudiziari; 5) protocolli d'intesa (nazionali o locali).

[54] In argomento si veda il recente M. Daniele, *La crisi del codice di procedura penale: un fenomeno irreversibile?*, in M. Donini – L. Garlati – M. N. Miletti – R. Orlandi (a cura di), *I cardini della modernità penale dai Codici Rocco alle stagioni dell'Italia Repubblicana*, Roma, 2024, 259 ss.

E poi c'è il tema della estensione degli atti. Non se ne parla, ma credo sia ormai incombente anche nel settore penale l'inoculazione di stringenti limiti dimensionali. Per il momento si può guardare al *volet civil*, e in particolare all'art. 46 disp. att. c.p.c.[55], che demanda al Ministro della giustizia la individuazione di tali paletti, attualmente stabiliti con il controverso decreto ministeriale n. 110 del 2023[56]. Il *Regolamento* – con la dichiarata finalità di assicurare la chiarezza e la sinteticità degli atti secondo quanto previsto dall'art. 121 c.p.c. – descrive una specifica articolazione da seguire per il confezionamento degli atti: un vero e proprio schema, che definisce le istruzioni per costruire una sorta di *template*; e indica, in migliaia, il limite massimo di caratteri a seconda della tipologia di atto processuale.
Insomma, ci si incammina nella chiara direzione della modellizzazione degli atti e dei provvedimenti[57].

3. Il processo penale telematico e la digitalizzazione degli atti

Iniziamo ora a mettere sul tappeto fattori di matrice tecnologica. E su questo terreno non possiamo non prendere le mosse dal macro-tema del processo penale telematico[58]. Esso si atteggia ormai ad autentico micro-e-

[55] Per un'analisi della disciplina dettata sull'asse degli artt. 121 c.p.c. e 46 disp. att. c.p.c., si veda F. De Giorgis, *Le disposizioni generali in materia di sinteticità e chiarezza degli atti processuali nella riforma Cartabia*, in *Judicium*, 16 giugno 2023.

[56] Cfr. decreto 7 agosto 2023 n. 110 del Ministero della giustizia, recante il *Regolamento per la definizione dei criteri di redazione, dei limiti e degli schemi informatici degli atti giudiziari con la strutturazione dei campi necessari per l'inserimento delle informazioni nei registri del processo, ai sensi dell'articolo 46 delle disposizioni per l'attuazione del codice di procedura civile*. In argomento, anche per un'accurata analisi dei profili linguistici, si veda I. Benevieri, *La parola (in)difesa*, Torino, 2024, 19 ss.

[57] È questa l'espressione adoperata da B. Galgani, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Padova, 2022, 378-379, la quale, nel ragionare sulla «rinnovata "morfologia" degli atti processuali» tracciata dalla legge n. 134 del 2021 (delega Riforma Cartabia) e cogliendo «una suggestione proveniente dal parallelo percorso di riforma del rito civile», ipotizza lo sviluppo di «una sorta di "schema informatico dell'atto"» e paventa «l'opportunità di implementare un modello di atto secondo criteri redazionali predefiniti, sì da rendere davvero virtuoso il connubio tra impiego delle tecnologie informatiche ed esercizio della funzione giurisdizionale». È evidente la differente prospettiva rispetto alle osservazioni critiche sviluppate in questo mio lavoro.

[58] Per lo studio del tema e per ulteriori riferimenti bibliografici, si veda anzitutto B. Galgani, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, cit.; F. Trapella (a cura di), *La rivoluzione digitale. Processo penale telematico e processo penale da remoto*, Roma, 2021. Tra i contributi in rivista, si vedano, tra i più ampi e approfonditi, B. Galgani, *Il processo penale in "ambiente" digitale: ragioni e (ragionevoli) speranze*, in *questionegiustizia.it*, 17 gennaio 2022, ora anche in *Questione giustizia*, 4, 2021, 181 ss.; Ead., *Digitalizzazione e processo penale: riflessioni sul dover essere di una nuova "cartografia"*, in *disCrimen*, 3 giugno 2021; Ead., *Innovazione tecnologica e tradizione personalistica. Dalla partecipazione "a distanza" alle cc.dd. "Metaverse Courtrooms"?*, in *archiviopenale.it*, 7 luglio 2023; L. Giordano, *La giurisprudenza e la* digital transformation *del processo penale*, in *sistemapenale,it*, 8 gennaio 2024; id., *La giurisprudenza di legittimità sulle prime applicazioni del processo penale telematico*, in *sistemapenale.it*, 21 maggio 2021; L. Tavassi, *Formalismi giurisprudenziali e forme tecnologiche nel giusto processo digitale*, in *archiviopenale.it*, 1 marzo 2024; Ead., *Il labirinto telematico per la*

cosistema[59], con regole e princìpi autonomi. Sembra così avere assunto le sembianze di una dimensione parallela alla procedura, per certi versi completamente avulsa da questa, caratterizzato, com'è, da una sua filosofia e da una sua grammatica.

Qui occorre anzitutto denunciare un profilo estremamente critico, che rischia di far deragliare il sistema processuale e che, però, sembra essere sfuggito, almeno finora, ai radar degli studiosi. La disciplina trova il suo fulcro normativo negli artt. 111-*bis* e 111-*ter* c.p.p., ma queste disposizioni rappresentano solo il punto di partenza: esse evocano, sul piano disciplinare, una non meglio definita «normativa, anche regolamentare». Proprio questa scelta di tecnica normativa produce un autentico strappo alla riserva di legge e una slabbratura nella maglia delle fonti della procedura penale.

La verità è che il legislatore ordinario, obliterando del tutto il principio di legalità processuale sancito dall'art. 111, c. I, Cost.[60], già dai tempi della disciplina emergenziale nel periodo Covid, ha iniziato a compiere la scelta di delegare a fonti sub-primarie una significativa porzione della regolamentazione della materia processuale[61]. È una criticità di cui, prima o poi, ci si dovrà fare carico se si vuole conservare centralità al codice.

Sul piano empirico la digitalizzazione comporta l'utilizzo di documenti costruiti in un formato del tutto "nuovo", radicalmente diverso da quello

---

trasmissione degli atti, in *dirittodidifesa.eu*, 8 gennaio 2025; F. Trapella, *La rivoluzione digitale alla prova della riforma*, in *archiviopenale.it*, 15 dicembre 2022. Molto interessante, per un inquadramento generale del fenomeno della digitalizzazione, l'autorevole intervento di P. Tonini, *Le nuove tecnologie e la riforma Cartabia*, in *Diritto penale e processo*, 3, 2022, 293 ss., il quale segnala l'inadeguatezza delle «vecchie categorie concettuali della prova che risalgono a più di cento anni fa e che valevano quando gli atti scritti a mano erano gli unici documenti utilizzati nel processo».

[59] B. Galgani, *Il processo penale in "ambiente" digitale: ragioni e (ragionevoli) speranze*, cit., 181, parla di «ecosistema giustizia penale dalla peculiare angolazione dell'"ambiente" digitale».

[60] Sul tema della legalità processuale la letteratura non è molto vasta, e questa mancanza di ricchezza è purtroppo specchio di una scarsa attenzione riservata dalla dottrina all'argomento. Possiamo però contare su alcuni contributi di altissimo pregio: F. R Dinacci, *I tortuosi percorsi della legalità mancata: dalla flessibilizzazione del "tipo" alla libertà delle forme probatorie e alla imprevedibilità della decisione*, in *archiviopenale.it*, 3 maggio 2022; id., *Legalità processuale e nomofilachia tra limiti ermeneutici e diritto giurisprudenziale*, in *archiviopenale.it*, 19 novembre 2019; D. Negri, *Il processo penale italiano a venticinque anni dalla riforma del codice*, in *Criminalia*, 2014, 219 ss. (spec. 228-229); Id., *Delle procedure criminali: parte di legislazione così principale e così trascurata*, in *Cassazione Penale,* 2014, 3946 ss.; Id., *Dallo scandalo della vicenda Taricco risorge il principio di legalità processuale*, in A. Bernardi – C. Cupelli (a cura di), *Il caso Taricco e il dialogo tra le Corti. L'ordinanza 24/2017 della Corte costituzionale*, Napoli, 2017, 297 ss.; Id., *Splendori e miserie della legalità processuale. Genealogie culturali,* èthos *delle fonti, dialettica tra le Corti*, in *Archivio Penale,* 2, 2017, 421 ss.; O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *Diritto penale contemporaneo*, 3, 2013, 4 ss.; Id., *Il crepuscolo della legalità processuale al tempo del giusto processo*, in *Studi senesi*, CXXIX, 2017, 112 ss.; S. Lorusso, *Interpretazione, legalità processuale e convincimento del giudice*, in *penalecontemporaneo.it*, 10 giugno 2015; C. Valentini, *Contro l'invenzione del diritto: piccolo elogio della legalità processuale, ricordando Piero Calamandrei*, in *archiviopenale.it*, 2, 2018.

[61] Per una denuncia di questa tendenza, si veda, volendo, A. Franceschini, *Ancora per la legalità processuale, contro il fenomeno della delegificazione*, in *Rassegna Penale*, 1, 2020, 9 ss. Il tema, con specifico riferimento alla legislazione emergenziale, è affrontato anche da G. Sambuco, *La normativa di emergenza alla prova della legalità processuale*, in F. Trapella (a cura di), *La rivoluzione digitale*, cit., 339 ss.

tradizionale (quello che oggi identifichiamo con il termine "analogico")[62]. Si tratta di atti generati con l'utilizzo degli elaboratori e che devono rispondere a specifiche caratteristiche tecniche affinché possano essere processati sul portale del deposito degli atti penali (PDP)[63].
Ma questa trasformazione di paradigma favorisce anche la possibilità, in un futuro prossimo, che gli atti siano lavorati da *software* progettati per svolgere ulteriori e ben specifiche funzioni. Non è difficile immaginare, tra queste abilità di prossima realizzazione, il *detecting* di situazioni di carenza dei requisiti di ammissibilità degli atti impugnatori, la comparazione con il testo del provvedimento attaccato e la verifica di conformità ai princìpi consolidati nella giurisprudenza di legittimità.
Anche qui l'aspetto nevralgico è rappresentato dell'imbrigliamento in schemi omologanti; e dunque ritorna il discorso sulla modellizzazione degli atti.

4. Le risorse tecnologiche al servizio del giudice

La galassia delle transizioni digitali – con l'impetuosa evoluzione compiuta negli ultimi anni dalla tecnologia informatica e il suo progressivo impiego in ambito giudiziario – è molto variegata; il processo penale telematico ne rappresenta solo un tassello.
Per ampliare lo sguardo si pensi, tra le tante cose, alle funzionalità via via implementate nella c.d. *consolle* del magistrato[64]: nel settore civile già da tempo essa è munita di un redattore atti, mentre in ambiente penale alla *consolle* è collegato un modulo, denominato *Atti e Documenti*, che ha, tra le sue funzioni, anche quella di consentire la redazione di documenti[65].

[62] Sul ruolo rivestito dalla scelta di adottare, nella realizzazione di una pratica istituzionale, una «specifica tecnica documentaria» anche nel senso di condizionarne le modalità evolutive, si veda M. Q. Silvi, *Tecniche documentarie ed evoluzioni istituzionali. Una prospettiva artefattuale*, in *Rivista di filosofia del diritto*, 2, 2024, 385 ss.

[63] In tal senso si veda B. Galgani, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Cedam, 2022, 380, la quale afferma: «nessuno può mettere seriamente in dubbio come un linguaggio vieppiù lineare e intelligibile da una parte, e una struttura semplificata e tendenzialmente standardizzata del provvedimento dall'altra, contribuirebbero non soltanto all'elevazione della qualità degli atti in genere, ma consentirebbero altresì una migliore "processazione informatica" dei medesimi, con positivi riverberi di non poco momento in tema – tanto per fare solo alcuni esempi -di funzionalità dei sistemi di OCR (*Optical Character Recognition*) e di ricerca delle banche dati».

[64] Parlano dell'applicativo Consolle del Magistrato A. Bigiarini, *Il punto di vista del pubblico ministero*, in F. Trapella (a cura di), *La rivoluzione digitale. Processo penale telematico e processo penale da remoto*, Roma, 2021, 65, e S. Zen, *Il punto di vista del giudice*, *ibid*., 83-84.

[65] S. Zen, *Il punto di vista del giudice*, cit., 84, la quale spiega che «il sottosistema Atti e Documenti è una funzionalità del SICP che permette di redigere alcuni atti e provvedimenti in maniera dinamica attingendo i dati strutturati del fascicolo processuale tra quelli presenti sul database distrettuale del sistema. Al momento è stata sviluppata la versione 2.0 che non si presenta solo come un redattore di documenti, ma che può svolgere ulteriori funzioni come la possibilità di firmare digitalmente alcuni atti e depositarli a fascicolo». Per approfondire le funzionalità di questi strumenti, si possono consultare le schede e i documenti ad essi dedicati sul sito istituzionale del Consiglio

Per dare il senso del livello di sviluppo cui sono giunti gli strumenti già utilizzati in ambito giudiziario, è di estremo interesse la lettura della *Relazione sullo stato della giustizia telematica 2024* del Consiglio superiore della magistratura[66], dalla quale, tra le altre cose, si rileva l'operatività, a corredo della *Banca Dati di Merito riservata*[67], di due applicativi basati su tecniche di intelligenza artificiale generativa: un *AI Abstracts*, «capace di generare in tempo reale una sintesi dei provvedimenti ad uso degli utenti», e un *Assistente virtuale Chat Bot*, «in grado di fornire informazioni e risposte alle domande in linguaggio naturale»[68]. Per inciso, in una piega della *Relazione* non si fa mistero di uno dei gravi rischi che una tecnologia del genere reca con sé, in quanto essa «potrebbe anche favorire effetti potenzialmente negativi, facilitando, per mero produttivismo, la passiva ricezione di apparati motivazionali, con conseguente conformismo giudiziario ed impoverimento della stessa qualità della giurisdizione»[69].

Ma il quadro è davvero ampio e frastagliato, difficile tracciare un quadro ricognitivo completo. Al di là degli strumenti già introdotti, si devono prendere in considerazione anche i progetti in via di sviluppo presso alcuni uffici giudiziari, molti dei quali sono incentrati sull'evoluzione dei processi di elaborazione del linguaggio naturale, non solo per potenziare e raffinare la ricerca all'interno delle banche dati, ma anche per implementare, tra le altre, funzionalità di *argument mining* e *document building*[70]. Progetti che a breve termine potrebbero offrire i loro frutti e popolare di nuove figure il già ricco scenario tecnologico.

superiore della magistratura, rispettivamente alle voci *Consolle e Atti & documenti*, per il settore penale, e *Consolle del magistrato*, per quello civile.

66 CSM, *Relazione sullo stato della giustizia telematica 2024* (delibera 24 luglio 2024).

67 Si tratta della banca dati massiva nazionale di giurisprudenza di merito, aperta il 20 novembre 2023 dal Dipartimento per la transizione digitale. Sul tema, di grande attualità, delle banche dati di merito, si vedano, volendo A. Franceschini, *Banche dati di merito: circolarità evolutiva o conformismo giudiziario?*, in *archiviopenale.it*, 15 marzo 2024; C. Perago – M. Orlando – A. Albanese, *Banca dati di merito tra automatismo decisionale e umanità della decisione*, in *Judicium*, 15 maggio 2024; M. Ciccarelli, *Ufficio per il processo e banche dati di giurisprudenza*, in C. Castelli (a cura di), *L'ufficio per il processo*, Pisa, 2024, 93 ss. Per una panoramica sullo stato dell'arte dei vari progetti si veda CSM, *Relazione sullo stato della giustizia telematica 2024* (delibera 24 luglio 2024), 52 ss.

68 Cfr. CSM, delibera 24 luglio 2024, *Relazione sullo stato della Giustizia Telematica 2024*, cit., 54.

69 *Ibid.*

70 Si veda l'*Accordo quadro* stipulato il 29 settembre 2021 tra il CED della Cassazione e l'IUSS di Pavia, volto a perseguire i seguenti obiettivi (art. 3): «a) predizione dell'esito dei processi decisionali giudiziari, amministrativi e politici (*prediction*), b) estrazione di argomenti giuridici dal corpus delle sentenze e decisioni di Italgiure (*argument mining*), c) creazione automatica di massime (*summarization*); d) strumenti di creazione automatica di documenti (*document builder*), nonché altre possibilità di valorizzazione del patrimonio documentario di Italgiure».

5. L'intelligenza artificiale generativa e l'esplosione del *Natural Language Processing*

Uno snodo imprescindibile, ai fini delle nostre riflessioni, consiste nel puntare il fuoco sull'intelligenza artificiale generativa[71]. Che si tratti di tecnologia già in uso nel contesto giudiziario lo si desume facilmente dal documento licenziato dal *Gruppo di lavoro sulla Cybergiustizia e intelligenza artificiale* della Commissione europea per l'efficienza della giustizia (Cepej)[72], nel quale, oltre a mettere in fila i suoi possibili impieghi in tale settore[73], si evidenziano anche i (non trascurabili) rischi[74].
D'altra parte già si annoverano alcuni esperimenti "artigianali" sul funzionamento dei *chatbot* in campo giuridico[75], in particolare di *ChatGPT* di

[71] In argomento si veda il recente M. Flora – L. Maggi, *Intelligenza artificiale generativa. Opportunità e sfide legali*, Pisa, 2024; J. Kaplan, *Generative A.I. Conoscere, capire, usare l'intelligenza artificiale generativa*, Roma, 2024. Sul tema dell'utilizzo dell'intelligenza artificiale generativa in ambito giuridico, si vedano L. Romanò, *La responsabilità penale al tempo di ChatGPT: prospettive de iure condendo in tema di gestione del rischio da intelligenza artificiale generativa*, in *sistemapenale.it*, 17 maggio 2023; F. Contini, *Unboxing Generative AI for the Legal Professions: Functions, Impacts and Governance*, in *International Journal for Court Administration*, Vol. 15, n. 2, 20 agosto 2024. Con specifico riferimento al processo penale, si vedano A. Craviotto – L. Vitali – L. Egitto – C. Canepa, *Per un uso responsabile dell'IA nel processo (penale)*, in *giurisprudenzapenale.it*, 1 marzo 2024, 5 ss., e R.E. Kostoris, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Cassazione Penale*, 5, 2024, 1642 ss. Molto utile l'approfondimento descrittivo che si rinviene in G. Lo Sapio, *L'Intelligenza Artificiale Generativa nella Giustizia Amministrativa: scenari, rischi e opportunità*, in *giustizia-amministrativa.it*, 3 febbraio 2025, spec. § 1 e nel *Glossario* posto in coda al contributo.

[72] Cepej, *Use of Generative Artificial Intelligence (AI) by judicial professionals in a work-related context*, 12 febbraio 2024. Per una prima lettura del documento, si veda F. De Stefano, *Le iniziative del Consiglio d'Europa in materia di intelligenza artificiale generativa nella giustizia: un aggiornamento*, in *giustiziainsieme.it*, 5 marzo 2024.

[73] Secondo il documento del Cepej (*sub* par. B), l'intelligenza artificiale generativa garantisce buoni risultati con riferimento alle seguenti attività: 1) traduzione di testi; 2) creazione di testi coerenti (ma non necessariamente veri), immagini e suoni; 3) riassunto automatico di testi; 4) analisi semantica e individuazione delle opinioni; 5) estrazione di testo (c.d. *text mining*, ossia la trasformazione di grandi quantità di testo non strutturato in dati significativi e strutturati) e accesso ai contenuti.

[74] I rischi classificati (*sub* par. C) sono i seguenti: 1) *potential production of factually inaccurate information (false answer, "hallucinations" and bias)*; 2) *possible disclosure of sensitive data and risk condifentiality*; 3) *lack of references for the information provided and potential violation of intellectual property and copyright*; 4) *limited capability of providing the same answer to an identical question*; 5) *potential replication of outputs*; 6) *varying stability and reliability of Generative AI models for critical and time-sensitive processes*; 7) *exaggeration of cognitive biases*. Si tratta, dunque, di: 1) potenziale produzione di informazioni di fatto inesatte (risposte false, allucinazioni e pregiudizi); 2) rischio di rivelazione di dati sensibili o riservati; 3) mancanza dei riferimenti dei dati forniti e di una possibile violazione del diritto di autore o di proprietà intellettuale; 4) limitata capacità di fornire la stessa risposta alla medesima domanda; 5) potenziale replicazione dei risultati; 6) variabilità, in termini di stabilità e affidabilità, dei modelli di intelligenza artificiale generativa per quanto riguarda i processi critici e sensibili al fattore temporale; 7) amplificazione dei pregiudizi cognitivi (traduzione a cura dell'Autore).

[75] Sul tema si veda il recentissimo R. Gaeta, *L'impiego dei* chatbot *nelle attività di* law enforcement, in V. Maffeo – A. Romano – P. Troncone, *Intelligenza artificiale e processo*, Torino, 2024, 89 ss.

OpenAI[76]. I risultati sembrano tutti piuttosto deludenti dal punto di vista della qualità dei risultati[77]. Ma la scena attuale è già affollata da prodotti, realizzati da altri *competitors*, che promettono migliori capacità ed efficienza: ci si riferisce in particolare a *Bard* (*Gemini*) di *Google*, *Claude* di *Anthropic*[78] e *DeepSeek-V3* di *High-Flayer Quant*.

In ogni caso occorre ricordare che, per quanto sorprendentemente performativo possa sembrare la loro resa dal punto di vista della prosa generata – sotto il profilo grammaticale, contenutistico e stilistico – l'intelligenza artificiale generativa e, in particolare, i *chatbot* nascono con un compito "semplice", molto lontano dalla complessità della giustizia umana: prevedere la parola successiva in una sequenza di parole[79].

6. La futuribile automazione delle decisioni in materia di inammissibilità delle impugnazioni

Digitalizzazione, modellizzazione degli atti, applicativi di intelligenza artificiale generativa che impiegano tecniche di linguaggio naturale, formalismo tecnologico. In un contesto del genere non è difficile preconizzare la costruzione, in un orizzonte temporale piuttosto breve, di procedure automatizzate[80] per il vaglio di ammissibilità delle impugnazioni.

Non solo per setacciare le impugnazioni e scremarle da quelle inammissibili, per cause "forti", macroscopiche (tardività, mancanza di legittimazione, etc.), il che potrebbe tutto sommato anche ritenersi accettabile; ma anche per ipotesi che richiedono un vaglio più penetrante: il riferimento corre alla già *ex se* discutibile aspecificità estrinseca dell'appello o del ricorso.

E non si può escludere che anche la così critica ipotesi di inammissibilità per manifesta infondatezza possa essere vagliata, almeno in prima battuta, da un algoritmo, soprattutto per quanto riguarda le questioni di natura giuridica. Il giudice-robot potrebbe riconoscere nei motivi spiegati dal ricorrente una tesi ermeneutica contraria ai consolidati arresti delle Sezioni unite.

La temibile prospettiva qui adombrata rischia di rivelarsi meno remota di

---

[76] M. Coeckelbergh – D. J. Gunkel, *ChatGPT: deconstructing the debate and moving it forward*, in *AI & Society*, 2024, 2221-2231. Molto interessante la ricostruzione evolutiva dalla prima versione di GPT fino a quella GPT-3 che si ritrova in N. Cristianini, Machina sapiens. *L'algoritmo che ci ha rubato il segreto della conoscenza*, in *Psiche*, 2, 2024, 527 ss.

[77] D. Amidani, *ChatGPT bocciato all'esame di diritto processuale penale. Attendibilità e trasparenza dei sistemi di intelligenza artificiale alla luce di un esperimento*, in *sistemapenale.it*, 3 ottobre 2024; G. Carlizzi – G. Tuzet (intervista a), C. Conti (condotta da), *Il ragionamento probatorio nel processo penale: logica e probabilità nell'era dell'intelligenza artificiale*, in *Diritto penale e processo*, 12, 2024, 1631 ss., in particolare *Appendice 1) Esperimento con chat-GPT* (svolto da Gaetano Carlizzi nel mese di agosto 2024).

[78] Ne parla M. Montan, *Nella mente della macchina*, su *Il Foglio*, 16 dicembre 2024.

[79] N. Cristianini, Machina sapiens. *L'algoritmo che ci ha rubato il segreto della conoscenza*, in *Psiche*, 2, 2024, 528, 536.

[80] Si sofferma diffusamente sulle decisioni automatizzate, anche approfondendo profili di compatibilità con la legislazione vigente, L. Pressacco, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in *BioLaw Journal*, 4, 2022, 503 ss., spec. § 3.

quanto si potrebbe immaginare se solo si pensi all'approccio adottato dalla giurisdizione di legittimità, dove i ricorsi – non da oggi – vengono ormai sottoposti ad una valutazione ponderale per classificarli in base alla loro complessità, con l'attribuzione di uno specifico coefficiente numerico[81].
Insomma, per avere una lucida visione di quali siano le reali prospettive future, è necessario comporre un mosaico con tutti i tasselli che mostrano interferenza, anche quelli non immediatamente riconducibili ad applicazioni di intelligenza artificiale.

7. La "preferenza per l'umano"

Non è questa la sede per proporre considerazioni di carattere generale sull'intelligenza artificiale[82], né tanto meno per avventurarsi in impervi tentativi definitori. Aspetti per i quali non posso che rinviare alla ormai sterminata letteratura disponibile, proponendo semmai una selezione orientata dal taglio problematico che contraddistingue il mio approccio al tema[83].
In ogni caso, oggi, in un'ottica normativa, non può prescindersi dalla de-

[81] CSM, delibera 5 luglio 2017, *Linee guida in materia di esame preliminare delle impugnazioni e modalità stilistiche di redazione dei provvedimenti*; Id., delibera 22 novembre 2017, *Esame preliminare delle impugnazioni e tecniche di redazione degli atti del giudizio d'appello: cooperazione tra il Consiglio superiore della magistratura ed il Consiglio nazionale forense per l'attuazione pratica delle linee guida*; Id., delibera 20 giugno 2018, *Prima attuazione delle linee guida in tema di esame preliminare delle impugnazioni e modalità stilistiche di redazione dei provvedimenti*. In questi documenti si parla dell'attribuzione di «un coefficiente ponderale di complessità, a sua volta funzionale alla razionale formazione dei ruoli, all'equa distribuzione degli affari ai singoli magistrati, al rispetto di carichi esigibili di lavoro che consentano di coniugare il dato quantitativo con quello qualitativo» e di «diversa complessità degli affari in base a criteri di misurazione ponderale alla stregua di parametri predeterminati». Questo aspetto è segnalato e stigmatizzato da O. Mazza, *Distopia del processo artificiale*, in *archiviopenale.it*., 7 gennaio 2025, 19.

[82] P. Benanti, *Le macchine sapienti. Intelligenze artificiali e decisioni umane*, Bologna, 2018; S. Natale, *Macchine ingannevoli. Comunicazione, tecnologia, intelligenza artificiale*, Torino, 2022; N. Cristianini, *La scorciatoia. Come le macchine sono diventate intelligenti senza pensare in modo umano*, Bologna, 2023; P. Garzia, *Non sono un'intelligenza artificiale*, in *Mind*, 2024, maggio, 24 ss.; E.J. Larson, *Il mito dell'intelligenza artificiale. Perché i computer non possono pensare come noi*, Milano, 2022; T. Poggio – M. Magrini, *Cervelli menti algoritmi. I misteri dell'intelligenza naturale, gli enigmi di quella artificiale*, Segrate, 2023.

[83] Molto efficace la definizione di F. Amigoni – V. Schiaffonati – M. Somalvico, voce *Intelligenza artificiale*, in *Enciclopedia della Scienza e Tecnica*, Vol. V, *Tecnologia*, Roma, 2008, 323, la definiscono: «quella disciplina, appartenente all'informatica, che studia i fondamenti teorici, le metodologie e le tecniche che consentono di progettare sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana». In ambito processual-penalistico, di recente, L. Marafioti, *Intelligenza artificiale, giudizio penale e garanzie processuali*, in *Indice Penale*, 3, 2023, 3, ricorda una delle definizioni più recenti, sviluppata dal Gruppo di esperti istituito dalla Commissione europea nel 2018 e licenziata nel documento intitolato *Una definizione di IA: principali capacità e discipline scientifiche*, secondo cui sarebbe riconducibile alla nozione di intelligenza artificiale ogni «sistema progettato dall'uomo che agisce attraverso l'acquisizione e l'interpretazione dei dati raccolti, elaborando le informazioni derivate da questi ultimi al fine di decidere le migliori azioni da intraprendere per raggiungere un certo obiettivo».

finizione accolta nell'*AI Act*[84], secondo cui per sistema di intelligenza artificiale 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»[85].

Può essere invece proficuo indugiare su di un aspetto tendenzialmente trascurato nelle riflessioni intorno all'impiego degli algoritmi in ambito giudiziario: quale significato attribuiamo al termine intelligenza quando discorriamo di quella "artificiale"?

Molti studiosi di discipline extra-giuridiche evidenziano come sia «fuorviante» il confronto, il quale implica «l'idea […] di riprodurre con le macchine (artificialmente) l'intelligenza umana»[86]. Su di una circostanza potremmo però trovarci d'accordo: «l'intelligenza artificiale non pensa come noi»[87]. E questo perché, al fondo, «i sistemi di intelligenza artificiale non sono autocoscienti» e perché, riflettendo in particolare sulla tecnologia che viene in gioco nel tema che ci occupa, «un modello linguistico di grandi dimensioni non possiede un modello di conoscenza»[88].

Non si tratta di una sterile considerazione di natura teorica. Tutt'altro, essa risulta strettamente funzionale alla riflessione critica che voglio proporre sul rischio di introdurre, sia pure per decisioni apparentemente innocue, processi automatizzati.

E in questa prospettiva diviene allora essenziale un passaggio a proposito del modello c.d. collaborativo che gli entusiasti[89] cercano di promuovere,

---

[84] Si tratta, come noto, del *Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 12 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale*, pubblicato sulla GU dell'UE del 12 luglio 2024. Per un approfondimento della parte del *Regolamento* relativa all'ambito della giustizia penale, si veda il recentissimo contributo di S. Quattrocolo, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in *dirittodidifesa.eu*, 16 gennaio 2025, ora anche in *Diritto di Difesa*, 3-4, 2023, 703 ss.

[85] Si tratta di un sostanziale recepimento della definizione elaborata in seno al Consiglio dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), con la Raccomandazione del 3 maggio 2024 sull'intelligenza artificiale, di aggiornamento della precedente adottata nel 2019: «un sistema basato su una macchina che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. I diversi sistemi di AI variano nei loro livelli di autonomia e adattabilità dopo l'implementazione».

[86] E. Esposito, *L'intelligenza degli algoritmi*, in *Psiche*, 2, 2024, 538.

[87] È l'icastico titolo del recente contributo D. Weinberger, *L'intelligenza artificiale non pensa come noi*, in *Psiche*, 2, 2024, 567 ss. L'Autore, prendendo le mosse dall'assunto secondo cui «una rappresentazione formale del pensiero non è sufficiente a generare coscienza», afferma: «queste macchine non sanno nulla. Ciò, a sua volta è una conseguenza del fatto che non pensano come noi».

[88] D. Weinberger, *L'intelligenza artificiale non pensa come noi*, cit., rispettivamente, 569 e 574.

[89] In A. Franceschini, *L'accertamento dei fatti nel giudizio penale, tra le lusinghe dell'intelligenza artificiale e gli approdi (ancora inesplorati) di saperi extra-giuridici* (*paper* ammesso al convegno *L'informazione ed il diritto*, Napoli, 29-30-31 maggio 2024 (PRIN 2022, Prova e Processo Informatizzato e presentato nel panel Il futuro del processo penale tra tecnologie digitali e intelligenza artificiale), ho classificato i possibili approcci all'impiego dell'intelligenza artificiale in tre gruppi: entusiasti, reazionari, cauti. Si definisce «guardingo», Carlizzi in

edificato sul tranquillizzante presupposto – imposto da istanze assiologicamente dure – che si possa preservare, in ogni caso, la centralità dell'uomo. L'obiezione che si muove agli scettici, preoccupati che si smarrisca una visione antropocentrica della giustizia, suona più o meno così: il modello che si immagina non è di tipo sostitutivo, ma meramente ancillare, e alla fine di qualsiasi processo decisionale ci sarà sempre il giudice-uomo a supervisionare il responso dell'algoritmo. È il concetto compendiato nella "fortunata" formula del *controllo umano significativo*.

Ebbene, a me pare che quella del *controllo umano*, soprattutto in certi ambiti, sia null'altro che un'ingenua illusione[90]. Conclusione cui si giunge non necessariamente immaginando scenari distopici.

In primo luogo l'astratta possibilità di un controllo effettivo presuppone la esatta conoscibilità del funzionamento dell'algoritmo. Già questa circostanza pare, di fatto, irrealizzabile a causa di almeno due fattori, piuttosto scontati. Il primo risiede nella c.d. opacità degli algoritmi[91], ossia nella loro mancanza di trasparenza, che «rende difficile comprendere i calcoli alla base delle conclusioni formulate dai sistemi, compromettendo così la loro *spiegabilità*»[92]. Si tratta di una connotazione oggettivamente insuperabile[93], specie con i sistemi che adoperano tecniche di *deep learning*. Il secondo nella necessità che l'operatore umano sia dotato di conoscenze iper-specialistiche di natura tecnologica in aggiunta a quelle del proprio settore professionale (medico, giudiziario, etc.).

E poi non può non pesare, in modo determinante, l'aspetto cognitivo. Pensando all'atteggiamento dell'uomo nei confronti dell'algoritmo, possiamo isolare due posizioni estreme[94]: l'eccessiva fiducia in esso, stimato infallibile (*automation bias*)[95], e, all'opposto, la tendenziale sfiducia nel suo

---

G. Carlizzi – G. Tuzet (intervista a), C. Conti (condotta da), *Il ragionamento probatorio nel processo penale: logica e probabilità nell'era dell'intelligenza artificiale*, in *Diritto penale e processo*, 12, 2024, 1631. Distingue tra approccio entusiastico e approccio scettico J. Nieva-Fenoll, *Intelligenza artificiale e processo*, Torino, 2019, 1.

[90] Questa è l'espressione che ho adoperato in A. Franceschini, *L'accertamento dei fatti nel giudizio penale, tra le lusinghe dell'intelligenza artificiale e gli approdi (ancora inesplorati) di saperi extra-giuridici*, cit.

[91] Affronta il tema S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 3, 2020, 130 ss.

[92] G. Romeo, D. Conti, *Oltre l'automazione: riconfigurare il binomio Uomo-Intelligenza Artificiale*, in *Sistemi intelligenti*, 3, 2024, 642. Su questi profili si veda anche G. Barone, *Intelligenza artificiale e processo penale: la linea dura del Parlamento europeo. Considerazioni a marine della Risoluzione del Parlamento europeo del 6 ottobre 2021*, in *Cassazione Penale*, 3, 2022, 1187 ss. Stigmatizza «l'impossibilità […] di poter effettivamente comprendere il funzionamento dell'algoritmo» e le ricadute negative sul principio di parità, S. Quattrocolo, *Equità del processo penale e* automated evidence *alla luce della convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 1, 2019, 107 ss., spec. 120.

[93] D. Weinberger, *L'intelligenza artificiale non pensa come noi*, cit., 572, afferma che «attualmente […] l'inspiegabilità è un dato di fatto in molti utilizzi dell'apprendimento automatico». Propone, in prospettiva futura, alcuni spunti per superare questa criticità M. Menna, *Intelligenza artificiale e controllo contenutistico delle "forme" di produzione dei suoi* outputs *conoscitivi*, in *archiviopenale.it*, 10 giugno 2020.

[94] L. Introzzi – P. Cherubini – C. Reverberi, *L'interazione umano-IA come cooperazione. Verso una teoria della mente artificiale*, in *Sistemi intelligenti*, 2, 2024, 503.

[95] L. Introzzi – P. Cherubini – C. Reverberi, *L'interazione umano-IA come cooperazione. Verso*

impiego a supporto delle decisioni e delle azioni umane (*algorithm aversion*). C'è però chi declina questo secondo atteggiamento, certamente destinato alla frustrazione, in termini di più equilibrata "preferenza per l'umano", intesa come preferenza per informazioni e decisioni generate da esseri umani[96], che potrebbe manifestarsi anzitutto: 1) in domini rilevanti per l'identità umana, in cui i criteri di valutazione sono più ambigui e difficili da oggettivare (e certamente la giustizia si iscrive in questa categoria); 2) in *compiti soggettivi* in cui, diversamente da *compiti oggettivi*, ci sono più risposte plausibili invece di una sola risposta corretta.

Non credo ci sia nulla di retrogrado o retrotopico[97] nel predicare una scelta ispirata a tale approccio, che difenda il nucleo della funzione giurisdizionale da contaminazioni artificiali, relegando strumenti algoritmici alla gestione di aspetti organizzativi dell'amministrazione della giustizia.

Sono convinto che, purtroppo, il sentimento prevalente, soprattutto in un contesto che pretende sempre più efficienza, sarà quello settato sul registro di una estrema apertura e di una grande fiducia: perché una scelta del genere conviene; perché questa scelta genera un grande beneficio pure in termini di agio. E a tale proposito non dimentichiamo che i giudici, anche quelli supremi, sono pur sempre uomini[98], con tutti i vizi collegati a questa condizione, compresa la pigrizia.

Riprendendo ora la precisazione con cui abbiamo aperto il paragrafo, il portato di una implementazione di sistemi di intelligenza artificiale in processi decisionali nell'universo giudiziario significherebbe, in ultima analisi, affidarsi a qualcosa di "diverso" dall'intelligenza umana e, quindi, accettare l'idea di un radicale cambiamento di paradigma, incentrato sulla sostan-

---

una teoria della mente artificiale, cit., 503, che lo definiscono come «una forma di compiacenza acritica». Sul tema si vedano anche C.D. Wickens – F. Giannotti – B.A. Clegg – AZ. Vieane – A.L. Sebok, *Complacency and Automation Bias in the Use of Imperfection Automation*, in *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 2015, 728 ss. G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *archiviopenale.it*, 21 novembre 2019, 8, evoca il rischio connesso «ad un intenso e diffuso ricorso all'intelligenza artificiale […] rappresentato dall'*automation bias*, ossia dalla fiducia che gli esseri umani tendono a riporre, in modo inconscio e irrazionale, nelle tecnologie, ritenute oggettive e meritevoli di fiducia per il solo fatto di essere… tecnologie». Da ultimo, denuncia il rischio di appiattimento «sulla soluzione suggerita dal software», provando, nel contempo, ad individuare possibili strumenti di contenimento dello stesso, G. Gallone, *Riserva di umanità, intelligenza artificiale e funzione giurisdizionale alla luce dell'IA Act. Considerazioni (e qualche proposta) attorno al processo amministrativo che verrà*, in *Judicium*, 7 novembre 2024, § 4.

[96] L. Introzzi – P. Cherubini – C. Reverberi, *L'interazione umano-IA come cooperazione*, cit., 503, i quali spiegano che, in questo tipo di processo, «l'operatore umano tendenzialmente mostra poca fiducia nei confronti delle decisioni del sistema di supporto, anche se esse sono affidabili».

[97] Z. Baumann, *Retrotopia*, Roma-Bari, 2017.

[98] Lo ricordava, a metà del secolo scorso, P. Calamandrei, *Anche i giudici sono uomini*, pagine scritte per prefazione alla traduzione in tedesco del suo *Elogio dei giudici scritto da un avvocato* e poi pubblicate su *Il Ponte*, 10, 1956, 1683 ss. Il testo è ora disponibile in P. Calamandrei, *Opere giuridiche*, vol. II, Roma, 2019, 478 ss. Il tema presenta notevoli profili tecnici, esplorati soprattutto con l'ausilio delle scienze cognitive. Per un approccio a questi argomenti, è molto utile G. Cevolani-V. Crupi, *Come ragionano i giudici: razionalità, euristiche e illusioni cognitive*, in *Criminalia*, 2017, 181 ss. Per approfondire, è centrale A. Forza – G. Menegon – R. Rumiati, *Il giudice emotivo. La decisione tra ragione ed emozione*, Bologna, 2017.

ziale disumanizzazione della giustizia penale[99]. Metamorfosi che solleverebbe più che legittimi dubbi di compatibilità costituzionale, tenuto conto dell'impronta personalistica della nostra *Grundnorm*[100], oltre che di accettabilità dal punto di vista etico.

Recupero ora il nostro tema per giungere a una considerazione conclusiva. Il punto non è se o quando un algoritmo, processando un atto di impugnazione, sarà in grado di riconoscere una (sospetta) ipotesi di inammissibilità. Probabilmente già siamo giunti a questo livello. Il vero nodo è se l'uomo sia in grado di avvalersene riservando un controllo effettivo sull'*output*.

D'altra parte, a fugare le preoccupazioni messe qui sul tappeto, certamente non appare rassicurante l'approdo dell'*AI Act*, che pure formalmente sancisce il diritto a una decisione umana e pone diversi divieti conseguenti alla classificazione «ad alto rischio» del suo utilizzo in ambito giudiziario. Come già rilevato da autorevole dottrina, si tratta di previsioni tutto sommato aggirabili[101].

Così come non tranquillizza affatto la prospettiva di regolamentazione interna, affidata al disegno di legge governativa di materia di intelligenza artificiale, approvato dal Senato e in corso di discussione alla Camera[102]. La norma chiave ammette l'impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria, limitandosi a prescrivere che sia «riservata al magistrato ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti»[103]. Essa si inscrive in una logica permissiva, diametralmente opposta a

---

[99] G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, cit., 2, il quale si chiede, in modo evidentemente provocatorio, «in che modo possono conciliarsi le legali attività investigative ed ancor più il processo formativo della decisione giudiziale con strumenti di origine matematica e di carattere virtuale con una materia del diritto che si nutre di principi e regole di genesi costituzionale, che "umanizzano" il giudizio penale in ogni settore e forma, costituendo la Procedura penale la disciplina dei *moda* dell'accertamento e della decisione finale». Sensibili al rischio paventato nel testo anche G. Gallone, *Riserva di umanità, intelligenza artificiale e funzione giurisdizionale alla luce dell'IA Act. Considerazioni (e qualche proposta) attorno al processo amministrativo che verrà*, cit., spec. §§ 1 e 2; C. G. Giabardo, *Il giudice e l'algoritmo (in difesa dell'umanità del giudicare)*, in ***giustiziainsieme.it***, 9 luglio 2020.

[100] Coglie, con grande lucidità e dovizia argomentativa, questo profilo critico G. Gallone, *Riserva di umanità, intelligenza artificiale e funzione giurisdizionale alla luce dell'IA Act. Considerazioni (e qualche proposta) attorno al processo amministrativo che verrà*,, cit.

[101] V. Manes, *Giustizia artificiale. Siamo davvero disposti ad essere giudicati da un algoritmo?*, cit., 6, il quale segnala che i divieti in questione «risultano tradotti in formulazioni marcatamente compromissorie, ed inframmezzati da deroghe ambigue, se non apertamente contraddittorie, cosicché non si può essere altrettanto sicuri che questi limitati argini normativi possano rivelarsi davvero sufficienti, e solidi». D'altra parte, la fragilità di formulazioni normative di questo tipo non sfugge neanche agli studiosi che propendono per l'implementazione di strumenti algoritmici. Si vedano così le osservazioni di L. Pressacco, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in *BioLaw Journal*, 4, 2022, spec. § 3

[102] Si tratta del d.d.l. recante *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*, presentato il 20 maggio 2024 dal Presidente del Consiglio dei ministri e dal Ministro della giustizia, approvato dal Senato il 20 marzo 2025 con modifiche rispetto al testo dei proponenti (S-1146), attualmente in corso di esame in commissione alla Camera dei deputati (C-2316).

[103] Si tratta del c. 1 dell'art. 15 del testo approvato dal Senato, rubricato *Impiego dell'intelligenza artificiale nell'attività giudiziaria*.

quella che sembrava animare la formulazione originaria del testo presentato dal Governo, centrata sull'utilizzo di tali sistemi «esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario, nonché per la ricerca giurisprudenziale e dottrinale»[104].
Va infine segnalato che la costruzione di procedure automatizzate per il vaglio di ammissibilità delle impugnazioni, in uno con gli altri fattori evidenziati nella prima parte del lavoro (si pensi, in particolare, al tema dell'ufficio per il processo), finiranno per favorire serie criticità in termini di deresponsabilizzazione per la decisione[105]. Aumentando la platea dei soggetti e delle entità che giocano un ruolo nel processo decisionale, diventerà estremamente arduo individuare un centro di responsabilità.

8. L'intollerabile abuso del processo penale come luogo di sperimentazione tecnologica

Concludo segnalando, con una vibrante preoccupazione, un certo atteggiamento che mi pare stia prendendo il sopravvento in ampie frange della dottrina penalistica e processual-penalistica. Si assiste, infatti, a un particolare sforzo orientato a proporre le più svariate modalità di impiego delle innovazioni algoritmiche [106], anche mediante lo sviluppo di concreti e importanti progetti di ricerca[107].

---

[104] Cfr. il c. 1 dell'art. 14 del d.d.l. S-1146, rubricato *Uso dell'intelligenza artificiale nell'attività giudiziaria*. Va detto che, a una lettura attenta, forse neanche la iniziale formulazione delle disposizioni di riferimento sfuggiva ad alcune perplessità, tenendo conto della estrema genericità della locuzione «semplificazione del lavoro giudiziario» e della precisazione contenuta nel c. 2 dell'art. 14, a mente del quale «[è] sempre riservata al magistrato la decisione sull'interpretazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione di ogni provvedimento». La previsione di questa riserva cautelativa sembrava in realtà implicare l'ammissibilità dell'uso dell'intelligenza artificiale in funzione quantomeno ausiliaria rispetto alle attività giudiziarie descritte.

[105] Il rischio di deresponsabilizzazione è segnalato, ancora una volta, da O. Mazza, *Distopia del processo artificiale*, in *archiviopenale.it*., 7 gennaio 2025, 17.

[106] Sono già numerosi i contributi in cui si prospettano disparati impieghi di applicativi di intelligenza artificiale nell'ambito della giustizia penale. Tra di essi: J. Della Torre, *La ragionevole previsione di condanna alla prova della realtà giudiziaria*, in *legislazionepenale.eu*, 19 luglio 2024, 39-41, in tema di decisione sulla richiesta di rinvio a giudizio; R.E. Kostoris, *Predizione decisoria,* diversion *processuale e archiviazione*, cit., §§ 5, 6, in ordine alla decisione sulla richiesta di archiviazione e alle scelte dei riti alternativi; F. Falato, *L'inferenza generata dai* sistemi esperti *e dalle* reti neurali *nella logica giudiziale*, in *archiviopenale.it*, 10 giugno 2020, 12 ss., nel contesto delle indagini preliminari e a supporto del ragionamento probatorio del giudice; E. Guido, *Intelligenza artificiale e procedimento penale: ragionando di valutazione del rischio* de libertate, in *archiviopenale.it*, 8 marzo 2023, sui *risk assessment tools* per la gestione delle misure cautelari; L. Pressacco, *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in *BioLaw Journal*, 4, 2022, per il supporto alla valutazione probatoria. Per un'utile panoramica, si vedano il recente contributo di M. Gjaluz, *Prove fondate sull'intelligenza artificiale e diritti fondamentali*, in *dirittodidifesa.eu*, 15 gennaio 2025, ora anche in *Diritto di Difesa*, 3-4, 2023, 677 ss., e L. Marafioti, *Intelligenza artificiale, giudizio penale e garanzie processuali*, in *Indice Penale*, 3, 2023, 3 ss.

[107] G. Lasagni – G. Contissa, *Un approccio computabile ai diritti processuali penali e al principio del mutuo riconoscimento. I progetti di ricerca* Crossjustice *e* Facilex, in *dirittodidifesa.eu*, 27 gennaio 2025, ora anche in *Diritto di Difesa*, 3-4, 2023, 662 ss.

Ebbene, la mia idea è che, almeno in questo, non guasterebbe una postura intransigente, rifuggendo dalla tentazione di utilizzare il processo – in particolare quell'arnese così delicato rappresentato dal processo penale – come terreno di frenetica e precoce sperimentazione degli ultimi ritrovati tecnologici[108].

Si pensi, per fare un solo (quanto emblematico) esempio, al progetto c.d. *Metacourt*, caratterizzato dallo svolgimento di udienze dibattimentali in ambiente totalmente virtuale con l'utilizzo di *avatar*[109].

Nell'universo della giustizia penale si dovrebbe lucidamente resistere alla fascinazione esercitata dall'intelligenza artificiale e scegliere di lasciare che i collaudi, fino al loro positivo completamento, avvengano in ambienti lontani; e, in particolare, lontani dall'assolvimento dei compiti intrinseci alle funzioni giudiziarie (accertamento, valutazione, decisione).

Un domani, di un futuro remoto, si vedrà.

[108] L. Lupária Donati, *La promessa della giustizia tecnologica*, in *sistemapenale.it*, 1 agosto 2024, 7, il quale, nel proporsi di contrastare quella che definisce una sorta di sindrome di *wunderkammer* tecnologica, osserva: «Viviamo […] imbevuti in una inclinazione mentale per la quale, ove si appalesi un ritrovato di ultimo conio, ci sembra scontato provare a trapiantarlo all'istante ai fini del raggiungimento della verità giudiziale. Si tratta di una impostazione totalmente fuorviante che andrebbe possibilmente eliminata dal nostro orizzonte culturale». Di *wunderkammer* parla anche B. Galgani, *Forme e garanzie nel prisma dell'innovazione tecnologica. Alla ricerca di un processo penale "virtuoso"*, Padova, 2022, 358 ss.

[109] B. Galgani, *Innovazione tecnologica e tradizione personalistica. Dalla partecipazione "a distanza" alle cc.dd. "Metaverse Courtrooms"?*, cit., 13 ss. Si veda pure la notizia dell'evento *MetaCourt*, descritta come la prima simulazione processuale nel Metaverso, realizzata il 1° dicembre 2023 dalle Cattedre di Diritto penale e di Diritto penale e Intelligenza artificiale del Dipartimento di Scienze giuridiche dell'Università degli Studi di Salerno.

Abstract

Il lavoro, dopo aver operato una ricognizione delle più significative linee di tendenza normativa, paranormativa e giurisprudenziale in materia di inammissibilità delle impugnazioni penali – e aver evidenziato la comune visione efficientista che le accomuna –, prova ad analizzare lo stato dell'arte delle tecnologie a disposizione degli attori processuali, con particolare riferimento alla possibilità di affidare a sistemi algoritmici la valutazione di ammissibilità degli atti impugnatori. L'idea di fondo è quella che i processi valutativi e deliberativi in campo penale debbano essere riservati al decisore umano. È un'ingenua illusione credere che, una volta delegati alla dimensione robotica compiti significativi, l'uomo possa mantenere un effettivo controllo su di essi e rimanere immune da fisiologici condizionamenti.

This work, after making an overview of most significant legislative, para-legislative and jurisprudential trends with regard to inadmissibility of criminal appeals – and after highlighting common hyper-efficient vision – tries to analyze the-state-of-the-art of technologies available to the procedural actors, with particular reference to possibility to entrust the admissibility assessment of appeals to algorithm systems. The idea behind it is that the evaluative and deliberative processes must be reserved for the human decision-maker. It's a naïve illusion to believe that human being can keep under control robotic tools and remain immune to its influences.

Keywords

Impugnazioni penali – inammissibilità – intelligenza artificiale generativa – decisioni automatizzate – processo penale

L'IA nel procedimento penale: tra riconoscimento facciale e finalità investigative

Christian Pallante

Sommario

1.L'IA e il procedimento penale: un rapporto in continua trasformazione – 2. Il riconoscimento facciale: aspetti tecnici – 3. Le insidie del riconoscimento algoritmico nel contesto eurounitario: tra prospettive nazionali e *AI Act* – 4. Il riconoscimento facciale come elemento di scambio nel contesto unionale: gli approdi del sistema Prüm II – 5. Lo strumento algoritmico nel contesto italiano – 6. Prospettive *de jure condendo*.

1. L'IA e il procedimento penale: un rapporto in continua trasformazione

Negli ultimi anni, le nuove tecnologie dotate di intelligenza artificiale (IA) hanno iniziato a permeare ogni aspetto della vita quotidiana, trasformando radicalmente il modo in cui ogni persona lavora, comunica e si relaziona con il mondo.

La c.d. "rivoluzione algoritmica" rappresenta ormai la nuova frontiera tecnologica in cui l'umano è chiamato a "misurarsi" con la macchina[1].

L'approccio "tradizionale" di taluna dottrina nordeuropea e d'oltreoceano[2] definisce l'IA come l'insieme di applicazioni che svolgono gli ordinari compiti umani in maniera migliore rispetto all'uomo.

Sebbene in parte anacronistica, la definizione in realtà vuole sintetizzare il forte legame che si crea con l'essere umano, il quale risulta essere ancora al centro della "alimentazione" dell'IA.

Detto legame permea anche le dinamiche del procedimento penale, il quale risulta essere il naturale "banco di prova" di questi nuovi strumenti algoritmici[3].

---

[*] L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

[1] A tal proposito, S. Lorusso, *La sfida dell'intelligenza artificiale al processo penale nell'era digitale*, in *Sist. pen.*, 28 marzo 2024, 1 s.

[2] Su questa concezione, fra gli altri, P. Russell-S.J. Norvig, *Artificial intelligence. A modern approach*, IV ed., Upper Saddle River, 2021, 3.

[3] In tal senso, fra gli altri, W. Nocerino, *Il principio di immediatezza alla prova della tecnologia*, in F.S. Cassibba-L. Foffani-G. Garuti (a cura di), *La riforma Cartabia. Riflessioni sulla legge delega n. 134 del 2021. Atti della Tavola rotonda del 21 aprile 2022*, Torino, 2021, 110, in cui l'A. ricorda come «[S]e è vero che il processo penale è lo specchio della società e rappresenta

Partendo dalla fase che «non conta[va] e non pesa[va]»[4], l'IA prosegue la sua corsa inarrestabile fino alla conclusione dell'arco procedimentale, giungendo anche nella c.d. "giustizia predittiva", ove l'algoritmo tende ad affiancarsi (e, paradossalmente, a "sovrapporsi") alle classiche funzioni dell'organo giudicante[5].

Le tecnologie algoritmiche, in quest'ottica, riflettono la profondissima trasformazione del procedimento penale, caratterizzato dalla progressiva perdita di centralità della fase processuale in senso stretto in ragione del massiccio potenziamento delle indagini preliminari. Infatti, queste ultime rappresentano la nuova sede in cui la prova inizia a formarsi[6] e ad essere addirittura acquisita per la valutazione giudiziale.

In tale frangente, gli strumenti dotati di IA – fra cui il riconoscimento facciale – costituiscono uno dei principali elementi del rafforzamento delle operazioni investigative, tramite cui individuare nuovi elementi probatori (se non direttamente prove) per giungere a una tempestiva identificazione dei possibili autori di reato.

Appare, dunque, fondamentale indagare il ruolo dell'IA all'interno di un procedimento penale profondamente mutato rispetto ai suoi canoni originari, ponendo l'accento proprio sui possibili utilizzi del riconoscimento biometrico che rappresentano una parte sempre più rilevante delle modalità investigative.

---

i valori della società in un determinato momento storico, è altrettanto vero che ogni volta in cui cambia la società, cambia il processo»; S. Quattrocolo, *An introduction to AI and criminal justice in Europe*, in *Rev. Bras. der. proc. pen.*, 2019, 1519 ss.; Ead., *Artificial intelligence, computational modelling and criminal procedure*, Cham, 2020, 3 ss. Sulla medesima scia, B. Custers, *AI in criminal law: an overview of AI applications in substantive and procedural criminal law*, in B. Custer-E. Fosch-Villaronga (a cura di), *Law and artificial intelligence*, Berlino, 2022, 205 ss.; G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in *Dir. pen. cont.*, 4, 2020, 75 ss.; Id., *Perizia, prova scientifica e intelligenza artificiale nel processo penale*, in *Sist. pen.*, 3 giugno 2024, 18 s.

[4] Così, M. Nobili, *Scenari e trasformazioni del processo penale*, Padova, 1998, 35.

[5] Basti pensare ai recenti impieghi dell'IA nel processo penale cinese, in cui negli ultimi anni si è cercato di sperimentare possibili usi dell'algoritmo sia per le attività meramente burocratiche che per la valutazione probatoria, specialmente in casistiche molto semplici. In tema, fra gli altri, G. Barone, *Intelligenza artificiale e metrologia forense. Note a margine delle risoluzioni dell'AIDP su AI e processo penale*, in *Cass. pen.*, 2024, 4063 ss.; I. Cardillo, *Disciplina dell'intelligenza artificiale e intelligentizzazione della giustizia in Cina*, in *Biolaw journal*, 3, 2022, 139 ss.; A. Dell'erba, *La giustizia predittiva come possibile antidoto all'inadeguatezza della giurisdizione*, in *Sist. pen.*, 28 marzo 2024, 2 ss.; R.E. Kostoris, *Intelligenza artificiale, strumenti predittivi e processo penale*, in *Cass. pen.*, 2024, 1642 ss.; G. Ubertis, *Intelligenza artificiale e giustizia predittiva*, in *Sist. pen.*, 16 ottobre 2023, 1 ss.

[6] Su questo profilo, F. Vergine, *Indagini e dibattimento: il singolare funzionamento della clessidra*, in *Dir. pen. proc.,* 2020, 1158, ricorda che il processo penale «[…] è andato (*rectius*, mandato) in crisi, avendo posto in discussione gli stessi ruoli delle varie fasi, decolorando la centralità del dibattimento e arretrando sempre di più il momento tipico dell'accertamento, da un lato rendendo più "libere" le indagini e assegnando una sorta di ultrattività probatoria ai suoi atti e dall'altro intervenendo proprio sul dibattimento ponendo limiti e producendo scorciatoie». Sulla stessa scia, G. Canzio, AI Act *e processo penale: sfide e opportunità*, in *Sist. pen.*, 14 ottobre 2024, 9; W. Nocerino, *La durata delle indagini e il controllo giurisdizionale sui tempi del procedimento*, in *Cass. pen.*, 2023, 2621, la quale precisa che «[S]empre più spesso, infatti, si assiste ad una relazione osmotica tra indagini e giudizio, sia perché gli atti investigativi sono destinati di sovente a trasmigrare nel processo, sia perché molte "prove" sono suscettibili di formarsi già durante la fase preliminare».

2. Il riconoscimento facciale: aspetti tecnici

Gli strumenti di riconoscimento biometrico risultano essersi evoluti e trasformati nell'ultimo decennio.
Tale trasformazione, come riportato da parte della dottrina[7], ha impattato sui tradizionali concetti di "identità" e "identificazione" nel contesto investigativo.
Il primo termine, in particolare, può essere visto come l'insieme delle caratteristiche che connotano un soggetto e che consentono di individuare, o di identificare, quella specifica persona. L'identificazione, invece, rappresenta l'insieme delle tecniche che mira ad attribuire una specifica identità a un soggetto proprio in funzione delle caratteristiche univoche che lo contraddistinguono.
In altri termini, le connotazioni derivanti dal concetto di identità diventano strumentali per l'attività identificativa, considerando che solo grazie a queste peculiarità è possibile distinguere i soggetti d'interesse da una «moltitudine indifferenziata»[8].
Evidente la portata che queste nuove tecnologie possono avere nelle complesse operazioni di individuazione degli autori di reato.
Volendo addentrarsi nell'aspetto più propriamente tecnico, occorre preliminarmente comprendere in cosa si sostanzia il riconoscimento facciale. Attualmente, questo strumento rappresenta l'insieme delle applicazioni di IA che permettono, mediante l'ausilio di algoritmi, di eseguire delle analisi sui tratti biometrici del volto di una persona e, al contempo, di confrontarli con le sembianze dei soggetti inserite in un apposito *database*[9], oltre che di conservarli all'interno della medesima banca dati[10].
Occorre distinguere principalmente due funzioni: il riconoscimento in differita e quello in tempo reale.
In particolare, la prima funzione permette di ricercare – all'interno di una banca dati – l'identità di un volto presente in un'immagine selezionabile di volta in volta dall'operatore. In questo caso, l'apparato di videosorveglianza e la banca dati agiscono in maniera asincrona.
La modalità *Real-time*, invece, permette un riconoscimento pressoché immediato su più video provenienti da impianti di video sorveglianza, in cui la ripresa del soggetto e la sua identificazione sono contestuali.
Dal punto di vista operativo, è innegabile il potente apporto che queste

[7] Sul punto, K. La Regina, *L'identificazione della voce nel processo penale*, Padova, 2018, 2. Più recentemente, C. Pallante, *Identità e identificazione: uno scopo, tante normative*, in G. Bottaro (a cura di), *Identità europea. Storia, tradizione, innovazione*, Messina, *in press*.

[8] Così, P. Foschini, *Le parti responsabili penali*, in *Arch. pen.*, 1954, 31.

[9] Su questi profili, C.S. Milligan, *Facial recognition technology, video surveillance, and privacy*, in *Southern California interdisciplinary law journal*, 9, 1999, 304 ss.; D. Morane-R. Pagar-K. Patil-S. Patil-P.N. Pathak, *Criminal identification using facial recognition*, in *International research journal of modernization in engineering technology and science*, 5(5), 2023, 54; K. Y. Santamaria, *Facial recognition technology and law enforcement: select constitutional consideration*, in W. Lambert (a cura di), *Issues with facial recognition technology*, New York, 2021, 3.

[10] In argomento, E. Wright, *The future of facial recognition is not fully known: developing privacy and security regulatory mechanisms for facial recognition in the retail sector*, in *Fordham intellectual property media & entertainment law journal*, 2019, 29, 621 ss.

tecnologie forniscono alle indagini[11] – tanto nella fase procedimentale, quanto in quella preventiva –, rendendole maggiormente performanti e veloci[12] e determinando, nel medesimo frangente, un forte impatto sui diritti fondamentali delle persone interessate.

Proprio su questo fronte si registrano alcune questioni critiche legate, per ora, al dato tecnico, dal momento che vi possono essere elementi che intaccano l'accuratezza dei riconoscimenti, limitandone fortemente l'affidabilità.

In primis, la scarsa qualità degli strumenti video-fotografici e, conseguentemente, delle immagini catturate da suddette strumentazioni. Infatti, con *frames* di bassa qualità, il programma non ha a disposizione le caratteristiche univoche per associare il volto e fornire un'identificazione, creando il rischio di individuare un soggetto diverso da quello impresso nella foto[13].

In secondo luogo, talune prassi investigative poco chiare, le quali alimentano ulteriori dubbi sull'uso di detti strumenti.

A tal proposito, si possono ricordare alcune casistiche della polizia di New York riguardanti una serie di furti in supermercati[14]. In questi casi, l'indagato viene ripreso da una videocamera posta all'interno del *locus commissi delicti* ma i fotogrammi risultano poco nitidi e il *database* non riesce a fornire alcun riscontro.

Gli investigatori sostituiscono, a loro piacimento, suddetta immagine con una foto dell'attore Woody Harrelson, in quanto dotata (a loro dire) di caratteristiche simili, riuscendo a trovare un possibile risultato nella banca dati[15]. Ciò fornisce molteplici incertezze sull'affidabilità del riconoscimento effettuato.

---

[11] In tal senso, G.M. Baccari, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. Cadoppi-S. Canestrari-A. Manna-M. Papa (a cura di), *Cybercrime*, II ed., Torino, 2022, 1868 ss.; E.M. Mancuso, *L'ingresso dei* big data *nel procedimento penale*, in Associazione tra gli studiosi del processo penale (a cura di), *Diritti della persona e nuove sfide del processo penale*, Milano, 2019, 171 ss.

[12] Si può ben citare il pensiero di K.A. Gates, *Our biometric future. Facial recognition technology and the culture of surveillance*, New York, 2011, 1 s., in cui l'A. ricorda come queste tecnologie potessero essere d'aiuto già nell'attentato delle *Twin towers* che ha cambiato la visione di sicurezza a livello internazionale. Sulla stessa scia Q. Bu, *The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges*, in *International cybersecurity law review*, 2, 2021, 114 ss.

[13] In tema, M. Jacquet-C. Champod, *Automated face recognition in forensic science: review and perspectives*, in *Forensic science international*, 2020, 307, 110124 ss.; H.P. Filho, A. Trajcevski, K. Bhargava, N. Jawed, J.H. Elder, *Attentive sensing for long-range face recognition*, in The Computer Vision Foundation (a cura di), *Proceedings of the IEEE/CVF winter conference on applications of computer vision (WACV) workshops*, 2023, 613 ss.; R.A. Waelen, *The struggle for recognition in the age of facial recognition technology*, in *AI and ethics*, 3, 2023, 216 s.

[14] L'uso di immagini di tal tipo, legato a prassi investigative poco affidabili, ha portato la dottrina americana a parlare di "*fringe techniques*". Il termine esplica efficacemente la predisposizione delle forze di polizia a utilizzare tecniche che talvolta si pongono nel sottilissimo confine tra affidabilità probatoria e inattendibilità. Per tutti, R.D. Goldberg, *You can see my face, why can't I? Facial recognition and Brady*, in *HRLR online*, 5, 2021, 270 s.

[15] Sul punto, G. Edmond-D. White-A. Towler-M. San Roque-R. Kemp, *Facial recognition and image comparison evidence: identification by investigators, familiars, experts, super-recognisers and algorithms*, in *Melbourne university law review*, 45(1), 2021, 31 ss.; A. Pin, *"A Novel and controversial technology". Artificial face recognition, privacy protection, and algorithm bias in Europe*, in *William & Mary bill of rights journal*, 30(2), 2021, 306 ss.

Inoltre, le medesime perplessità vengono in evidenza anche con riferimento ai soggetti appartenenti alle c.d. minoranze.
Proprio nel contesto statunitense è stato studiato, a più riprese, l'impatto negativo che queste tecnologie registrano nei confronti di cittadini afro-americani e asiatici[16].
Questa criticità è dovuta principalmente alla costruzione dei c.d. *dataset*, vale a dire l'insieme di dati che vengono raggruppati all'interno della banca dati, e più precisamente alla scarsa numerosità e rappresentatività di tali dati che non permette all'intelligenza artificiale di "apprendere" nuove caratteristiche per migliorare il proprio algoritmo e, dunque, di giungere a risultati conformi alla realtà[17].

3. Le insidie del riconoscimento algoritmico nel contesto eurounitario: tra prospettive nazionali e *AI Act*

In definitiva, il diritto è sicuramente chiamato a contemperare le esigenze investigative e securitarie con i diritti posti in gioco[18], circoscrivendo le potenzialità d'uso di tecnologie così invasive.
Partendo da tale assunto, bisogna constatare che proprio nel contesto eurounitario si assiste a una stratificazione di provvedimenti[19], talvolta direttamente applicabili, che propongono i consueti problemi generati dal multilivello normativo[20].
Al contrario, sul piano nazionale sono pochissime le realtà che hanno iniziato a legiferare in tal senso, mentre la stragrande maggioranza degli Stati continua a navigare in "zone grigie"[21].
Fra i rari Paesi che hanno avviato un *iter* normativo in suddetta direzione, merita di essere citata la Francia.

---

[16] In suddetto contesto è stata registrata la massiccia presenza di falsi positivi sia nei cittadini afro-americani, specialmente se di sesso femminile, sia in quelli asiatici. Così, P. Grouter-M. Ngan-H. Hanaoka, *Face recognition vendor test (FRVT) part 3: demographic effects*, in *nist.gov*, 2019, 2 ss.; S. Perkowitz, *The bias in the machine: facial recognition technology and racial disparities*, in *MIT case studies in social and ethical responsibilities of computing*, 5 febbraio 2021, 1 ss.

[17] In tema, A. Holkar-R. Walambe-K. Kotecha, *Few-shot learning for face recognition in the presence of image discrepancies for limited multi-class datasets*, in *Image and vision computing*, 120, 2022, 104420 ss.; G.M. Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, 158 ss.

[18] Cfr. L. Lupària Donati-G. Fiorelli, *Diritto probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale*, in *Dir. pen. cont.*, 2, 2022, 39; M. R. Magliulo, *L'intelligenza artificiale nel processo penale: progresso o rischio per la tutela dei diritti costituzionali?*, in *Il Processo*, 3, 2022, 578; A. Pin, *Non esiste la "pallottola d'argento": l'*Artificial Face Recognition *al vaglio giudiziario per la prima volta*, in *DPCE on line*, 4, 2019, 3081.

[19] Si pensi, ad esempio, anticipando quanto si dirà meglio *infra* alle dir. n. 680/2016 e n. 794/2016 e al Reg. n. 982/2024, nonché all'*AI Act* (Reg. n. 1689/2024).

[20] Si rinvia, su tutti, a R.E. Kostoris, *Diritto europeo e giustizia penale*, in *Id.* (a cura di), *Manuale di procedura penale europea*, V ed., Milano, 2022, 1 ss.

[21] Cfr. A. Ramiro-L. Cruz, *The grey-zones of public-private surveillance: policy tendencies of facial recognition for public security in Brazilian cities*, in *Internet Policy Review*, 12(1), 2023, 1 ss.

Pur essendo un modello tipicamente connotato da una legislazione "d'emergenza", ossia caratterizzata dall'uso di situazioni emergenziali (come quelle securitarie) per normatizzare nuovi istituti procedimentali e per renderli applicabili anche nei contesti ordinari, il sistema francese da diversi decenni punta a disciplinare gli strumenti d'indagine, cercando di creare normative specifiche e puntuali in questa delicata materia[22].

Su tale scorta, in tempi più recenti, si sta procedendo a legiferare in merito ai nuovi possibili utilizzi del riconoscimento facciale[23].

Un primo impiego di tale tecnica è già rintracciabile nel casellario giudiziale, dove a norma dell'art. R40-26 c.p.p. è possibile ricorrere all'uso del riconoscimento facciale sulle foto conservate[24], in quanto si tratta di immagini di soggetti condannati e, in casi residuali, di persone scomparse[25].

Un ulteriore utilizzo dello strumento è disciplinato nel c.d. Sistema Parafe, introdotto con il decreto n. 1113 del 4 dicembre 2013 negli artt. R232-6 ss. del codice di sicurezza interna (CSI), che ne prevede l'uso per il controllo automatizzato dei viaggiatori entranti o uscenti dallo spazio Schengen. In tal caso, le immagini del volto sono catturate in tempo reale dagli apparati di videosorveglianza ma non vengono conservate per fini di alimentazione dei *database*[26].

Sulla stessa scia si pone anche la recente normativa in merito alle misure di sicurezza adottate per i giochi olimpici e paraolimpici del 2024[27], in cui il legislatore francese prevede un utilizzo dei sistemi di videosorveglianza in tempo reale, a titolo sperimentale, al solo fine di segnalare eventuali rischi alla sicurezza degli eventi senza ricorrere al riconoscimento facciale[28].

Si è poi avuta anche l'approvazione della legge n. 646/2021 «*pour une sécurité globale préservant les libertés*», con cui vengono potenziate le possibilità di utilizzare videocamere nel corso dell'attività investigativa[29], come nel caso delle *bodycam*.

La Francia, in questo frangente, dimostra di aver scelto di limitare temporaneamente l'uso delle tecnologie algoritmiche con lo scopo di compren-

---

[22] Ne sono chiari esempi l'*IMSI Catcher* e l'attività investigativa su *server* disciplinati nella sezione relativa alle altre tecniche speciali d'indagine del codice di procedura penale francese. Per un'analisi sulla disciplina, D. Curtotti-V. Rizzi-W. Nocerino-A.M. Russitto-G. Giliberti-G. Scarpa, *Piattaforme criptate e prova penale*, in *Sist. pen.*, 6, 2023, 173 ss.; S. Guinchard-J. Buisson, *Procédure pénale*, XV ed., Parigi, 2022, 715 ss.; W. Nocerino, *La tipizzazione dell'*IMSI Catcher *in Francia: sistemi a confronto*, in *Portale intelligence, security & investigation*, 23 giugno 2022; V. Wester-Ouisse, *État d'urgence et procédure pénale*, in *Revue juridique de l'ouest*, 1, 2016, 7 ss.

[23] In tema, M. Picaud, *La reconnaissance faciale: un marché en construction?*, in *Futuribles*, 16 aprile 2020.

[24] Questa disposizione è stata introdotta con il decreto n. 652/2012, relativo al trattamento dei precedenti giudiziari. Sul punto, H. Vlamync, *Droit de police*, VII ed., Parigi, 2021, 540.

[25] Come previsto dall'art. R40-26, c. 3, c.p.p.

[26] Come sancito dall'art. R232-7, c. 2, CSI.

[27] Trattasi della L. n. 2023-380 del 19 maggio 2023. Per un'analisi completa, Sénat, *Rapport d'information sur le project de loi relatif aux jeux olympiques et paralympiques de 2024*, in *sénat.fr*, 18 gennaio 2023.

[28] Questo aspetto viene ben evidenziato dall'art. 10, c. 4, della normativa.

[29] In argomento, F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Arch. pen.*, 2, 2023, 32 s.

derne gli effetti e di regolamentarlo in tempi più maturi[30].
Gli *escamotages*, tuttavia, non mancano. Proprio con riferimento al riconoscimento facciale, un'indagine amministrativa è stata avviata dal ministro dell'interno e condotta dalla *Commission Nationale de l'Informatique et des Libertés* (CNIL) nei confronti della polizia nazionale francese.
In particolare, a seguito del rapporto pubblicato dal giornale investigativo "*Disclose*"[31], emerge un possibile aggiramento della normativa vigente in quanto la *Police Nationale* utilizza un sistema dotato di IA che consente di svolgere il riconoscimento facciale. Il sistema in questione, denominato "*Video synopsis*" e fabbricato dall'azienda israeliana *Briefcam*, permette di analizzare lunghi video nel giro di pochi minuti e di seguire una persona o un veicolo ripresi da più videocamere grazie al proprio abbigliamento o al numero di targa. Il rapporto, più nel dettaglio, evidenzia come suddetto strumento sia stato sperimentato già a partire dal 2015, per poi essere implementato sempre più nelle singole articolazioni della polizia francese.
La questione più spinosa attiene alla possibile elusione della normativa europea, vale a dire la direttiva (UE) 680/2016, che prevede una valutazione d'impatto delle nuove tecnologie utilizzate nel caso in cui queste interferiscano pesantemente con i diritti e le libertà dei soggetti coinvolti, come specificato dall'art. 27 della direttiva.
Il quadro delineato appare sempre più incerto e l'unica possibile via risolutiva diventa un intervento legislativo piuttosto deciso che ne disciplini i limiti applicativi nelle indagini preliminari e, conseguentemente, ne legittimi l'utilizzabilità probatoria in sede processuale[32].
Volgendo lo sguardo al contesto eurounitario, è degno di nota il regolamento di recente approvazione teso a delineare i possibili usi dell'intelligenza artificiale, ossia il c.d. *AI Act* (Regolamento (UE) 1689/2024, "Regolamento").
In questa normativa, l'uso del riconoscimento facciale in sede investigativa viene relegato all'interno degli artt. 5 e 26, scindendo le due modalità di utilizzo, ossia in tempo reale e in differita.
Per quanto riguarda il *real time*, l'art. 5 pone un iniziale divieto di utilizzo degli strumenti di intelligenza artificiale, costruendo una successiva eccezione al veto in ragione della ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani e sfruttamento sessuale e di persone scomparse; della prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche e per quella relativa ad un attacco terroristico; la localizzazione e l'identificazione di una persona sospettata di aver commesso un reato, collegandosi con lo svolgimento di un'attività investigativa, con l'esercizio dell'azione penale e con l'esecuzione di una sanzione penale (art. 5, par. 1, lett. h), *AI Act*).

---

[30] Si può segnalare il rapporto informativo del Senato francese, in cui si riflette sui possibili rischi di detta tecnologia e si cerca di definire una serie di proposte per una futura legislazione in materia. Cfr. Sénat, *Rapport d'information sur la reconnaissance faciale et ses risques au regard de la protection des libertés individuelles*, in *sénat.fr*, 10 maggio 2022.

[31] Sul punto, M. Destal-C. Le Foll-G. Livolsi, *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale*, in *Disclose*, 14 novembre 2023.

[32] In argomento, S. Etoa, *L'image et le son? Le déploiement de la surveillance algorithmique dans l'espace public*, in *Cahiers de la recherche sur les droits fondamentaux*, 2023, 21, 82.

In questo caso, l'*AI Act* cerca di perimetrare l'utilizzo di queste strumentazioni sia per fini preventivi che repressivi sulla scorta dei reati previsti dall'allegato II[33] del Regolamento e della punibilità in concreto degli stessi con una pena o misura di sicurezza di almeno quattro anni, ma di fatto si indirizza sui c.d. "sospettati di reati" senza fornire adeguate garanzie[34] e, soprattutto, con un catalogo di fattispecie piuttosto ampio e poco circoscritto.

Dunque, l'art. 5 si profila come una norma costruita su "apparenti" divieti che, in conseguenza delle continue eccezioni previste, decadono in ragione di finalità chiaramente securitarie.

Inoltre, l'art. 5, par. 3, specifica la necessità di un atto autorizzativo *ex ante* da parte di un'autorità giudiziaria o amministrativa, con natura vincolante, qualora venga utilizzato un sistema di IA dotato di riconoscimento biometrico in tempo reale in spazi accessibili al pubblico.

In casi di urgenza debitamente giustificati è possibile usare il sistema anche in assenza di autorizzazione, a condizione che l'atto sia trasmesso alla competente autorità entro 24 ore per ottenerne l'assenso.

Anche il relativo par. 5 lascia un ampio spazio di manovra nelle mani dei legislatori nazionali, i quali saranno liberi di decidere circa la possibilità di introdurre o meno una specifica procedura autorizzativa.

Tale assetto viene confermato anche dalle linee guida della Commissione europea in merito agli utilizzi "proibiti" del riconoscimento facciale in tempo reale[35], non ancora formalmente adottate.

Per quanto attiene al riconoscimento facciale in differita, invece, l'art. 26, par. 10, del Regolamento inserisce come punto nodale la richiesta di un'apposita autorizzazione *ex ante* o senza indebito ritardo ed entro le 48 ore di un'autorità giudiziaria o amministrativa, la cui decisione deve essere vincolante e soggetta al controllo giurisdizionale.

L'unica eccezione a questa regola generale è dettata dall'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato, su cui tuttavia il Regolamento non fornisce alcuna linea esplicativa.

Si delinea, così, un regime differenziato per l'utilizzo di queste tecnologie, per cui il riconoscimento in differita appare tendenzialmente più garantito rispetto a quello in tempo reale. Infatti, proprio sull'uso in *real time* si profila un prevalere piuttosto netto delle operazioni a carattere preventivo rispetto alle garanzie dei soggetti coinvolti, con il pericolo di penetrare

---

[33] Si tratta, in particolare, dei reati di terrorismo, tratta di esseri umani, 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 e di partecipazione in un'organizzazione criminale finalizzata al compimento di reati.

[34] In tal senso, W. Nocerino, *Sulle modalità di acquisizione delle immagini provenienti dalle videocamere di sorveglianza*, in *Cass. pen.*, 2024, 2425.

[35] Sul punto, Commissione Europea, *Commission guidelines on prohibited artificial intelligence practises established by Regulation (EU) 2024/1689 (AI Act)*, in *digital-strategy.ec.europa.eu*, 4 febbraio 2025, 120 s.

sempre più nelle vicende procedimentali.

4. Il riconoscimento facciale come elemento di scambio nel contesto unionale: gli approdi del sistema Prüm II

Sul piano eurounitario, bisogna segnalare che i dati biometrici e, più nello specifico, il riconoscimento facciale fungono anche da nuovi elementi di scambio tra le forze di polizia europee. Infatti, con il fine di fornire un assetto legislativo che funga da guida, l'Unione europea sta cercando di irrobustire il sistema di cooperazione investigativa, tramite l'ammodernamento del Sistema Prüm[36].

La disciplina, nata sotto forma di proposta nel 2021, è attualmente contenuta nel Regolamento n. 982/2024 che il legislatore europeo ha sviluppato cercando di seguire le osservazioni critiche espresse dallo *European Data Protection Supervisor* in punto di mancanza di limitazioni allo scambio delle informazioni biometriche[37] e sulle misure tecniche da adottare per la protezione di suddetti dati[38], considerando che i criteri di raccolta adottati differiscono in ciascuna Nazione[39].

In particolare, il nuovo Sistema Prüm II rappresenta un'evoluzione dell'attuale struttura di scambio di dati tra Nazioni, in cui vengono inseriti nell'alveo delle informazioni – oltre alle impronte digitali, al DNA e ai dati di immatricolazione di veicoli – le immagini dei volti e il casellario giudiziale. Alla luce dei nuovi innesti normativi, il sistema amplia le sue finalità applicative – inizialmente ricomprese nella sola repressione dei reati – fino ad annoverare la fase preventiva, la ricerca di persone scomparse e l'identificazione di resti umani.

Dal punto di vista della sua struttura, suddetto sistema viene centralizzato mediante l'adozione di un *router*[40] che fornisce agli Stati membri e a Euro-

[36] In tema, A. Procaccino, *Securizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione*, in *Dir. pen. cont.*, 1, 2023, 165; L. Scaffardi, Next Generation Prüm *e le scelte strategiche della UE: dall'ampliamento nello spazio dei dati genetici all'introduzione del riconoscimento facciale*, in *Federalismi*, 8, 2021, 211 ss.

[37] Il Garante europeo nota, in particolare, la mancanza di una gradazione dei reati che permettono la ricerca e, il conseguente scambio, dei dati e che giustificherebbe l'attività di cooperazione tra Stati e la limitazione dei diritti dei soggetti interessati. Così, European Data Protection Supervisor, *Opinion 4/2022 on the proposal for a regulation on automated data exchange for police cooperation ("Prüm II")*, in *edps.europa.eu*, 2 marzo 2022, 9 ss.

[38] Specialmente considerando che la tecnica di pseudonimizzazione è insufficiente a garantire una proporzionalità delle attività. Su questo profilo European Data Protection Supervisor, *Opinion 4/2022 on the proposal for a regulation on automated data exchange for police cooperation ("Prüm II")*, cit., 12.

[39] Questa criticità è ancora presente anche nella precedente situazione delineata dal sistema Prüm. In tal senso, V. Toom-R. Granja-A. Ludwig, *The Prüm decisions as an aspirational regime: reviewing a decade of cross-border exchange and comparison of forensic DNA data*, in *Forensic science international: genetics*, 2019, 41, 50 ss.

[40] Come chiarito dall'art. 35, il *router* è formato da un'infrastruttura centrale, da un canale di comunicazione sicuro fra l'infrastruttura centrale e i punti di contatto delle singole Nazioni e, infine, da un'infrastruttura di comunicazione fra la struttura centrale e

pol la possibilità di ricercare eventuali corrispondenze con le informazioni raccolte da altri Paesi del contesto unionale.
Scendendo più in profondità, il Regolamento prevede, da un lato, l'alimentazione delle banche dati nazionali – indicizzando i dati per permettere un'associazione diretta con il soggetto interessato –, mentre dall'altro regola la consultazione automatizzata dei dati indicizzati messi a disposizione dagli Stati membri e da Europol.
Si precisa che la normativa definisce anche il tempo di risposta del sistema – e quindi di scambio – in un massimo di 48 ore, velocizzando di fatto la cooperazione investigativa.
Nell'espletamento della consultazione dei dati, le autorità competenti sono tenute a fornire una valida giustificazione che contenga la finalità dell'attività e il tipo di soggetto da individuare. Si precisa che tale atto dovrà specificare anche l'intenzione di ottenere maggiori informazioni su persone note oppure di identificare semplicemente autori (o presunti tali) ignoti[41].
Questo passaggio diventa essenziale per garantire la proporzionalità e la necessarietà dell'utilizzo del sistema per i fini investigativi e preventivi, assicurando una protezione dei dati da accessi non autorizzati e sproporzionati.
A questo profilo si collegano i controlli endogeni ed esogeni – da parte di titolari del trattamento nazionali e garanti per la protezione dei dati personali nazionali ed europei – previsti dall'art. 55 del Regolamento.
In questo caso, sebbene la rubrica indichi soltanto una "verifica interna", il tenore letterale della disposizione suggerisce una correlazione con le autorità di controllo nazionali e con il garante europeo.
Si ricorda che il sistema mantiene traccia su base triennale delle giustificazioni fornite e delle registrazioni delle interrogazioni svolte sul sistema dalle Forze di polizia.
La definizione delle sanzioni per l'uso improprio dello scambio e della consultazione di dati viene rimessa integralmente agli Stati membri, richiamando i canoni dell'effettività, della proporzionalità e della dissuasività[42].
I dati devono essere cifrati – in linea di continuità con il Regolamento europeo sulla protezione dei dati personali, n. 679/2016 (GDPR) – e gli Stati membri sono tenuti ad assicurare le misure appropriate per tutelarli.
Il periodo di conservazione di suddette informazioni viene regolato dall'art. 51.
In particolare, si disciplina la loro cancellazione quando non sono più necessari per le finalità investigative, oppure nel periodo specificato dalla normativa nazionale o, in alternativa, nel termine previsto dalla dir. n. 794/2016[43].

---

il portale di ricerca europeo.

[41] La disciplina inerente la giustificazione statale dell'interrogazione del sistema è indicata dall'art. 33.

[42] Come esplicitato dall'art. 56. Per un'analisi sui canoni di effettività, proporzionalità e dissuasività, si v. D. Vozza, *Le tecniche gradate di armonizzazione delle sanzioni penali nei recenti interventi dell'Unione europea*, in *Dir. pen. cont.*, 3, 2015, 19 ss.

[43] La direttiva n. 794/2016 sull'istituzione di Europol prevede all'art. 31, c. 2, un termine *standard* triennale che può essere esteso – previa giustificazione dei motivi per cui la conservazione è necessaria – ad ulteriori tre anni. Al superamento del periodo triennale,

Inoltre, la procedura di scambio delle informazioni viene sviluppata in maniera più specifica. Infatti, in questo frangente, il punto di contatto nazionale – che funge da collegamento con la piattaforma – deve confermare la corrispondenza evidenziata dal sistema per autorizzare lo scambio informativo e, come condizione aggiuntiva, tale compito spetta anche al personale qualificato mediante un esame manuale delle tracce interessate[44]. Entra così in gioco il necessario intervento umano, evidenziato dalla normativa come correttivo agli eventuali errori della "macchina".

Occorre precisare che i dati posti alla base del sistema devono rispettare degli *standard* minimi per il loro utilizzo – come un numero minimo di loci per il DNA o la qualità delle immagini dei volti e delle impronte digitali – che dovranno essere definiti dalla Commissione europea con successivi atti integrativi[45].

Per quanto attiene al collegamento con Europol, si prevede la possibilità di utilizzo dei dati da essa detenuti e, contestualmente, anche la consultazione delle banche dati nazionali da parte dell'Ufficio di polizia europeo.

In quest'ultimo caso, come chiarito dall'art. 49 del Regolamento, il passaggio di informazioni avviene solo dopo il soddisfacimento di alcune condizioni. In particolare, Europol deve trasmettere allo Stato membro interessato il nome del Paese terzo che ha fornito i dati oggetto di confronto, una descrizione dei fatti e del reato per cui si procede e, infine, deve confermare la comparazione tramite un esperto qualificato.

La normativa, inoltre, prevede come condizione necessaria, per connettere le banche dati al sistema centrale, una valutazione d'impatto – in continuità con l'art. 27 della dir. n. 680/2016 –, considerando l'elevato rischio che tale trattamento può comportare sui dati e la possibilità di consultare l'autorità nazionale di controllo[46].

In questo modo, il garante risulta informato sulle condizioni di strutturazione e impiego dei *database* e può svolgere gli opportuni controlli in caso di violazioni.

Il Regolamento, oltre agli aspetti legati alla protezione dei dati contenuti, si ispira al dettato normativo del Regolamento n. 679/2016 (il c.d. GDPR) e della dir. n. 794/2016[47] anche per disciplinare lo scambio di dati a Paesi terzi, mediante l'azione di Europol.

In particolare, Europol può fornire i dati a Nazioni non appartenenti all'Ue – previo consenso dello Stato membro detentore delle informazioni –, in presenza di una decisione di adeguatezza della Commissione

Europol dovrà eseguire una nuova analisi per verificare la necessità di conservare i dati e, qualora il periodo complessivo superi i cinque anni, dovrà informare il Garante europeo per la protezione dei dati personali.

[44] Il Regolamento prevede all'art. 72, par. 1, lett. h), una corrispondenza tra profili legati a soggetti noti e tracce repertate sulla scena del crimine, oppure tra singole tracce o tra profili non noti.

[45] Il riferimento a una successiva definizione degli *standard* di qualità è ben visibile negli artt. 9, 13 e 22 del Regolamento.

[46] La necessarietà della valutazione d'impatto è stata inserita nell'art. 50, par. 4, del Regolamento.

[47] Si tratta del Regolamento istitutivo di *Europol*.

europea[48] o di un accordo internazionale o di cooperazione tra l'Ue e il Paese terzo interessato[49].

Alla luce del quadro delineato si possono trarre alcune considerazioni.

Innanzitutto, l'aspetto maggiormente problematico è l'inserimento dei sospetti – rifacendosi alla definizione[50] offerta dall'art. 6, lett. a), della dir. n. 680/2016 – tra le categorie di soggetti su cui è possibile eseguire il riconoscimento biometrico e le successive operazioni di scambio tra Forze di polizia.

In tal caso, le previsioni in esame ampliano il novero di candidati fortificando le possibilità investigative ma non forniscono delle vere e proprie distinzioni tra soggetti noti e sospetti. Nel primo caso, trattandosi di persone condannate, si pongono sicuramente minori problemi, mentre per i semplici sospetti non vengono fornite garanzie ulteriori.

Inoltre, si notano continui rinvii ad atti integrativi per definire alcuni aspetti peculiari della disciplina, come l'entrata in vigore della normativa e la definizione dei criteri *standard* di qualità del materiale da scambiare, rendendo di fatto meno organica la materia *de qua*.

La disciplina europea lascia ampissimi margini di manovra agli Stati membri sia nella definizione degli aspetti tecnici (come l'acquisizione degli elementi probatori) che sulle procedure di utilizzo e di scambio dei dati, non diventando pienamente applicabile in questi frangenti.

Questo approccio fa, dunque, scorgere all'orizzonte l'insorgere di normative nazionali che dovranno disciplinare il funzionamento delle nuove banche dati – come quella per il riconoscimento facciale – e le procedure di collegamento con la moderna infrastruttura europea.

Ciò dimostra come, sebbene sia forte l'intenzione delle istituzioni europee di coniugare tra loro le discipline dei singoli Stati membri, non si può ancora affermare che si sia raggiunta un'armonizzazione concreta delle normative[51], considerando l'enorme distanza esistente tra i legislatori di ciascun contesto nazionale e le zone "d'ombra" ancora presenti.

---

[48] La decisione di adeguatezza è un atto con cui la Commissione europea deve esaminare il livello di protezione dei dati personali offerto dallo Stato non membro dell'Unione europea verso cui andrebbero trasferiti i dati. Per un'analisi dettagliata, si v. F. Balducci Romano, *I trasferimenti di dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 953 s.

[49] In particolare, l'art. 60 del Regolamento fornisce un rimando all'art. 25 della dir. n. 794/2016, in cui vengono esplicate le condizioni con cui Europol può trasferire i dati.

[50] L'art. 6, lett. a), della dir. 680/2016 annovera i dati delle «[…] persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato».

[51] In tal senso, D. Curtotti, *Indagini* hi-tech*, spazio* cyber*, scambi probatori tra Stati e* Internet provider service *e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 2021, 759, la quale ricorda che oggi la difficoltà è nel «[…] trovare soluzioni di bilanciamento, per un verso, tra interessi in gioco quali la sicurezza pubblica e diritti fondamentali (privacy, diritto di difesa, ecc.), e per altro verso tra normative statali ancora distanti tra loro».

5. Lo strumento algoritmico nel contesto italiano

Sul fronte nazionale, la situazione non appare più rassicurante.
Innanzitutto, dal punto di vista operativo, è attualmente in funzione il Sistema Automatico di Riconoscimento Immagini (S.A.R.I.) presso la Polizia di Stato.
Quest'ultimo si presenta come un *software*, basato su algoritmi, in grado di confrontare volti ignoti con quelli di soggetti foto-segnalati. Anche in questo caso si possono individuare due distinte procedure operative di suddetto programma, vale a dire le modalità *Enterprise* e *Real-time*[52].
In particolare, la prima procedura permette di ricercare, mediante un sistema automatico, l'identità di un volto presente in un'immagine all'interno di una banca dati di grandi dimensioni (con un massimo di 10 milioni di immagini), selezionabile di volta in volta dall'operatore. Suddetta attività può avvenire su base volto, su base anagrafica/descrittiva[53] o integrando entrambe le metodologie.
La modalità *Real-time*, invece, permette un riconoscimento in tempo reale su più video provenienti da impianti di video sorveglianza. I volti presenti nei fotogrammi vengono analizzati e confrontati, tramite un algoritmo di riconoscimento, con quelli presenti in una *watchlist* (con un massimo di circa 10.000 volti). Nel caso di *match*, ossia di confronto positivo, il sistema genera un *alert* che permette di avvisare l'operatore.
Detta piattaforma è stata oggetto di varie critiche.
Innanzitutto, la scelta di non inserire degli *standard* minimi per la qualità delle immagini da utilizzare rischia di amplificare il pericolo di un riconoscimento non attendibile[54], aumentando il tasso di errore[55].
Sebbene l'uso in differita del SARI sia stato approvato dal Garante per la Protezione dei Dati Personali[56], altrettanto non può dirsi per il *real-time*. Infatti, in questo caso la decisione negativa dell'autorità amministrativa è dettata dalla mancanza di una normativa, vista come situazione preoccupante per il rischio di sorveglianza massiva[57].
Dal punto del procedimento penale, bisogna comprendere quale possa essere la portata di uno strumento di tal tipo e se sia effettivamente ascrivibile all'interno degli istituti esistenti; in altre parole, è necessario capire

[52] Su suddette modalità Ministero dell'Interno, *Capitolato tecnico. Procedura volta alla fornitura della soluzione integrata per il Sistema Automatico di Riconoscimento Immagini (S.A.R.I.)*, in *poliziadistato.it*, 2016, 14 ss.

[53] La base analitica/descrittiva prevede una ricerca sulla base di informazioni anagrafiche o descrittive associate alle immagini nella banca dati dei soggetti fotosegnalati.

[54] Così, R. Lopez, *La rappresentazione facciale tramite software*, in A. Scalfati (a cura di), *Le indagini atipiche*, II ed., Torino, 2019, 244.

[55] Sul punto, C. Castelluccia-D. Le Métayer, *Analyse des impacts de la reconnaissance faciale. Quelques éléments de méthode*, in *Inria*, 20 novembre 2019, 8.

[56] Cfr. Garante privacy, *Sistema automatico di ricerca dell'identità di un volto*, 26 luglio 2018 (doc. web 9040256).

[57] A tal proposito, Garante privacy, *Parere sul sistema Sari Real Time*, 25 marzo 2021 (doc. web 9575877); R. Lopez, *Videosorveglianza biometrica tramite riconoscimento facciale: parere negativo del Garante per la "privacy"*, in *Proc. pen. giust.*, 2022, 798 ss.

come quest'ultimo si collochi nella tassonomia probatoria.
Innanzitutto, non appare molto condivisibile l'impostazione fornita da parte della dottrina[58] per cui il riconoscimento facciale sarebbe accostabile, seppur sotto forma di "filiazione spuria"[59], all'individuazione di persone e cose prevista dall'art. 361 c.p.p.
In primis, per lo scopo di questa disposizione. Non a caso, quest'ultima punta maggiormente alla "necessaria prosecuzione delle indagini" piuttosto che ad un suo possibile utilizzo in sede processuale. Infatti, sebbene il risultato dell'attività possa giungere nella fase di giudizio mediante l'*escamotage* della testimonianza dell'"individuatore", nella sostanza l'atto rimane nelle mani del p.m. e, tendenzialmente su sua delega, della p.g. e si colloca direttamente nelle indagini preliminari.
In secondo luogo, si tratta di un istituto piuttosto scarno[60], privo di una descrizione dettagliata delle modalità esecutive e documentative e influenzato dalla capacità mnemonica e dalle condizioni psicofisiche della persona chiamata a svolgere l'individuazione[61].
Sarebbe, quindi, impensabile assimilare la capacità di un soggetto a fare un "riconoscimento" con quella di un sistema algoritmico che punta a confrontare meccanicamente le caratteristiche dei volti. Si rischierebbe di confondere i processi della mente umana con quelli della macchina.
Analoghi problemi interpretativi si pongono anche con riferimento alla tesi di un uso "pacifico" dello strumento per le finalità dell'art. 349 c.p.p.[62].
Proprio sul fronte delle attività volte all'identificazione dell'indagato, la norma prevede la possibilità di eseguire «[…] ove occorra, rilievi dattiloscopici, fotografici e antropometrici nonché altri accertamenti».
Innanzitutto, risulterebbe complesso ridurre l'operazione di confronto e di analisi svolta dallo strumento tecnologico alle sole ipotesi previste dalla disposizione in esame.
Come evidenziato dalla dottrina[63], anche con riferimento alle altre tipologie di attività, il concetto di identificazione si è sviluppato mentre il dato normativo sembra ancora risentire di un mancato adeguamento all'odierna realtà operativa d'indagine.
Sicuramente il rilievo fotografico – connotato da una meccanicità dell'attività posta in essere[64] – risiede maggiormente nel fotosegnalamento del

[58] Tra gli altri, R. Lopez, *La rappresentazione facciale tramite software*, cit., 253.

[59] *Ibidem*.

[60] Sui problemi della disciplina dell'art. 361 c.p.p., fra gli altri, si v. T. Alesci, *Il corpo umano fonte di prova*, Padova, 2017, 92 s.

[61] Dal punto di vista dell'"individuatore" bisogna ricordare che ci sono dei fattori, sia di tipo emotivo che fisico, che possono distorcere la ricostruzione e il conseguente ricordo dell'immagine della persona da riconoscere. Su questi profili, G. Cecanese, *Aspetti problematici e snodi interpretativi dell'individuazione di persone e di cose*, in *Arch. pen.*, 2018, 1, 20; D. Mastro, *Le cause degli errori giudiziari e i meccanismi di prevenzione e riparazione delle condanne e imputazioni ingiuste*, in *Rev. Bras. dir. proc. pen.*, 8(3), 2021, 1383 ss.

[62] Così, M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, in *Dir. pen. proc.*, 8, 2021, 1052 ss.

[63] Su questi profili si rimanda alla puntuale analisi di D. Curtotti, *Rilievi e accertamenti tecnici*, Milano, 2013, 108 ss.

[64] In tema, A. Chelo, *Rilievi, accertamenti e accertamenti tecnici*, in C. Conti, A. Marandola (a

soggetto piuttosto che in una successiva operazione di confronto tra l'immagine della persona sottoposta alle indagini e quelle conservate in un'apposita banca dati, specialmente considerando che la seconda attività ha un grado di complessità maggiore e i suoi risultati sono connotati da un valore probatorio più profondo[65].

A tal proposito, non va trascurato l'ingente apporto che dovrebbe essere fornito dagli operatori che procedono al riconoscimento algoritmico, cadendo quindi in un accertamento, per verificare l'attività svolta dalla macchina. Si potrebbe ragionevolmente pensare che sia ricompreso negli "altri accertamenti" richiamati dalla disposizione *de qua*, ma ciò rischierebbe di ampliare eccessivamente le maglie entro cui può muoversi la p.g. nell'espletamento delle operazioni identificative, senza esplicare i limiti di un insieme di operazioni piuttosto invasive per il soggetto *ivi* sottoposto. Inoltre, la finalità delle attività identificative si dovrebbe ridurre ad una valenza meramente indiziaria e, quindi, per l'immediata prosecuzione delle indagini[66].

Al pari, non convince neppure una possibile interpretazione estensiva dell'art. 189 c.p.p. Difatti, la c.d. "prova atipica" consta di tre importanti limiti, ossia deve essere idonea ad accertare il fatto da provare, deve rispettare la libertà morale dei soggetti coinvolti e, sotto il punto di vista processuale, richiede un contraddittorio anticipato tra le parti sulle modalità di acquisizione probatoria[67]. Applicare questi criteri al riconoscimento facciale non appare molto agevole[68], considerando che questa disposizione rappresenta un vero e proprio "*escamotage* investigativo"[69].

Innanzitutto, l'autorità giudiziaria non ha modo di valutare in maniera concreta l'idoneità del *software* per i fini di accertamento del fatto[70]. Ciò è dovuto alla circostanza per cui la procedura eseguita per individuare la persona e, conseguentemente, le componenti specifiche – vale a dire il tasso di errore, la grandezza del *dataset* di cui è costituito e la qualità delle

---

cura di), *La prova scientifica*, Milano, 2023, 711 ss.; D. Curtotti, *Rilievi e accertamenti tecnici*, cit., 14 ss.

[65] In tal senso, R.E. Kostoris, *Prelievi biologici coattivi*, in R.E. Kostoris-R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Torino, 2005, 329.

[66] In argomento, P.P. Paulesu, Sub *art. 349 c.p.p.*, in A. Giarda-G. Spangher (a cura di), *Codice di procedura penale commentato*, VI ed., II, Padova, 2023, 1678 ss.

[67] Con riferimento ai dubbi interpretativi legati alla possibile lettura estensiva dell'art. 189 c.p.p., si v., fra gli altri, C. Conti, Sub *art. 189 c.p.p.*, in A. Giarda-G. Spangher (a cura di), *Codice di procedura penale commentato*, I, cit., 2601 ss.; P. Ferrua, *Ammissibilità della prova e divieti probatori*, in *Rev. Bras. dir. proc. pen.*, 7(1), 2021, 228 s.; A. Procaccino, *Prove atipiche*, in A. Gaito (a cura di), *La prova penale*, Milano, 2008, 265 ss.; P. Tonini-C. Conti, *Il diritto delle prove penali*, II ed., Milano, 2014, 196 ss.

[68] Su questo profilo, tra gli altri, G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *Legisl. Pen.*, 11 dicembre 2021, 23.

[69] Come ben sottolinea A. Scalfati, *IA e processo penale: prospettive d'impiego e livelli di rischio*, in *Proc. pen. giust.*, 2024, 1408, l'art. 189 c.p.p. diventa «[...] il canale mediante cui profittarne [...]», creando rischi sui diritti fondamentali e contestazioni sul risultato probatorio prospettato.

[70] In tema, A. Marandola, *Il riconoscimento facciale*, in C. Conti-A. Marandola (a cura di), *La prova scientifica*, cit., 510 s.

immagini utilizzate – dello strumento sono avvolte da un'opacità, piuttosto ardua da contrastare, che non permette di conoscere questi elementi costitutivi[71], considerando che la valutazione deve essere svolta *ex ante*[72].
Questo insieme di profili critici rende, quindi, difficoltoso un possibile ricorso all'atipicità, in vista di una carenza di garanzie minime che assicurino l'affidabilità degli elementi probatori raccolti. Si rischierebbe, così, di cadere in un'inutilizzabilità dei risultati appresi, permettendo delle vere e proprie "scorciatoie probatorie"[73].
Si pone su un terreno piuttosto scivoloso anche la prospettiva offerta dalle Forze di polizia[74], in cui l'attività verrebbe qualificata come "accertamento tecnico". Un'impostazione di tal tipo rischierebbe di far entrare suddetto "*genus*" di attività identificativa, come già evidenziato piuttosto opaca, nel processo penale.
In particolare, la tipologia di attività da eseguire, avendo prevalentemente carattere ripetibile, verrebbe ricompresa nell'alveo delle operazioni dell'art. 359 c.p.p. e, in casi particolari e residuali, nell'art. 354 c.p.p.
Così facendo, vengono meno le garanzie difensive e, come analizzato da alcuni[75], queste norme non danno contezza dei limiti applicativi entro cui possono spingersi le Forze di polizia nell'applicazione dello strumento.
Inoltre, questo disposto normativo risulta anche carente, se applicato allo strumento in esame, di un vero e proprio controllo da parte dell'autorità giudiziaria.

6. Prospettive de *jure condendo*

Alla luce delle osservazioni svolte in sede investigativa e della ricostruzione delle possibili interpretazioni possono sicuramente trarsi alcune considerazioni sistematiche.
Innanzitutto, l'attuale panorama legislativo non pare offrire in questa delicata materia sufficienti garanzie all'utilizzo di moderni strumenti tecnici d'indagine, come quelli di tipo algoritmico. Si assiste a una realtà a doppia velocità, dove la tecnologia continua a fare numerosi passi in avanti e il diritto non riesce a svilupparsi di pari passo[76].

---

[71] Sul punto, J. Della Torre, *Quale spazio per i* tools *di riconoscimento facciale nella giustizia penale?*, in G. Di Paolo-L. Pressacco (a cura di), *Intelligenza artificiale e processo penale. Indagini, prove e giudizio*, Trento, 2022, 38 s.; M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, 64 s.

[72] In tal senso, E. Aprile, *La prova penale*, Milano, 2002, 60 s.

[73] Così, F.R. Dinacci, *Le regole generali delle parole*, in G. Spangher (a cura di), *Procedura penale. Teoria e pratica del processo*, I, Torino, 2015, 776; A. Scalfati-D. Servi, *Premesse sulle prove penali*, in A. Scalfati (a cura di), *Trattato di procedura penale*, II, I – *Le prove*, Torino 2008, 28 ss.

[74] In argomento, Ministero dell'Interno, *Sistema automatico di riconoscimento immagini: un futuro che diventa realtà*, in *interno.gov*, 19 settembre 2021.

[75] Tra gli altri, J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, in *Riv. it. dir. proc. pen.*, 3, 2022, 1084 s.

[76] Su questo aspetto si rimanda all'analisi di D. Curtotti, *L'inadeguatezza delle norme al*

Sebbene una parte della dottrina[77] abbia tentato di colmare la lacuna legislativa con delle interpretazioni di sistema, queste soluzioni non sembrano molto praticabili. Infatti, al pari di quanto avvenuto in tema di prova scientifica[78], il codice di rito risente ancora di un'obsolescenza delle sue norme – essendo ancora legato all'impianto originario di un procedimento penale ancora formalmente polarizzato sulla fase dibattimentale– che non permette un adattamento a "nuovi" strumenti come quelli algoritmici, non contemplando le garanzie minime che il procedimento penale contemporaneo richiede.

Al contempo, proprio sul fronte delle nuove tecnologie – specialmente nel caso del riconoscimento facciale – non sembra auspicabile neppure un adattamento *tout court* a impostazioni dottrinali per cui tutte le attività non espressamente vietate dalla legge sono da considerarsi pienamente lecite[79], per via delle potenzialità dello strumento biometrico e dell'alta invasività sui diritti e sulle libertà dei soggetti interessati. In questo modo, infatti, si rischia di far entrare nel procedimento (o peggio ancora nel processo) elementi provenienti da uno strumento opaco, ancora poco controllato, connotandoli di un'utilizzabilità intrinseca con l'*escamotage* dell'art. 189 c.p.p.

Emerge chiaramente, come auspicato da parte della dottrina, l'esigenza di introdurre una disposizione normativa che fissi l'*an* e il *quomodo* di utilizzo di queste moderne strumentazioni[80].

Anche il legislatore è conscio di questa necessità[81].

---

cospetto della nuova realtà investigativa e le soluzioni giuridiche percorribili, in D. Curtotti-L. Saravo (a cura di), *Manuale delle investigazioni sulla scena del crimine*, II ed., Torino 2022, 171 ss.; M. Tallacchini, *Scienza e tecnologia: paradigmi normativi e nuove tecnologie*, in P. Tincani (a cura di), *Diritto e futuro dell'Europa*, Colle di Val d'Elsa, 2021, 135 ss.

[77] V., tra gli altri, R. Lopez, *La rappresentazione facciale tramite software*, cit., 253; M. Torre, *Nuove tecnologie e trattamento dei dati personali nel processo penale*, cit., 1052 ss.

[78] Si v., fra gli altri, E. Aprile, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, 4034; C. Bonzano, *Prova "scientifica": le garanzie difensive tra progresso tecnologico e stasi del sistema*, in C. Conti (a cura di), *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, Milano 2011, 116; A. Camon, *La fase che "non conta e non pesa": indagini governate dalla legge?*, in *Dir. pen. proc.*, 2017, 425 s.; D. Curtotti, *Rilievi e accertamenti tecnici*, cit., 161 s.; P. Felicioni, *La prova del DNA nel procedimento penale*, Torino 2018, 11; A. Scalfati, *La deriva scientista dell'accertamento penale*, in *Proc. pen. giust.*, 2011, 148.

[79] Su questa impostazione, F. Cordero, *Tre studi sulle prove penali*, Milano, 1963, 157 ss.

[80] In tal senso, J. Della Torre, *Tecnologie di riconoscimento facciale e procedimento penale*, cit., 1093; W. Nocerino, *Sulle modalità di acquisizione delle immagini provenienti dalle videocamere di sorveglianza*, cit., 2425; C. Pallante, *Identità e identificazione: uno scopo, tante normative*, cit., *in press*; A. Scalfati, *IA e processo penale: prospettive d'impiego e livelli di rischio*, cit., 1409; M. Torre, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali*, in *Proc. pen. giust.*, 6, 2024, 1544.

[81] Sulla necessità di una normativa, si sono registrate alcune piccole aperture anche da parte del legislatore. Infatti, in un primo momento è stata approntata una prima proposta di legge che bloccasse temporaneamente l'installazione e l'uso di impianti di videosorveglianza che utilizzano sistemi di riconoscimento facciale, nell'attesa di una normativa che ne disciplinasse i relativi limiti, senza tuttavia riuscire nell'intento (Proposta n. 3009/2021). Successivamente, con la L. n. 205 del 3 dicembre 2021, di conversione del D.lgs. n. 139 dell'8 ottobre 2021 *recante* "*Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali*", il Parlamento ha previsto nell'art. 9, co. 9, un blocco dell'installazione

Inoltre, sul fronte dei diritti solo l'esplicitazione dei limiti[82] può fornire un effettivo contemperamento tra i fini securitari e i diritti dei cittadini coinvolti. Non bisogna, infatti, trascurare che libertà e sicurezza rappresentano due facce di una stessa medaglia[83] e non più degli interessi totalmente contrapposti tra loro.

Al contrario, uno scenario privo di limiti espliciti – in cui l'uso di queste strumentazioni sia permesso *tout court* e dove i risultati possono fornire una base per l'accertamento dei fatti – rischia di formare la base di un controllo massivo sui cittadini[84].

Analizzando le vicissitudini del sistema francese appare piuttosto ovvia questa considerazione di sistema. Infatti, il rischio di un aggiramento della normativa e, quindi, di un utilizzo incontrollato degli strumenti algoritmici è sempre presente.

Le esperienze internazionali insegnano proprio questi aspetti.

Sebbene possa sembrare potenzialmente «illusorio»[85], unicamente la predisposizione di peculiari normative può contribuire a rendere maggiormente trasparenti gli strumenti investigativi, mirando a fornire le opportune garanzie per i soggetti coinvolti.

Con ciò non si vuole limitare l'attività investigativa con un eccessivo formalismo giuridico ma si intende garantire che quest'ultima sia conforme ai principi di uno Stato di diritto, all'interno di un ordinamento che, al giorno d'oggi, risulta essere ancora orfano di regole[86].

Come già accaduto per alcuni ritrovati della tecnica[87], anche in questo fran-

---

e dell'utilizzazione di impianti di tal tipo in luoghi pubblici o aperti al pubblico fino all'emanazione di una disciplina legislativa *ad hoc*, fornendo come termine ultimo il 31 dicembre 2023. Allo stato, non risulta ancora pronta un'effettiva normativa in materia ma il legislatore, mediante l'art. 8-*ter* della L. n. 87 del 3 luglio 2023 di conversione del D. l. n. 51 del 10 maggio 2023 "*recante disposizioni urgenti in materia di amministrazione di enti pubblici, di termini legislativi e di iniziative di solidarietà sociale*", ha preferito prorogare il termine previsto al successivo 31 dicembre 2025. Su questa ricostruzione, F. Di Matteo, *La riservatezza dei dati biometrici nello spazio europeo dei diritti fondamentali: sui limiti all'utilizzo delle tecnologie di riconoscimento facciale*, in *Freedom, security & justice: European legal studies*, 2023, 1, 110; A. Procaccino, Soft law *e giustizia penale*, Pisa, 2023, 56 s.

[82] In tema, J. Della Torre, *Novità dal Regno Unito: il riconoscimento facciale supera il vaglio della* High Court of Justice, in *Dir. pen. cont.*, 2020, 1, 243 s.; E. Sacchetto, Face to face*: il complesso rapporto tra* automated facial recognition technology *e processo penale*, in *Legisl. pen.*, 16 ottobre 2020, 13 s.; *Ead.*, *Spunti per una riflessione sul rapporto tra biometria e processo penale*, in *Dir. pen. cont.*, 2, 2019, 477.

[83] Su questo peculiare concetto, W. Nocerino, *Le intercettazioni e i controlli preventivi*, cit., 393 s.

[84] In tal senso, M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in G. Balbi-F. De Simone-A. Esposito-S. Manacorda (a cura di), *Diritto penale e intelligenza artificiale*, Torino, 2022, 126; W. Nocerino, *Le intercettazioni e i controlli preventivi*, cit., 384.

[85] Così, G.M. Baccari-C. Conti, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla* privacy*: uno sguardo d'insieme*, in *Dir. pen. proc.*, 2021, 721 s.

[86] In questo senso, D. Curtotti, *L'inadeguatezza delle norme al cospetto della nuova realtà investigativa e le soluzioni giuridiche percorribili*, in D. Curtotti-L. Saravo (a cura di), *Manuale delle investigazioni sulla scena del crimine*, II ed., Torino, 2022, 171 ss.; *Ead.*, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. giust.*, 2018, 435 ss.

[87] Sul punto, si v., fra gli altri, W. Nocerino, *Il tramonto dei mezzi di ricerca della prova nell'era*

gente ci si trova di fronte a un problema tipicamente normativo. In questi casi, infatti, la giurisprudenza ha cercato di sopperire alle carenze legislative, fornendo agli interpreti possibili coordinate sistemiche nelle categorie probatorie esistenti[88].

Nel contempo, anche le Corti sovranazionali hanno tentato di fornire possibili risposte[89].

Sicuramente, un legislatore assente che si affida alle "cure" costanti della giurisprudenza non sembra essere una soluzione appagante, con il pericolo di generare nuove "zone grigie" e di non regolare una materia connotata da profili critici e da continue opacità[90].

Non sembra neppure sostenibile una posizione di totale chiusura verso queste nuove potenzialità investigative, con il rischio di indebolire l'efficienza investigativa in ragione delle prerogative individuali[91].

Guardando al modello francese, anche con riferimento ad altri strumenti tecnici[92], è probabilmente giunto il momento di riflettere su possibili interventi normativi che ne riescano a fornire un'organicità e una precisa

2.0, in *Dir. pen. proc.*, 2021, 1029 s.

[88] Si pensi, più recentemente, a quanto avvenuto in materia di indagini su piattaforme criptate e di trojan, in cui si sono susseguite molteplici sentenze della Corte di Cassazione. Su questo profilo, si v., tra gli altri, W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle Sezioni Unite*, in *Pen. DP*, 3, 2023, 485 ss.; *Ead.*, *Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale*, in *Cass. pen.*, 2016, 3546 ss.; V. Rizzi-D. Curtotti-A.M. Russitto-G. Giliberti-G. Scarpa-W. Nocerino, *Piattaforme criptate e prova penale. L'etere digitale alla sfida del codice di rito*, in *Polizia moderna*, 8, 2023, 50 ss.

[89] Si pensi alla sentenza *Glukhin vs. Russia* del 2023, con cui la Corte Europea dei diritti dell'uomo arriva a riconoscere, per la prima volta, il pieno utilizzo in sede investigativa del riconoscimento facciale, pur in mancanza di atti investigativi che ne "testimonino" l'effettivo uso. Questa conclusione viene suffragata dall'identificazione di un cittadino moscovita in sole 48 ore e dalle attività di estrazione dei filmati dalle videocamere della metropolitana di Mosca da parte delle forze di polizia. Sulla base di questi elementi, la Corte si trova a sviluppare il ragionamento già intrapreso con la sentenza *Gaughran* vs. *United Kingdom* del 2020, in cui aveva riconosciuto un potenziale rischio per le libertà nella conservazione delle immagini da parte delle forze di polizia – le quali possono razionalmente confluire in futuri *database* investigativi –, sino a introdurre il riconoscimento facciale nell'alveo dell'art. 8 CEDU, richiamando l'esigenza di una riserva di legge che perimetri l'uso di tale strumento. Cfr. CEDU, *Glukhin c. Russia*, ric. 11519/20 (2023), in *Proc. pen. giust.*, 2024, 413, con nota di O. Bruno, *La condanna per manifestazione pacifica (non preavvisata e) con riconoscimento facciale viola i diritti fondamentali*; G. Gallo, *Tecnologie di riconoscimento facciale e diritti fondamentali a rischio: il caso* Glukhin c. Russia *dinanzi alla Corte europea dei diritti dell'uomo*, in questa *Rivista*, 3, 2023, 195 ss.; G. Mobilio, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico: osservazioni a partire dal caso* Glukhin c. Russia, in *DPCE online*, 2024, 1, 695 ss.; C. Nardocci, *Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU* Glukhin c. Russia, in *Biolaw journal*, 2024, 1, 279 ss.

[90] F. Paolucci, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in questa *Rivista*, 2021, 1, 216.

[91] In questo senso, L. Camaldo, *Intelligenza artificiale e investigazione penale predittiva*, in *Riv. it. dir. proc. pen.*, 2024, 1, 249 s.

[92] Sul punto, S. Guinchard-J. Buisson, *Procedure pénale*, cit., 557 s.; W. Nocerino, *Ancora in tema di criptofonini: nuovi arresti giurisprudenziali in attesa delle sezioni unite*, cit., 487 ss.; E. Vergès, *La procédure pénale technicienne (ou l'asphyxie procédurale)*, in *Revue de sciences criminelles*, 3, 2019, 673 ss.

collocazione nel codice di rito.
Si potrebbe pensare a una norma aperta che punti a circoscrivere l'attività apprensiva e non il singolo strumento. Una sorta di "acquisizione di immagini biometriche", ossia un nuovo mezzo di ricerca della prova la cui titolarità (in termini di atti autorizzativi) potrebbe spettare alla giurisdizione e, in casi urgenti, all'organo inquirente.
In questo modo si potrebbero prevenire eventuali rischi di obsolescenza normativa, permettendo gli appositi adattamenti del testo legislativo ai mutamenti della società e della tecnica.
La norma, inoltre, potrebbe fungere da base anche per disciplinare la Banca dati SARI, inserendo le garanzie minime (tecniche e giuridiche) per connotare il risultato comparativo di un'elevata affidabilità processuale.
Così, si scongiurerebbe il rischio paventato dal Garante privacy di utilizzi massivi degli strumenti di riconoscimento biometrico[93], restituendo una dimensione investigativa a strumenti nati in sede preventiva.
Allo stesso modo – senza sacrificare eccessivamente le prerogative individuali – si individuerebbero l'*an* e il *quomodo* di attività di tal tipo, perimetrandole e rispettando il principio di proporzionalità.
Dunque, se quest'ultimo appare essere il più nobile obiettivo, non resta che attendere che i singoli legislatori nazionali e, più nello specifico quello italiano, forniscano indicazioni volte a perimetrare queste nuove potenzialità investigative e, soprattutto, a far comprendere i possibili utilizzi in sede probatoria.

[93] In tema, Garante privacy, *Parere sul sistema Sari Real Time*, 25 marzo 2021 (doc. web 9575877), cit.

Abstract

Negli ultimi anni, le nuove tecnologie dotate di intelligenza artificiale (IA) hanno iniziato a permeare ogni aspetto della vita quotidiana, trasformando radicalmente il modo in cui ogni persona si relaziona con il mondo. A partire da queste semplici applicazioni, l'IA sta progressivamente potenziando il suo raggio d'azione, entrando a pieno titolo anche nelle dinamiche dell'investigazione penale. Ne costituisce un classico esempio l'impiego dell'IA a fini di riconoscimento facciale che consente di eseguire analisi sui tratti biometrici del volto per confrontarli con le caratteristiche inserite in un apposito *database*, nonché di conservarli all'interno della banca dati. Partendo da queste considerazioni preliminari, lo scritto analizza l'uso crescente dell'IA nel procedimento penale con particolare riferimento al riconoscimento facciale, ponendo l'attenzione sulle sue principali applicazioni investigative all'interno della legislazione nazionale ed eurounitaria.

In recent years, new technologies equipped with artificial intelligence (AI) have begun to permeate every aspect of daily life, radically transforming the way in which each person relates to the world. Starting with these simple applications, AI is gradually expanding its scope, becoming an integral part of criminal investigation. A classic example of this evolution is the use of AI for facial recognition, which allows biometric facial features to be analyzed and compared with characteristics stored in a specific database, as well as stored within the database itself. Starting from these preliminary considerations, this paper analyzes the growing use of AI in criminal proceedings, with particular reference to facial recognition technologies, focusing on its main investigative applications within national and EU legislations

Keywords

intelligenza artificiale – riconoscimento facciale – indagini preliminari – Prüm II – giustizia penale

Tra Neuromanti e pecore elettriche: Metaverso e tutela dei dati personali e della *privacy*[*]

Alessandro Rosanò

Sommario

1. Introduzione. – 2. Cenni sul dibattito relativo al rapporto tra neuroscienze e diritto e sugli esiti normativi a cui ha finora condotto. – 3. Cenni su caratteristiche e funzionamento del Metaverso e sui problemi relativi alla protezione dei dati personali e alla tutela della *privacy* nel Metaverso. – 4. Considerazioni sulla protezione dei dati personali nel Metaverso. – 5. Considerazioni sulla tutela della *privacy* nel Metaverso. – 6. Conclusioni.

1. Introduzione

«*For decades, technologists have dreamed of an era when our virtual lives play as important a role as our physical realities. In theory, we would spend lots of time interacting with our friends and colleagues in virtual space. As a result, we would spend money there, too, on outfits and objects for our digital avatars*»[1].

Sembra che quell'epoca a lungo immaginata sia prossima a diventare la nostra realtà grazie allo sviluppo e alla diffusione del Metaverso. La parola richiede preliminarmente un chiarimento semantico. Infatti, è possibile ormai parlare di metaversi, al plurale, visto che ne esistono circa centocinquanta, anche se non tutti sono *Metaverse Ready*, ossia liberamente accessibili, persistenti ed economicamente attivi[2]. L'insieme dei metaversi dà luogo al Metaverso quale piattaforma che integra molteplici tecnologie, come intelligenza artificiale, tecnologia interattiva, *cloud computing* ed *edge computing*, 5G, 6G, Internet delle cose, *blockchain*[3], ha le caratteristiche della socialità e, essendo un mondo virtuale, parallelo e strettamente correlato a

[*] L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

[1] B.X. Chen, *What's All the Hype About the Metaverse?*, in *New York Times*, 18 gennaio 2022, disponibile *online*.

[2] L. Tremolada, *Metaverso, esistono 141 mondi virtuali ma gli investitori puntano sui soliti tre*, in *Il Sole 24ore*, 10 gennaio 2023, disponibile *online*, il quale rinvia a uno studio dell'Osservatorio Realtà Aumentata e Metaverso della School of Management del Politecnico di Milano. Si chiarirà *infra* cosa si intende quando si afferma che un metaverso, per essere *Metaverse Ready*, deve essere persistente ed economicamente attivo.

[3] R. Moro Visconti – A. Cesaretti, *Il metaverso tra realtà digitale e aumentata: innovazione tecnologica e catena del valore*, in *Diritto di Internet*, 3 2022, 627 ss.

quello reale, ha altresì quelle dell'iper-spazialità[4].
In termini generali, si può dire che si tratta di un immenso parco giochi virtuale da esplorare[5], una distesa di spazio digitale fondato sulla connessione sociale, un ambiente ipotetico sintetico legato al mondo fisico[6], una tecnologia immersiva che supera la logica binaria reale-virtuale e proietta l'utente in una realtà in cui il confine tra corporeo e incorporeo diviene labile[7], un «*mundus novus* digitale, uno spazio virtuale collettivo condiviso, creato dalla convergenza di una realtà virtuale immersiva e di una realtà fisica migliorata virtualmente», il cui obiettivo pare essere quello di sostituire una parte significativa della realtà analogica con quella digitale[8]. Si capisce, allora, perché Mark Zuckerberg l'abbia definito il Sacro Graal dell'interazione sociale[9] e si può aggiungere che così arriva a realizzarsi l'idea di una continua interazione tra realtà materiale e realtà virtuale in relazione a cui Floridi ha coniato il termine *onlife*[10]. Dal punto di vista del diritto dell'Unione europea, in maniera molto meno prosaica, può parlarsi del Metaverso come di un servizio della società dell'informazione, visto che è prestato a distanza, per via elettronica e a richiesta individuale di un destinatario[11].
Lasciando da parte per ora gli aspetti definitori, ciò che preme porre in evidenza è che il Metaverso è realtà. *Meta Horizon*, *Decentraland*, *The Sandbox*, *Anyland* e *Roblox* sono solo alcuni degli esempi che si possono fare[12], i quali fanno presagire uno sviluppo importante dell'economia digitale. Secondo alcune ricerche, il mercato del Metaverso varrà più di 750 miliardi di dollari nel 2026[13], mentre, stando ad altre, il valore dovrebbe arrivare a superare il trilione in un futuro non meglio determinato[14].

---

[4] H. Ning et al, *A Survey on Metaverse: the State-of-the-art. Technologies, Applications, and Challenges*, in *arxiv*, 2021, 12-15.

[5] Q. Terry – S. Keeney, *Metaverso. Guida all'uso*, Milano, 2023, 1.

[6] R. Moro Visconti – A. Cesaretti, *Il metaverso tra realtà digitale e aumentata*, cit., 627. Si veda anche B. Cantley – G. Dietrich, *The metaverse: virtual world with real world legal consequences*, in *Rutgers Computer and Technology Law Journal*, 1, 2022, 3.

[7] A. Donini – M. Novella – M.L. Vallauri, *Prime riflessioni sul lavoro nel metaverso*, in *Labour&Law Issues*, 2, 2022, III.

[8] G. Cerrina Ferroni, *Il metaverso tra problemi epistemologici, etici e giuridici*, in questa *Rivista*, 1, 2023, 3, 7.

[9] C. Newton, *Mark in the metaverse. Facebook's CEO on why the social network is becoming 'a metaverse company'*, in *The Verge*, 22 luglio 2021, disponibile *online*.

[10] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

[11] Si consideri l'art. 1, par. 1, lett. b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015 che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione. A tale definizione fa rinvio anche il regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (cosiddetto regolamento sui servizi digitali o *Digital Services Act*).

[12] Per un primo elenco, V. Cosenza, *La mappa del metaverso*, in *Osservatorio Metaverso*, 29 luglio 2022, disponibile *online*.

[13] *Global Metaverse Market to Reach US$758.6 Billion by the Year 2026*, in *GlobeNewswire*, 22 febbraio 2022, disponibile *online*.

[14] D. Grider, *The Metaverse*, in *Gray Scale*, 24 novembre 2021, disponibile *online*.

Si comprende allora perché l'Unione europea abbia manifestato interesse per la materia. Nel programma di lavoro per il 2023, la Commissione europea ha affermato di volere proporre strumenti per lo sviluppo di mondi virtuali aperti antropocentrici, come i metaversi, i quali offrono una miriade di possibilità per le industrie e i settori dei servizi, le arti creative e i cittadini[15]. Lo stesso anno, nell'iniziativa dell'Unione sul web 4.0, l'esecutivo europeo ha messo in risalto il fatto che i mondi virtuali avrebbero rappresentato un aspetto importante del decennio digitale europeo, arrivando a incidere sul modo in cui le persone vivono, lavorano e creano e le imprese operano, innovano, producono e interagiscono con i clienti[16].

Dunque, anche con riferimento a tale profilo, l'Unione europea dovrebbe fare propria l'esigenza di promuovere l'evoluzione tecnologica, così da migliorare il benessere delle persone e della società e la competitività dell'industria europea, fermo però il rispetto dovuto ai valori sui quali poggia il processo di integrazione europea, *in primis* per quel che riguarda la tutela dei diritti fondamentali[17]. Sul punto, ancorché *en passant*, merita ricordare la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, proclamata solennemente dal Parlamento europeo, dal Consiglio dell'Unione e dalla Commissione europea agli inizi del 2023 con lo scopo di specificare «come si dovrebbero applicare nell'ambiente digitale i suoi valori e diritti fondamentali applicabili *offline*»[18] e ricordare «i diritti più pertinenti nel contesto della trasformazione digitale»[19]. In tale documento si sottolinea l'esigenza di mettere le persone al centro della trasformazione suddetta, di assicurare solidarietà e inclusione, di garantire libertà di scelta, partecipazione allo spazio pubblico digitale, sicurezza e sostenibilità. Si tratta di un modo attraverso cui si è cercato di dare una prima risposta alle sfide derivanti dall'evoluzione tecnologica e al fatto che lo strumentario a disposizione dell'Unione per proteggere i diritti incontra difficoltà nello stare al passo con il progresso[20]. Indubbiamente, tale risposta ha valore meramente programmatico, non giuridicamente vincolante e, perciò, carente di meccanismi di implementazione[21]. Si capisce così chi ha espresso una posizione critica al riguardo, affermando che è ben difficile immaginare come la Dichiarazione possa influenzare l'interpretazione e

[15] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Programma di lavoro della Commissione per il 2023. Un'Unione salda e unita*, COM(2022) 548 final, 7.

[16] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Un'iniziativa dell'UE sul web 4.0 e i mondi virtuali: muoversi in anticipo verso la prossima transizione tecnologica*, COM(2023) 442 final, 1.

[17] A. Adinolfi, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE*, 14 marzo 2023, 322-323.

[18] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, considerando 3.

[19] Ivi, considerando 7.

[20] P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *Osservatorio europeo*, marzo 2022, 1.

[21] L. Cianci, *Dichiarazione europea sui diritti e i principi digitali: quid pluris?*, in *Diritto pubblico comparato ed europeo*, 2, 2022, 381.

l'applicazione del diritto dell'Unione[22]. Al tempo stesso, però, si condivide l'opinione di chi ritiene che essa individui nient'altro che nuove declinazioni di fattispecie di diritti che già formano oggetto di tutela nella Carta dei diritti fondamentali[23].

Dunque, il tema diventa non tanto individuare nuove figure di diritti, ma permettere a quelle già esistenti di manifestare la loro portata anche nell'ambito della trasformazione digitale[24], eventualmente attraverso un'opera di interpretazione estensiva ove non si sia (ancora) proceduto, attraverso atti di diritto derivato, a introdurre strumenti di regolazione delle nuove tecnologie che permettano di assicurare il rispetto dei diritti fondamentali grazie a standard di protezione omogenei[25].

Il Metaverso sembra offrire una simile opportunità per il giurista. In realtà, le sfide poste sul piano giuridico da questa nuova realtà sono innumerevoli: basti considerare, oltre a quello della natura giuridica del Metaverso stesso, i temi della legge applicabile e del foro competente[26], della tutela

---

[22] E. Quinn, *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *verfassungsblog.de*, 22 dicembre 2022.

[23] A. Adinolfi, *Evoluzione tecnologica e tutela dei diritti fondamentali*, cit., 331.

[24] Come ha detto la Commissione europea, si tratta di rendere la Carta dei diritti fondamentali efficace nell'era digitale (Relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Tutela dei diritti fondamentali nell'era digitale - Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea*, COM(2021) 819 final, 39).

[25] A. Adinolfi, *Evoluzione tecnologica e tutela dei diritti fondamentali*, cit., 342 e C. Amalfitano – F. Ferri, *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*, Torino, 2023, 22.

[26] Va detto che le problematiche di natura giuridica che riguardano il Metaverso si ricollegano in primo luogo all'assenza di uno Stato; dunque, alla carenza di un elemento territoriale; dunque, alla difficoltà di individuare la disciplina applicabile e alla possibile deresponsabilizzazione che ne potrebbe derivare (M.C. De Vivo, *Viaggio nei metaversi alla ricerca del diritto perduto*, in *Informatica e diritto*, 1, 2009, 191 ss.). Si ripropongono allora le questioni già emerse con riferimento a Internet e al dibattito tra chi riteneva che, trattandosi di un fenomeno globale e di uno spazio senza confini, sarebbe stato impossibile e/o sbagliato imporre leggi nazionali (si vedano per esempio D. Wisebrod, *Controlling the Uncontrollable: Regulating the Internet*, in *Media and Communications Law Review*, 4, 1995, 331 ss. e D.R. Johnson – D. Post, *Law and Borders – The Rise of Cyberspace*, in *Stanford Law Review*, 5, 1996, 1367 ss.) e chi invece reputava che applicare il diritto a Internet comporta lo stesso tipo di operazione che si ricollega all'applicazione di norme giuridiche a una qualsiasi nuova realtà: si procede per analogie e si ricorre alla normativa esistente, in attesa che una specifica venga elaborata (*ex multis*, J.H. Sommer, *Against Cyberlaw*, in *Berkeley Technology Law Journal*, 3, 2000, 1145 ss.; per una panoramica su questi temi, J. Kulesza, *International Internet Law*, London, 2012 e G.M. Ruotolo, *Internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012, 28 ss.). Che sia prevalsa quest'ultima soluzione è cosa nota: le corti nazionali affermano la sussistenza della loro giurisdizione nei confronti di soggetti che operano su scala globale e applicano il diritto interno ai casi transfrontalieri, trattando le controversie sorte in Internet come se si trattasse di controversie del mondo reale (A. Savin, *EU Internet Law*, III ed., Cheltenham-Northampton, 2020, 88). Anche nel caso del Metaverso sono emerse due posizioni contrapposte. Vi è chi sostiene che le interazioni che hanno luogo nel Metaverso avvengono nell'ambito di un rapporto di natura contrattuale tra piattaforma e utente e, quindi, i termini di servizio sono il punto di riferimento di cui tenere conto (J.M. Garon, *Legal Implications of a Ubiquitous Metaverse and a Web3 Future*, in *Marquette Law Review*, 1, 2022, 185, 187) e chi invece asserisce che, per quanto il *software* e i dati – ossia, gli strati virtuali del Metaverso e, in generale, del cyberspazio – svolgano un

della proprietà intellettuale, della responsabilità penale[27]. Quella attinente alla protezione dei diritti fondamentali degli utenti del Metaverso è tra le principali, visto che, come è stato sostenuto, «l'opera della costruzione delle macchine è elevata espressione della capacità umana di riplasmare il dato a misura d'uomo [...] e nel contempo, proprio con questa creazione, viene messa al mondo una nuova entità, un nuovo processo che, in modo definitivo e prima inimmaginabile, espone l'uomo a una eterodeterminazione per mezzo di ciò che ha creato»[28].

Nel presente articolo si intende affrontare la questione della tutela dei dati personali e della *privacy* nel Metaverso[29]. Per farlo, si reputa necessario trarre alcuni spunti dal fecondo dibattito in atto sul rapporto tra neuroscienze e diritto, visto che in tale ambito sono emerse indicazioni importanti per quel che riguarda la protezione dei diritti. Pertanto, dopo avere offerto una panoramica sul tema ora menzionato (paragrafo 2), si delineano gli aspetti relativi alle caratteristiche e al funzionamento del Metaverso e le

---

ruolo significativo nel permettere al Metaverso di operare, l'*input*, l'elaborazione e l'*output* dei dati medesimi dipendono da un substrato fisico, da componenti *hardware* quali cavi, satelliti, onde radio, computer e milioni di circuiti al silicio, tutti situati da qualche parte nel mondo reale, con la conseguenza che il Metaverso, come Internet, risulta radicato in infrastrutture fisiche tangibili (D. Akande – A. Coco – T. de Souza Dias, *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies*, in *International Law Studies*, 4, 2022, 22). Come è stato detto in relazione al cyberspazio, questo è «*nothing but a metaphor to express simulated spaces or experiences, such as online gaming, dating, or social media (…) just as global transportation networks do not give rise to a new "world" or "domain," so does cyberspace not constitute a new "space"*» (ivi, 21).

[27] Per un'introduzione quanto ai profili ora citati, I.O. Epicoco – M. Pierro – F. Sarzana Di Sant'Ippolito, *Il diritto del metaverso. NFT, DeFi, GameFi e privacy*, Torino, 2022 e G. Cassano – G. Scorza (a cura di), *Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT*, Pisa, 2023.

[28] H. Popitz, *Verso una società artificiale*, Roma, 1996, 23.

[29] Evidentemente, non è questa la sede in cui affrontare l'annoso tema del rapporto e della differenza tra protezione dei dati personali e *privacy*. Come è stato detto, al pari di Pallade Atena, scaturita già adulta e armata dalla testa di Zeus, così la prima è derivata dalla seconda (l'immagine è tratta da M. Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right*, in *International Data Privacy Law*, 1, 2013, 88 ss.). Il dibattito sul tema è stato ampio: si vedano per esempio D.H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, in *Case Western Reserve Law Review*, 3, 1991, 831 ss.; M. Froomkin, *The Death of Privacy?*, in *Stanford Law Review*, 5, 2000, 1461 ss.; P. de Hert – S. Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in A. Duff – S. Gutwirth (eds), *Privacy and the criminal law*, Cambridge, 2006, 61 ss.; N. Nuno Comes de Andrade, *Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights*, in S. Fischer-Hübner et al (eds), *Privacy and Identity Management for Life*, Berlin-Heidelberg, 2011, 90 ss.; J. Kokott – C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 4, 2013, 222 ss.; O. Lynskey, *Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order*, in *International & Comparative Law Quarterly*, 3, 2015, 590 ss.; A. Forde, *The Conceptual Relationship between Privacy and Data Protection*, in *Cambridge Law Review*, 1, 2016, 135 ss. Si condivide comunque la tesi avanzata dai già citati de Hert e Gutwirth, secondo i quali *privacy* e tutela dei dati svolgono ruoli fondamentali distinti, eppure complementari. Infatti, la prima assolve a una funzione di opacità, impedendo l'invasione sproporzionata della sfera privata dell'individuo da parte di terzi, mentre della seconda è propria una funzione di trasparenza, ossia di definizione delle regole che rendono ammissibile il trattamento dei dati, in particolare per imporre obblighi al responsabile del trattamento.

sfide poste da questa nuova realtà per i dati personali e il diritto alla *privacy* (paragrafo 3). In seguito, si svolgono alcune considerazioni relative alle modalità attraverso cui assicurare la protezione dei dati personali (paragrafo 4) e della *privacy* nel Metaverso (paragrafo 5) assumendo il punto di vista del diritto dell'Unione europea e, ove necessario, della Convenzione europea sui diritti dell'uomo (CEDU). Le conclusioni riassumono l'analisi svolta in questa sede (paragrafo 6).

2. Cenni sul dibattito relativo al rapporto tra neuroscienze e diritto e sugli esiti normativi a cui ha finora condotto

È stato detto che neuroscienze e diritto sono partner naturali[30]. Probabilmente, l'affermazione vale per ogni campo del sapere e dell'esistenza umana, in relazione al quale si impone l'elaborazione di regole giuridiche che ne rendano lo sviluppo coerente con i fondamenti dell'ordinamento considerato. A prescindere da questo, però, non si può negare che negli ultimi decenni l'attenzione del diritto nei confronti delle neuroscienze sia andata significativamente aumentando, in ragione dell'esigenza di fornire un'elaborazione normativa concernente le scoperte neuroscientifiche, ossia di arrivare a una più adeguata regolamentazione e valutazione dei comportamenti umani grazie alla migliore comprensione che le neuroscienze forniscono degli stessi, nonché dell'esigenza di disciplinare le sperimentazioni realizzate e l'utilizzo dei dati ottenuti di conseguenza in maniera non distonica con il rispetto della dignità umana e dei diritti fondamentali dell'individuo[31]. L'applicazione in campo tecnologico delle risultanze delle neuroscienze va a complicare ulteriormente tale panorama. Le neurotecnologie, infatti, non sono più confinate agli ambiti della ricerca clinica e biomedica. Anzi, si è assistito negli ultimi due decenni alla proliferazione delle cosiddette *consumer neuro-technologies*, dette anche neurotecnologie non invasive, le quali registrano l'attività fisiologica dell'organismo umano e, in particolare, l'attività elettrica del cervello, principalmente tramite elettroencefalografia[32]. Progressivamente, sono state elaborate interfacce neurali (in inglese, *Brain Machine Interfaces*, spesso indicate con l'acronimo BMI), che permettono a sistemi di intelligenza artificiale di entrare in dialogo con il cervello umano, acquisendo i segnali neurali, elaborandoli e trasformandoli in *output*, tanto che risulta possibile registrare un brano musicale estraendolo dalle onde cerebrali di chi lo pensa[33]. A questo si aggiungono tecniche di controllo a distanza, di connessione di cervelli e di *network* di

[30] O. Goodenough – M. Tucker, *Law and Cognitive Neuroscience*, in *Annual Review of Law and Social Science*, 1, 2010, 62.

[31] M.C. Errigo, *Neuroscienze, tecnologia e diritti: problemi nuovi e ipotesi di tutela*, in *dirittifondamentali.it*, 3, 2020, 216.

[32] M. Ienca, *Neurodiritti: storia di un concetto e scenari futuri*, in *Privacy e neurodiritti La persona al tempo delle neuroscienze*, 2021, 37-41, disponibile *online*.

[33] U. Ruffolo – A. Amidei, *Diritto dell'Intelligenza Artificiale. Volume II*, Roma, 2024, 226-227.

cervelli, che prefigurano la realizzazione di forme di sorveglianza di massa e di controllo sociale, oltre che di profilazione estremamente avanzata[34].
Si comprende allora perché si parli ormai da tempo di neurodiritto (in inglese, *neurolaw*) per riferirsi a un settore di ricerca che deriva dall'integrazione tra i due campi del sapere[35], la cui giustificazione di fondo è evidentemente quella di porre dei limiti[36].
Il motivo è di facile comprensione. L'attività neurale può essere identificata come il substrato critico dell'identità di una persona[37]. Le neurotecnologie non possono leggere la mente, ma permettono di fare inferenze accurate su stati mentali, pensieri e processi cognitivi ed emotivi. Si pensi al *brain imaging*, ossia all'insieme delle tecniche, quali risonanza magnetica funzionale, tomografia a emissione di positroni ed elettroencefalogramma[38], attraverso cui si può realizzare la mappatura della struttura, della funzione e della farmacologia del sistema nervoso. I dati che possono essere raccolti mediante tali modalità, qualificabili come dati neurali, sono estremamente rilevanti per l'individuo perché possono rivelare informazioni non note all'individuo stesso o che si collocano al di fuori del suo controllo o che, ancora, possono essere usate a fini predittivi, cioè per individuare caratteristiche o predisposizioni che non solo non sono conosciute dal singolo, ma che in realtà potrebbero non arrivare mai a manifestarsi[39]. Non solo: alcune informazioni, come per esempio i segnali registrati dall'elettroencefalogramma, possono essere utilizzati come identificatori biometrici univoci, al pari delle impronte digitali o del DNA[40]. Ne deriva che la lettura dell'attività neurale può avere ripercussioni sull'identità dell'individuo e dunque erodere «l'ultimo territorio inaccessibile» dell'informazione privata[41].
Se si pone attenzione alla diffusione delle *consumer neuro-technologies*, si com-

---

[34] *Ibidem*.

[35] A. D'Aloia, *Neuroscienze e diritto. Appunti preliminari*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2017, 1. Per i necessari approfondimenti, F.X. Shen, *The Overlooked History of Neurolaw*, in *Fordham Law Review*, 2, 2016, 667 ss. e A. D'Aloia – M.C. Errigo (eds), *Neuroscience and Law. Complicated Crossings and New Perspectives*, Cham, 2020.

[36] Per una panoramica, S.K Erickson, *The Limits of Neurolaw*, in *Houston Journal of Health Law & Policy*, 2, 2011, 303 ss.; A.J. Kolber, *Will There Be a Neurolaw Revolution*, in *Indiana Law Journal*, 2, 2014, 807 ss.; D.W. Opderbeck, *The Problem with Neurolaw*, in *Saint Louis University Law Journal*, 2, 2014, 497 ss.; E. Picozza (ed.), *Neurolaw. An Introduction*, Cham-Torino, 2016; G.D. Caruso, *Neurolaw*, Cambridge, 2024; F. Cirillo, *Neurolaw, Neurorights and Neuroprivacy: Theoretical and Constitutional Issues*, in questa *Rivista*, numero speciale I-2024, 212 ss.

[37] M. Ienca, *Tra cervelli e macchine: riflessioni su neurotecnologie e su neurodiritti*, in *Notizie di Politeia*, 133, 2019, 56.

[38] G. D'Alessandro – F. Cirillo, *Neurodiritti: prospettive critiche e questioni dogmatiche*, in R. Torino – S. Zorzetto (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023, 106.

[39] D. Hallinan et al, *Neurodata and Neuroprivacy: Data Protection Outdated?*, in *Surveillance & Society*, 1, 2014, 55, 65.

[40] M. Ienca – R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sciences Society and Policy*, 1, 2017, 13. Si tornerà sul tema *infra*.

[41] M. Ienca, *Tra cervelli e macchine*, cit., 56. Si veda anche S. Ligthart et al, *Minding Rights: Mapping Ethical and Legal Foundations of 'Neurorights'*, in *Cambridge Quarterly of Healthcare Ethics*, 4, 2023, 467.

prende quale sia la questione di fondo che il diritto deve affrontare e, auspicabilmente, risolvere. Il ruolo centrale assunto da soggetti privati nel campo tecnologico fa sì che siano queste le entità da cui possono venire le minacce più serie ai diritti fondamentali, e non i governi com'era in passato, con la conseguenza che al diritto non spetta più – almeno, primariamente – il compito di promuovere la competizione tra privati, bensì di limitare il potere digitale di questi ultimi[42]. Perciò, si capisce perché sia emersa la categoria dei neurodiritti, ossia diritti specificamente previsti con lo scopo di tutelare l'individuo dai rischi che derivano da usi dannosi delle neurotecnologie[43], situazioni giuridiche soggettive di vantaggio correlate all'impiego dei nuovi strumenti offerti dalle neuroscienze[44], tramite le quali assicurare l'integrità della sfera di autodeterminazione e la libertà di conoscenza e di giudizio del singolo[45], che dovrebbero configurarsi come specificazioni non meramente ripetitive di diritti già esistenti, intese a proteggere il dominio mentale e neurale della persona[46].

Il dibattito al riguardo è risultato particolarmente fecondo[47]. Secondo una delle teorie più diffuse, formulata da Ienca e Andorno, i neurodiritti sarebbero quattro: il diritto alla libertà cognitiva, che comprenderebbe sia il diritto a utilizzare le neurotecnologie, sia la protezione dall'utilizzo coercitivo e senza consenso di tali tecnologie nei confronti dell'individuo; il diritto alla *privacy* mentale, il quale mirerebbe a tutelare le persone dall'accesso illecito alle informazioni presenti nel loro cervello e a prevenire la diffusione indiscriminata di tali dati nell'infosfera; il diritto all'integrità mentale, inteso in questo caso non con riferimento alla tutela della salute mentale dell'individuo, ma alla protezione della sfera mentale da danni potenziali; e il diritto alla continuità psicologica, che preserverebbe l'identità personale e la coerenza del comportamento dell'individuo rispetto a modifiche non concordate, apportate da terzi[48]. Parzialmente diversa è la tesi avanzata dalla *Neurorights Foundation*, istituita presso la Columbia University, secondo cui i neurodiritti dovrebbero essere cinque: il diritto all'identità personale, tramite cui impedire alle neurotecnologie di alterare

---

[42] G. De Minico, *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti*, in *federalismi.it*, 15 marzo 2024, 3-5, 15.

[43] J.M. Munoz – J.Á. Marinaro, *Neurorights as reconceptualized human rights*, in *Frontiers in Political Science*, 2023, 01.

[44] M.R. Anglani, *Neurolaw: l'incidenza delle neuroscienze sugli standard del processo penale e sulla «libertà morale della persona»*, in *federalismi.it*, 15 marzo 2024, 49.

[45] M. D'Angelosante, *Accelerare la Nottola di Minerva? IA, diritto e (neuro-)diritti*, in *federalismi.it*, 15 marzo 2024, 92-94.

[46] M. Ienca, *On Neurorights*, in *Frontiers in Human Neuroscience*, 15, 2021, 9.

[47] Per un'introduzione, J.S. Taylor – J.A. Har – T. Elliott, *Neuropsychologists and Neurolawyers*, in *Neuropsychology*, 4, 1991, 293 ss.; A. Roskies, *Neuroethics for the New Millenium*, in *Neuron*, 1, 2002, 21 ss.; J.-C. Bublitz, *My Mind is Mine!? Cognitive Liberty as a Legal Concept*, in E. Hildt – A. Francke (eds), *Cognitive Enhancement*, Cham, 2013, 233 ss.; J. Cascio, *Do brains need rights?*, in *New Scientist*, 2017, 24 ss.; N. Hertz, *Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought*, in *Neuroethics*, 2023, 4 ss.; R. Yuste – T. de la Quadra-Salcedo, *Neuro-rights and new charts of digital rights: dialogue beyond the limits of the law*, in *Indiana Journal of Global Legal Studies*, 1, 2023, 15 ss.

[48] M. Ienca, R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, cit., 1 ss.

il senso del sé individuale; il diritto al libero arbitrio, così da garantire che l'individuo mantenga il controllo sulle proprie decisioni, senza subire manipolazioni delle quali non sia consapevole; il diritto alla *privacy* mentale, sostanzialmente identico a quello identificato in precedenza; il diritto alla parità di accesso al potenziamento mentale; e il diritto alla protezione contro le discriminazioni algoritmiche[49].

Con riferimento alla loro tesi, Ienca e Andorno reputano che non si sarebbe in presenza di un fenomeno di *rights inflation*, in quanto le fattispecie identificate rispecchierebbero un valore sociale di particolare rilievo[50]. Un profilo che merita di essere preso in considerazione è proprio questo. Fermo il fatto che esiste un gap di tutela che deve essere colmato, è legittimo chiedersi se la risposta vada cercata nell'elaborazione di nuovi diritti o non piuttosto in un'interpretazione evolutiva di fattispecie già definite[51], posto che «le fondamenta giuridiche dei neurodiritti potrebbero essere già presenti (quasi profeticamente) nelle Carte esistenti»[52]. Quindi, si tratterebbe di riaffermare e rafforzare diritti consolidati[53].

Allo stato attuale, si individuano almeno due casi in cui si è arrivati alla previsione *per tabulas* di nuovi diritti: quelli del Cile e del Colorado. Alla fine del 2021, il Cile è diventato il primo Stato al mondo ad affrontare il tema dei neurodiritti nel proprio testo costituzionale[54], riformato al fine di prevedere che lo sviluppo scientifico e tecnologico sia al servizio dell'uomo e ne rispetti l'integrità fisica e mentale e che la legge debba in particolare proteggere l'attività cerebrale e le informazioni a essa correlate (art. 19). L'iniziativa è di sicuro interesse, visto che identifica nell'essere umano il fine della scienza e della tecnologia, impone l'introduzione di una disciplina funzionale a proteggere l'individuo dalle nuove tecnologie e riconosce il diritto all'integrità e alla *privacy* mentale[55]. A partire da questo cambiamento, nel 2023 si è registrata un'importante pronuncia resa dalla Corte suprema cilena, che ha ritenuto che una società americana che commercializzava un dispositivo *wireless* in grado di monitorare le prestazioni cognitive, compresi i livelli di attenzione o di stress, e di raccogliere informazioni sull'attività elettrica del cervello avesse violato il nuovo precetto costituzionale, con la conseguenza che è stato imposto alla società in questione di cancellare i dati acquisiti e alle autorità sanitarie e doganali nazionali di valutare la conformità del dispositivo rispetto alle normative vigenti[56]. Si segnala altresì un progetto di legge sulla tutela dei neurodiritti e dell'integrità mentale e

[49] Si veda *neurorightsfoundation.org/mission*.

[50] M. Ienca – R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, cit., 7-9.

[51] M.C. Errigo, *Neuroscienze, tecnologia e diritti*, cit., 240.

[52] O. Pollicino, *Costituzionalismo, privacy e neurodiritti*, in questa *Rivista*, 2, 2021, 12.

[53] S. Lighthart – C. Bublitz – S. Alegre, *Neurotechnology: we need new laws, not new rights*, in *Nature*, 29 agosto 2023, 950.

[54] A. McCay, *Neurorights: the Chilean constitutional change*, in *AI & Society*, 39, 2024, 797.

[55] C. Amunategui Perello, *Neurorights: The World's First Court Case*, in *Intellectual Property and Technology Law Journal*, 1, 2024, 129.

[56] Per i necessari riferimenti, si veda l'articolo citato nella nota precedente.

sullo sviluppo della ricerca e delle neurotecnologie[57].
Quanto al Colorado, in una legge adottata nel 2024 si afferma che le tecnologie che raccolgono dati sulle funzioni corporee e mentali dell'utente stanno trasformando il volume e la sensibilità dei dati personali. I dispositivi in grado, tra l'altro, di registrare e interpretare la risposta del sistema nervoso centrale o periferico di un individuo all'ambiente interno o esterno sono sempre più diffusi e pongono problemi pressanti. Viene pertanto introdotta la nozione di dato neurale, inteso come qualsiasi informazione generata dalla misurazione dell'attività del sistema nervoso centrale o periferico di un individuo e che può essere elaborata da o con l'assistenza di un dispositivo, estendendo così l'ambito di applicazione del *Colorado Privacy Act* in ragione del fatto che ogni cervello umano è unico, che quindi i dati neurali sono specifici dell'individuo da cui sono stati raccolti e che tali dati possono rivelare informazioni sulla salute, sugli stati mentali, sulle emozioni e sul funzionamento cognitivo di quell'individuo. In particolare, viene evidenziato che la raccolta di dati neurali comporta sempre la divulgazione involontaria di informazioni e che, anche se le persone acconsentono alla raccolta e al trattamento dei loro dati per un uso limitato, è improbabile che siano pienamente consapevoli del contenuto o della quantità di informazioni che stanno condividendo[58].
En passant, si fa presente che in Ecuador è in discussione un progetto di *ley orgánica* sulla neuroprotezione e l'applicazione etica delle neurotecnologie[59] e che in Spagna è stato adottato un atto non vincolante, denominato Carta dei diritti digitali, che individua 27 diritti rilevanti per l'individuo nel mondo non analogico, tra i quali figura il diritto all'identità personale nel contesto digitale[60].
Infine, nel contesto delle organizzazioni internazionali, si ricorda che sia l'OCSE, sia l'UNESCO hanno incoraggiato gli Stati a introdurre forme di tutela dei neurodiritti[61], e che lo stesso ha fatto il Parlamento europeo con riferimento alla Commissione europea, invitandola a «considerare un'iniziativa sui neurodiritti con l'obiettivo di proteggere il cervello umano da interferenze, manipolazioni e controlli da parte della neurotecnologia basata sull'intelligenza artificiale»[62].

[57] Riguardo all'*iter*, si v. il sito *camara.cl*.

[58] *House Bill 24-1058 Concerning Protecting the Privacy of Individuals' Biological Data, and, in connection therewith, Protecting the Privacy of Neural Data and Expanding the Scope of the Colorado Privacy Act accordingly*, disponibile *online*.

[59] Disponibile online.

[60] Disponibile online.

[61] OCSE, *Recommendation on Responsible Innovation in Neurotechnology*, 11 dicembre 2019, punto 7 e UNESCO, *Report of the International Bioethics Committee of UNESCO (IBC) on ethical issues of neurotechnology*, SHS/BIO/IBC-28/2021/3, punto 190.

[62] Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale (2020/2266(INI), punto 247.

3. Cenni su caratteristiche e funzionamento del Metaverso e sui problemi relativi alla protezione dei dati personali e alla tutela della *privacy* nel Metaverso

Agli inizi degli anni Novanta del secolo scorso, vi è stato chi, osservando gli sviluppi tecnologici e scientifici, ha avanzato l'idea dell'*ubiquitous computing*, ossia di computer integrati nell'ambiente circostante, i quali avrebbero portato alla realizzazione di una *embodied virtuality*, una virtualità incarnata resa possibile da connessioni *wireless*, *touch-screen* e nuovi *software*[63]. È in effetti in quel periodo che cominciano a diffondersi tecnologie sempre più pervasive, che permettono di realizzare interazioni senza soluzione di continuità in contesti ben determinati, quali uffici e case[64].

Il Metaverso sembra configurarsi allora come la prosecuzione di quegli sviluppi. Volendo andare oltre le definizioni di ordine generale date *supra*, si può sostenere che il Metaverso è «una rete di massima scalabilità e interoperabile di mondi virtuali 3D renderizzati in tempo reale, che possono essere vissuti in modo sincrono e persistente da un numero effettivamente illimitato di utenti con un senso individuale di presenza al loro interno, e che garantiscono la continuità dei dati relativi a identità, storia, diritti, oggetti, comunicazioni e pagamenti»[65]. Scomponendo la definizione nei suoi singoli elementi, i mondi virtuali sono ambienti simulati generati da computer, di natura ludica o non ludica; tali mondi sono realizzati in 3D perché la tridimensionalità determina un modello di interazione intuitivo per gli esseri umani e più fedele al mondo reale; il *rendering* è il processo che porta a generare un oggetto o un ambiente usando un programma per il computer e il *rendering* in tempo reale è funzionale alla creazione di un mondo virtuale vivo, in grado di rispondere agli *input* dell'utente; l'interoperabilità permette di scambiare le informazioni relative a quanto accaduto in un mondo virtuale con gli altri mondi virtuali; la scalabilità sta a indicare la capacità di ospitare un numero potenzialmente infinito di mondi virtuali; la sincronia attiene alla possibilità di condividere esperienze con altri utenti; la persistenza riguarda il fatto che i mondi virtuali continuano a esistere e a cambiare a prescindere dal singolo utente[66].

Per una definizione meno articolata, ma comunque in grado di permettere di comprendere le peculiarità del Metaverso, si possono riprendere le indicazioni date dal Consiglio dell'Unione europea, secondo il quale il Metaverso è una realtà persistente, immersiva, massiva, sincrona, digitale e reale, economicamente attiva e interoperabile. È persistente, immersiva e massiva perché esiste e continua a esistere a prescindere dalla presenza degli utenti, sembra davvero esistente e ha l'estensione di un mondo; è sincrona perché permette agli utenti di vivere situazioni in tempo reale; è digitale e reale in quanto le esperienze vissute nel mondo digitale si ri-

[63] M. Weiser, *The Computer for the 21st Century*, in *Scientific American*, 1, 1991, 78.

[64] M. Lombardi, *Il lavoro nel metaverso: uno spazio indefinito del possibile*, in *Labour&Law Issues*, 2, 2022, 29.

[65] M. Ball, *Metaverso*, Milano, 2022, 55.

[66] Ivi, 56 ss.

flettono su quello reale (si pensi all'acquisto, con soldi reali, di un terreno nel Metaverso); è economicamente attiva dato che le persone fisiche e giuridiche che vi operano creano valore; è interoperabile in ragione del fatto che i dati, i contenuti, gli oggetti digitali ottenuti possono essere usati su varie piattaforme, ossia i beni ottenuti in un metaverso possono essere "trasportati" e "utilizzati" in un altro metaverso[67]. L'interoperabilità è resa possibile dalla tecnologia *blockchain*, che crea una struttura sottostante unificante mediante la quale possono essere effettuate tutte le interazioni, comprese quelle commerciali. In assenza di questa, i numerosi mondi virtuali esistenti sarebbero dei compartimenti stagni e l'utente dovrebbe fornire dati personali per accedere a ognuno di essi. Tramite la tecnologia *blockchain*, gli utenti possono interagire e svolgere attività in ogni metaverso senza dover rivelare informazioni riservate a ciascuno[68].

Per avere accesso al Metaverso, è necessario creare un *avatar*, un gemello digitale dell'utente, il quale si muove nell'universo messo a sua disposizione. Serve quindi una duplicazione digitale, però serve altresì una tecnologia che renda possibile l'ingresso e l'interazione nel Metaverso[69]. In realtà,

---

[67] Per queste caratteristiche, Consiglio dell'Unione europea, *Metaverse – Virtual world, real challenges*, 9 marzo 2022, 3, disponibile *online*.

[68] R.L. Pate, *Legal Issues Inside the Unnatural World of Metaverse*, in *Business Law Review*, 5, 2022, 188. Si ricorda *en passant* che una *blockchain* è una sorta di libro mastro, utilizzato per la registrazione di dati, che fa ricorso alla crittografia per rendere difficile la manomissione delle voci presenti nello stesso e che ha un processo concordato per la memorizzazione di una o più copie del libro mastro e per l'aggiunta di nuove voci. Propriamente, la *blockchain* è composta da una serie di blocchi. Ogni blocco contiene i dati relativi a varie transazioni e un'intestazione che include un valore (detto valore di *hash*) per il blocco precedente, che a sua volta presenta un'intestazione che include l'*hash* del blocco precedente, e così via. Qualsiasi tentativo di manomettere i dati in un particolare blocco della catena risulta evidente, visto che l'*hash* dei suoi dati non corrisponderà più all'*hash* del blocco successivo, con la conseguenza che la catena viene interrotta (così C. Millard, *Blockchain and law: Incompatible codes?*, in *Computer Law & Security Review*, 4, 2018, 844; ulteriormente, D. Szostek, *Blockchain and the Law*, Baden-Baden, 2019, 34 ss.). La *blockchain*, dunque, può essere definita come «un *database* distribuito, condiviso e la cui storia passata è inalterabile» (G. Zaccaroni, *Le Roi est Mort, Vive le Roi! La blockchain nel diritto dell'Unione europea*, in *I Post di AISDUE*, 18 gennaio 2022, 250), la cui integrità è garantita dal consenso dei partecipanti (M. Finck, *Blockchains: Regulating the Unknown*, in *German Law Journal*, 4, 2018, 668). Propriamente, metodi crittografici consentono di ottenere un consenso matematico per confermare la coerenza del record digitale di ogni transazione, il quale viene registrato in modo permanente sul database, impedendone l'alterazione o la cancellazione (K. Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law*, in *Modern Law Review*, 2, 2019, 207 ss.). Finora, l'innovazione più dirompente determinata dalla tecnologia *blockchain* è rappresentata dalle criptovalute e, in generale, dalla possibilità di creare unità di valore che circolano su una rete digitale *peer-to-peer* a livello mondiale (V. Ferrari, *The regulation of crypto-assets in the EU – investment and payment tokens under the radar*, in *Maastricht Journal of European and Comparative Law*, 3, 2020, 325; per un'introduzione ai riflessi di natura giuridica del fenomeno, J. Brito – H. Shadab – A. Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, in *Columbia Science & Technology Law Review*, 1, 2014, 144 ss.; E. Hewitt, *Bringing Continuity to Cryptocurrency: Commercial Law as a Guide to the Asset Categorization of Bitcoin*, in *Seattle University Law Review*, 2, 2016, 619 ss.; G. Befani, *Contributo allo studio sulle criptovalute come oggetto di rapporti giuridici*, in *Il diritto dell'economia*, 3, 2019, 379 ss.; E. Avgouleas – A. Seretakis, *How Should Crypto Lending Be Regulated Under EU Law?*, in *European Business Organization Law Review*, 3, 2023, 421 ss.).

[69] Y.K. Dwivedi et al, *Exploring the Darkverse: A Multi-Perspective Analysis of the Negative*

in un primo momento, l'accesso era possibile solamente attraverso computer, ma ormai i dispositivi mobili consentono di fare lo stesso. C'è però un ulteriore aspetto al quale va posta attenzione. Un sistema immersivo deve poter comprendere come l'utente interagisce con il mondo e, per fare questo, deve tenere traccia di ciò che l'utente guarda e per quanto tempo. Per questo, la tecnologia immersiva necessita di *hardware* per l'acquisizione di alcuni segnali, ossia per misurare e registrare i movimenti di varie parti del corpo dell'utente, come la testa che annuisce o gli occhi che sbattono le palpebre, nonché gli stati emotivi o fisiologici attraverso la mappatura dell'attività cerebrale[70].

Allora, deve essere considerato che, in effetti, per accedere al Metaverso è sufficiente un computer o uno *smartphone*. Tuttavia, per godere appieno delle esperienze offerte da questa nuova realtà e, in particolare, per viverla in tre dimensioni, si ricorre a visori che permettono all'utente di avere un'esperienza effettiva dei panorami e dei suoni dell'universo digitale in cui è entrato. I visori utilizzano un sistema di telecamere e sensori per tracciare e rispondere ai movimenti del corpo dell'utente, nonché di realizzare una rappresentazione dell'ambiente in cui egli si trova e monitorare la sua posizione e il contesto in tempo reale con estrema precisione[71].

Allo stato attuale, molti dei visori in commercio presentano sistemi di *eye tracking* e *face tracking*[72]. Sviluppi futuri concernono il ricorso a interfacce cervello-computer (in inglese, *brain-computer interfaces*, o BCI), capaci di estrarre i segnali cerebrali degli utenti e di elaborarli localmente o in remoto attraverso un'unità di calcolo. Il che vuol dire che una BCI potrà attingere alle intenzioni, ai pensieri e agli stati cognitivi dell'utente senza che vi sia bisogno di affidarsi ad azioni fisiche evidenti, come premere i pulsanti di un *controller*, essendo la BCI invece in grado di interpretare gli stati mentali dell'utente[73]. Per quanto i tentativi di arrivare a simili esiti procedano a rilento, sembra che la strada in quella direzione sia tracciata[74]. Parimenti, si sta cercando di integrare meccanismi che permettano di eseguire l'elettromiografia e l'elettrocardiogramma[75].

Giova allora ricordare qui la nozione di psicografia biometrica, introdotta dalla giurista Brittan Heller, che sta a indicare la pratica di usare i dati biometrici per identificare gli interessi di una persona e, quindi, il ricorso

---

Societal Impacts of the Metaverse, in *Information Systems Frontiers*, 2 giugno 2023, 7.

[70] B. Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, in *Vanderbilt Journal of Entertainment & Technology Law*, 1, 2020, 10, 23-24.

[71] Y. Wang et al, *A Survey on Metaverse: Fundamentals, Security, and Privacy*, in *arxiv*, 2022, 16.

[72] Disponibile online.

[73] H.Y. Zhu et al, *A Human-Centric Metaverse Enabled by Brain-Computer Interface: A Survey*, in *IEEE Communications Surveys & Tutorials*, 3, 2024, 2120 ss.

[74] M. Ball, *Metaverso*, cit., 221-222, ove si fa riferimento a sperimentazioni portate avanti da Neuralink e Meta.

[75] Y. Li – L. Zheng – X. Wang, *Flexible and wearable healthcare sensors for visual reality health-monitoring*, in *Virtual Reality & Intelligent Hardware*, 4, 2019, 1 ss.; K. Kim et al, *Metaverse Wearables for Immersive Digital Healthcare: A Review*, in *Advanced Science*, 10 novembre 2023, 2303234 ss.; Y. Shin – M. Lee, *Development of Sensory Virtual Reality Interface Using EMG Signal-Based Grip Strength Reflection System*, in *Applied Sciences*, 11, 2024, 1 ss.

a informazioni corporee per rivelare dettagli intimi su gusti, preferenze e interessi di un soggetto. Attraverso dati comportamentali e anatomici, risulta possibile misurare la reazione di un individuo agli stimoli e così comprendere il suo stato fisico, mentale ed emotivo[76]. Ciò può essere realizzato attraverso molteplici tecniche di tracciamento biometrico, quali il tracciamento degli occhi e della risposta della pupilla, le scansioni facciali, la risposta galvanica della pelle (vale a dire la misura delle variazioni nelle caratteristiche elettriche della pelle in ragione della variazione della sudorazione), l'elettroencefalografia, l'elettromiografia e l'elettrocardiografia[77].
Come affermato dal Parlamento europeo, il Metaverso risulta già soggetto a quadri legislativi pertinenti, che attengono per esempio ai servizi digitali e al diritto della concorrenza[78]; perciò, atti illeciti che si verifichino nel mondo virtuale assumono rilievo anche nel mondo reale, visto che essi integrano violazioni delle regole giuridiche di quest'ultimo.
Una questione che si pone in maniera pressante è certamente quella attinente alla tutela dei dati personali e al rispetto della *privacy*. Come è stato detto in generale con riferimento a Internet, in rete l'interesse comune è da ricollegarsi all'utilità sociale derivante dallo scambio di dati, il quale sembra prevalere sull'interesse a mantenere riservate certe informazioni[79].
Lo svolgimento di attività da parte dell'utente nel Metaverso comporta la condivisione di massicce quantità di informazioni, relative non solamente all'identità dell'utente stesso, bensì anche alle abitudini di consumo, alle opinioni e ai gusti. È stato quindi sostenuto che nel Metaverso si potrà assicurare la tutela dei dati personali, ma non della *privacy*, quanto meno nel suo significato originario di *right to be let alone*, visto che proprio la scelta di essere nel Metaverso comporterebbe l'impossibilità di realizzare ciò[80].
Indubbiamente, bisogna riconoscere che nel Metaverso vengono condivise informazioni personali e sensibili che difficilmente potrebbero essere ottenute nell'Internet attuale, considerato il ricorso alle tecniche di tracciamento biometrico di cui si è detto in precedenza e tenuto conto del fatto che non basterà intervenire sulle impostazioni *privacy* della piattaforma per porsi al riparo da certe situazioni. Anzi, se si procedesse in questo modo, il Metaverso finirebbe per perdere di senso. Si pensi al caso di un incontro galante o a un colloquio di lavoro nel Metaverso: sono situazioni nelle quali necessariamente gli utenti devono poter esprimere le loro preferenze, i loro gusti e le loro inclinazioni. Se non fosse possibile, l'esperienza del Metaverso verrebbe snaturata[81]. Lo stesso dicasi del caso di un partito politico o un movimento che intendesse organizzare un evento per comprendere l'opinione degli utenti rispetto a un certo tema e, in generale, di tutti i casi

[76] Ivi, 27-28.

[77] *Ibidem*.

[78] Risoluzione del Parlamento europeo del 5 maggio 2022 sulla politica di concorrenza – Relazione annuale 2021 (2021/2185(INI)), punto 55.

[79] M. Franzoni, *XIX lezione: lesione dei diritti della persona e tutela della privacy*, in U. Ruffolo (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, 343.

[80] G. Cerrina Ferroni, *Il metaverso tra problemi epistemologici, etici e giuridici*, cit., 9.

[81] Gli esempi sono tratti da L. Bolognini – M.E. Carpenelli, *Il futuro dei dati personali nel Metaverso*, in *Rivista Diritto, Economia e Tecnologie della Privacy*, 2022, 22.

in cui l'analisi delle emozioni degli utenti è funzionale a personalizzare un servizio.
Allora, l'aspetto da considerare è che i dispositivi portatili utilizzati per vivere appieno l'esperienza del Metaverso e, propriamente, le tecniche di tracciamento biometrico che si ricollegano al loro uso permettono di ottenere numerose informazioni di un utente, spesso senza che questi ne sia consapevole, visto che riguardano il dominio fisiologico e psichico dello stesso[82].

4. Considerazioni sulla protezione dei dati personali nel Metaverso

Dunque, è evidente che il Metaverso sollevi una serie di questioni concernenti la tutela dei dati personali e della *privacy*.
Per quel che riguarda la protezione dei dati personali, *in primis* va detto che inevitabilmente alcuni dati devono essere condivisi ai fini dell'iscrizione e, dunque, dell'accesso ai vari metaversi. Perciò, nome, cognome, indirizzo e-mail, data di nascita dell'utente vengono certamente ottenuti[83].
Detto questo, pare opportuno concentrarsi sulle tecniche di tracciamento cui già fanno ricorso i visori o che verranno implementate nei prossimi anni, ossia – come già si diceva *supra* – tracciamento degli occhi, scansioni facciali, risposta galvanica della pelle, elettroencefalografia, elettromiografia ed elettrocardiografia. La domanda sorge spontanea: le informazioni ottenute tramite queste modalità possono essere considerate dati personali?
Risaputamente, nell'ordinamento dell'Unione europea, la tutela assicurata dall'art. 16 TUE, dall'art. 8 della Carta dei diritti fondamentali e dal regolamento 2016/679 (cosiddetto GDPR) riguarda i dati personali, intesi, ai sensi dell'art. 4, n. 1) del regolamento ora menzionato, come informazioni riguardanti una persona fisica identificata o identificabile, ossia una 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. Tra questi rientrano i dati biometrici, definiti dallo stesso GDPR all'art. 4, n. 13), come dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Allora, alla luce di tale definizione, è evidente che le scansioni facciali per-

[82] In generale, si vedano A. McStay, *Emotional AI: The Rise of Empathic Media*, Los Angeles-London-New Delhi, Singapore-Washington, D.C.-Melbourne, 2018; J. Marín-Morales et al, *Affective Computing in Virtual Reality: Emotion Recognition from Brain and Heartbeat Dynamics Using Wearable Sensors*, in *Scientific Reports*, 8, 2018, 13657 ss.; M. Ienca – K. Ignatiadis, *Artificial Intelligence in Clinical Neuroscience: Methodological and Ethical Challenges*, in *AJOB Neuroscience*, 2, 2020, 77 ss.

[83] Si vedano per esempio le *Privacy Policies* di *Meta Horizon* e *Decentraland*, disponibili *online*.

mettano l'acquisizione di dati personali. Lo stesso vale, però, in quasi tutti gli altri casi. Infatti, l'occhio umano contiene un numero estremamente elevato di caratteristiche individuali che lo rendono particolarmente adatto al processo di identificazione di una persona, relative soprattutto all'iride e alla retina. In particolare, la retina presenta una struttura unica per ogni individuo in ragione della complessità della rete di vasi sanguigni che la compongono e delle loro ramificazioni[84].

Non solo: pure i segnali registrati tramite l'elettroencefalografia sono caratteristici del singolo individuo[85]. Questo vale anche per l'elettromiografia, in quanto tramite essa viene captato un segnale complesso, controllato dal sistema nervoso, che dipende dall'anatomia e dalle caratteristiche fisiologiche del muscolo e, poiché il collegamento tra muscolo e sistema nervoso dipende dalla fisiologia di ogni persona, il segnale è unico, stabile e difficile da falsificare[86].

Infine, pure tramite l'elettrocardiografia è possibile l'identificazione di un individuo, dato che le onde che vengono registrate, corrispondenti ai battiti cardiaci, presentano elementi peculiari, concernenti posizioni e intervalli, forme, proporzioni, picchi, pendenze e angoli, che variano da soggetto a soggetto[87].

Quindi, sembra potersi dire che attraverso le tecniche di tracciamento biometrico possono essere acquisiti dati attinenti alle caratteristiche fisiche o fisiologiche di una persona fisica che – almeno – ne consentono l'identificazione univoca. L'acquisizione avviene – o avverrà, nel caso delle tecniche in via di sperimentazione in relazione ai visori – attraverso un trattamento tecnico specifico che comporta – almeno – la raccolta di tali dati. Parrebbe così confermato il fatto che, mediante le modalità sopra indicate, si possano – o si potranno – ottenere dati personali riconducibili alla categoria dei dati biometrici *ex* art. 4, n. 14), GDPR. Perciò, le garanzie previste da tale atto concernenti liceità, correttezza e trasparenza del trattamento, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza devono – e dovranno – trovare applicazione.

---

[84] *Ex multis*, D. Marinović et al, *Personal Identification by Eyes*, in *Collegium Antropologicum*, 2, 2011, 347 ss.

[85] Per un'introduzione, S. Yang – F. Deravi, *On the Usability of Electroencephalographic Signals for Biometric Recognition: A Survey*, in *IEEE Transactions on Human-Machine Systems*, 6, 2017, 958 ss.; K. Aloui – A. Nait-Ali – M. Saber Naceur, *Using Brain Prints as New Biometric Feature for Human Recognition*, in *Pattern Recognition Letters*, 1° ottobre 2018, 38 ss.; Y.-Y. Yang et al, *Person-identifying brainprints are stably embedded in EEG mindprints*, in *Scientific Reports*, 12, 2022, 17031 ss.

[86] L. Lu et al, *A Study of Personal Recognition Method Based on EMG Signal*, in *IEEE Transactions on Biomedical Circuits and Systems*, 4, 2020, 681 ss. e J. Myung Kim – G. Choi – S. Pan, *User identification system based on 2D CQT spectrogram of EMG with adaptive frequency resolution adjustment*, in *Scientific Reports*, 14, 2024, 1340 ss.

[87] Per un'introduzione, S.A. Israel et al, *ECG to identify individuals*, in *Pattern Recognition*, 1, 2005, 133 ss.; L. Yousofvand – A. Fathi – F. Abdali-Mohammadi, *Person identification using ECG signal's symbolic representation and dynamic time warping adaptation*, in *Signal, Image and Video Processing*, 2, 2019, 245 ss.; A. Fratini et al, *Individual identification via electrocardiogram analysis*, in *BioMedical Engineering OnLine*, 14 agosto 2015, 1 ss.; A. Al-Jibreen et al, *Person identification with arrhythmic ECG signals using deep convolution neural network*, in *Scientific Reports*, 14, 2024, 4431 ss.

Ci si può poi domandare se sia possibile affermare che i dati in parola si configurano altresì come dati sensibili. L'art. 9, par. 1, GDPR chiarisce che rientrano in tale categoria non semplicemente i dati biometrici, ma quei dati biometrici che sono intesi a identificare in modo univoco una persona fisica. Si tratta di una fattispecie *purpose-based*, la quale definisce un'eccezione così da evitare che si determini un'automatica sovrapposizione tra dati biometrici e dati sensibili quando i primi siano stati ottenuti senza che vi fosse effettivamente l'intenzione di procedere a un'identificazione[88]. Ne deriva che, affinché la particolare tutela approntata dall'art. 9 per i dati sensibili possa assumere rilievo, si renderà necessario appurare quale sia la finalità del trattamento e se, dunque, i dati in questione siano stati ottenuti per identificare il soggetto (per esempio, per permettergli di accedere al Metaverso) o solamente per permettergli di interagire nel Metaverso.
Solamente la risposta galvanica della pelle non sembra riconducibile alla categoria dei dati biometrici, in quanto non pare idonea a permettere l'identificazione del singolo soggetto. Tuttavia, va ricordata l'esistenza di un'altra categoria di dati personali, definiti all'art. 4, n. 15), GDPR, come dati personali attinenti alla salute fisica o mentale di una persona fisica, che rivelano informazioni relative al suo stato di salute. Al considerando 35 del GDPR si afferma che essi concernono lo stato di salute fisica o mentale passata, presente o futura dell'interessato e che tra essi si possono ricomprendere informazioni riguardanti lo stato fisiologico o biomedico dell'interessato. Può quindi esserne data un'interpretazione ampia, tale da ricomprendere tutti gli aspetti inerenti alla salute di una persona, come confermato altresì dalla Corte di giustizia, dal Tribunale dell'Unione e dal Comitato europeo per la protezione dei dati[89]. Pertanto, i dati relativi alla salute vanno intesi non limitando il riferimento a situazioni patologiche che possono interessare l'individuo, ma considerando la fisiologia di questi nel suo complesso. Ecco allora che i dati ottenuti tramite la risposta galvanica della pelle, l'elettroencefalografia, l'elettromiografia e l'elettrocardiografia possono essere reputati dati relativi alla salute e, di conseguenza, rientrano tra i dati sensibili *ex* art. 9 GDPR[90].

5. Considerazioni sulla tutela della privacy nel Metaverso

Come si ricordava in precedenza, è già stata avanzata l'idea che nel Meta-

[88] In questi termini, P. Quinn – G. Malgieri, *The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework*, in *German Law Journal*, 8, 2021, 1594. Si veda inoltre C. Jasserand, *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*, in *European Data Protection Law Review*, 3, 2016, 297 ss.

[89] CGUE, C-101/01, *Lindqvist* (2003), § 50; Tribunale UE, T-343/13, *CN / Parlamento europeo* (2015), § 50; Comitato europeo per la protezione dei dati, *Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19*, 21 aprile 2020, punto 7.

[90] Quanto al fatto che informazioni che rivelano che un soggetto non presenta alcuna patologia sono comunque dati relativi alla salute, M. Ienca – G. Malgieri, *Mental data protection and the GDPR*, in *Journal of Law and Biosciences*, 1, 2022, 9.

verso potrà essere garantita la tutela dei dati personali, però non quella della *privacy*, almeno se si intende quest'ultima come *right to be let alone*. Espressa in tali termini, la tesi è pienamente condivisibile, dato che la scelta stessa di essere nel Metaverso comporta la rinuncia all'essere lasciati da soli.
Si ritiene però sia possibile individuare un'ulteriore dimensione dell'esperienza nel Metaverso di cui tenere conto e, di conseguenza, un'ulteriore dimensione del diritto alla *privacy* che potrebbe essere rilevante. Infatti, le interazioni nel Metaverso comportano la condivisione di informazioni sulle preferenze, i gusti e le emozioni dell'utente. In quanto tali, esse non possono essere evidentemente considerate dati personali. Tuttavia, non per questo dovrebbe ritenersi che esse possano essere liberamente accessibili dalle piattaforme e utilizzabili dalle stesse. Del resto, come sottolineato nella proposta di regolamento sulla vita privata e le comunicazioni elettroniche, al considerando 2, tra le informazioni altamente sensibili che possono essere rivelate da comunicazioni elettroniche si collocano anche le esperienze personali e le emozioni[91].
Sembra allora potersi recuperare l'idea di *privacy* mentale, cui si faceva riferimento *supra*, quale diritto attraverso il quale tutelare l'individuo rispetto all'accesso illecito alle informazioni presenti nel suo cervello e prevenire la diffusione indiscriminata di queste nell'infosfera[92].
Si è detto del rischio connesso alla *rights inflation* e, dunque, alla proliferazione di figure di diritti asseritamente nuovi che, in realtà, non assicurerebbero una reale forma di protezione. Si è detto altresì che diversi autori reputano preferibile procedere a un'interpretazione evolutiva di fattispecie già esistenti. Con riferimento alla *privacy* mentale, questo parrebbe realizzabile se si pone attenzione alla nozione di vita privata *ex* art. 8 CEDU elaborata dalla Corte europea dei diritti dell'uomo. Secondo la Corte, quello di vita privata è un concetto non suscettibile di una definizione esaustiva[93], che copre l'integrità fisica e psicologica di una persona e può riferirsi a vari aspetti della sua identità fisica e sociale, in quanto non è da intendersi come limitato a una cerchia ristretta in cui il singolo vive come meglio crede, escludendo il mondo esterno[94]. *Ex multis*, la vita privata ricomprende il benessere e la dignità dell'individuo[95], lo sviluppo della personalità[96], il diritto all'autodeterminazione[97], il diritto all'integrità psicologica[98], la pro-

[91] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)*, COM(2017) 10 final.

[92] Oltre agli scritti già citati, si veda F.X. Shen, *Neuroscience, Mental Privacy, and the Law*, in *Harvard Journal of Law & Public Policy*, 2, 2013, 653 ss.

[93] CEDU, *Niemietz c. Germania*, ric. 13710/88 (1992), § 29; *Pretty c. Regno Unito*, ric. 2346/02 (2002), § 61; *Peck c. Regno Unito*, ric. 44647/98 (2003) § 57.

[94] CEDU, *Denisov c. Ucraina*, ric. 76639/11 (2018), § 96.

[95] CEDU, *Beizaras e Levickas c. Lituania*, ric. 41288/15 (2020), § 117.

[96] CEDU, *Von Hannover c. Germania (n. 2)*, ric. 40660/08 e 60641/08 (2012), § 95.

[97] CEDU, *Pretty c. Regno Unito*, cit., § 61.

[98] CEDU, *Vavřička e altri c. Repubblica Ceca*, ric. 47621/13, 3867/14, 73094/14, 19298/15, 19306/15 e 43883/15 (2021), § 261 e *Söderman c. Svezia*, ric. 5786/08 (2013), § 80.

tezione dei dati personali[99], l'immagine di una persona[100] e molteplici altri profili.

In primo luogo, però, l'art. 8 CEDU mira a garantire lo sviluppo, senza interferenze esterne, della personalità di ciascun individuo nelle sue relazioni interpersonali, con la conseguenza che nella nozione di vita privata si può ricomprendere anche una zona di interazione di un soggetto con altri soggetti, anche in un contesto pubblico[101]. Perciò, il diritto alla *privacy* concerne anche il diritto a condurre una vita sociale privata[102].

Allora, alla luce di tale orientamento della Corte di Strasburgo, sembra potersi sostenere che la nozione di *privacy* possa essere estesa fino a ricomprendere il diritto a condurre una vita sociale privata anche nel Metaverso, con la conseguenza che il consenso dato con l'accesso al Metaverso non implicherebbe di necessità il consenso a che vengano acquisite e utilizzate indiscriminatamente le informazioni relative a gusti e preferenze dell'utente, derivanti dalle interazioni di quest'ultimo, riconoscendosi in tal modo l'esistenza e la tutelabilità della *privacy* mentale.

Come si diceva in precedenza, il ruolo dei privati nell'ambito tecnologico solleva il problema di garantire i diritti fondamentali nei rapporti con tali soggetti. È vero che le previsioni contenute nella CEDU vincolano gli Stati contraenti, i quali sono tenuti a rispettare i diritti contenuti in quelle secondo la logica degli obblighi negativi[103]. Tuttavia, la Corte di Strasburgo ha ammesso che la CEDU può essere altresì fonte di obblighi positivi e che, quindi, gli Stati devono assicurare che i diritti fondamentali elencati nella Convenzione siano rispettati dai privati. Ne deriva che, nel riconoscere la responsabilità di uno Stato per non avere adempiuto a tali obblighi positivi, la Corte europea dei diritti dell'uomo può individuare obblighi posti in capo ai privati. Ciò vale anche in relazione all'art. 8 CEDU[104]. Pertanto, gli Stati contraenti sono tenuti a fare in modo che il diritto alla *privacy* venga garantito anche dai privati, come le piattaforme del Metaverso.

Infine, vi è un ultimo aspetto che preme sottolineare. La ricostruzione ora proposta parrebbe applicabile anche nel contesto del diritto dell'Unione europea. Infatti, ai sensi dell'art. 52, par. 3, della Carta dei diritti fondamentali dell'Unione, nel caso in cui essa contenga diritti corrispondenti a quelli garantiti dalla CEDU, il significato e la portata dei primi sono uguali a quelli dei secondi, fermo il fatto che il diritto dell'Unione può concedere una protezione più estesa. L'art. 7 della Carta dei diritti fondamentali, dedicato al rispetto della vita privata e familiare, corrisponde all'art. 8 CEDU, come confermato dalla formulazione delle due previsioni e dalle Spiega-

[99] CEDU, *M.L. e W.W. c. Germania*, ric. 60798/10 e 65599/10 (2018), § 87 e *Liebscher c. Austria*, ric. 5434/17 (2021), § 31.

[100] CEDU, *Reklos e Davourlis c. Grecia*, ric. 1234/05 (2009), § 38.

[101] CEDU, *Von Hannover c. Germania (n. 2)*, cit; *Couderc e Hachette Filipacchi Associés c. Francia*, ric. 40454/07 (2015), § 83; *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, ric. 931/13 (2017), § 131.

[102] CEDU, *López Ribalda e altric. Spagna*, ric. 1874/13 e 8567/13 (2019), § 88.

[103] *Ex multis*, CEDU, *Kroon e altri c. Paesi Bassi*, ric. 18535/91 (1994), § 31.

[104] *Ex multis*, CEDU, *Gaskin c. Regno Unito*, ric. 10454/83 (1989), § 42; *Roche c. Regno Unito*, ric. 32555/96 (2005), § 157; *Hämäläinen c. Finlandia*, ric. 37359/09 (2014), § 65.

zioni della Carta dei diritti fondamentali. Pertanto, la nozione di vita privata nel diritto dell'Unione va interpretata in ragione della soglia minima di tutela scaturente dal sistema CEDU e dalla giurisprudenza della Corte di Strasburgo. Si ritiene allora che vi siano gli estremi per sostenere che la lettura sopra proposta quanto al diritto alla *privacy* mentale alla luce delle sentenze della Corte europea dei diritti dell'uomo possa trovare cittadinanza anche nell'ordinamento dell'Unione.

6. Conclusioni

In uno dei suoi capolavori, intitolato *Gli androidi sognano pecore elettriche?*, Philip K. Dick scrive che la vita degli androidi è sogno. In un altro testo fondamentale della fantascienza, *Neuromante*, William Gibson descrive il cyberspazio come un'allucinazione vissuta consensualmente ogni giorno da miliardi di persone. Grazie al Metaverso, è probabile che prima o poi anche la vita degli esseri umani si faccia sogno attraverso un'allucinazione vissuta consensualmente, ossia attraverso mondi virtuali che permetteranno di intrattenere relazioni, fare affari e ridefinire esistenze.
Le opportunità che si ricollegano allo sviluppo di questa nuova realtà sono indubbiamente affascinanti, ma compito del giurista (e non solo) è quello di interrogarsi sui rischi e sulle esigenze di tutela che a tali rischi si ricollegano. Nell'epoca del capitalismo delle informazioni, il diritto deve necessariamente sperimentare, reinventarsi, ridefinire i propri confini concettuali ed elaborare nuovi strumenti di tutela[105].
Questo vale anche per la protezione dei dati personali e della *privacy*. Nel presente scritto, chiarite le caratteristiche e le modalità di funzionamento del Metaverso, si è cercato di offrire soluzioni quanto a tali temi, interrogandosi sulla nozione di dato personale in relazione all'utilizzo dei visori che permettono di interagire nel Metaverso e su quella di *privacy* mentale.
Per quanto attiene alla protezione dei dati, si è sostenuto che sia i visori attualmente in commercio, sia quelli in via di sperimentazione permettono di avere accesso a dati biometrici, che sicuramente sono dati personali e, dunque, devono costituire oggetto di tutela nell'ordinamento dell'Unione europea coerentemente a quanto previsto dal GDPR. Se ottenuti per identificare in modo univoco l'utente, essi si configurano altresì come dati sensibili. Inoltre, si è sottolineato che i dati che in futuro potranno essere acquisiti tramite visori che sfruttano tecniche quali la risposta galvanica della pelle, l'elettroencefalografia, l'elettromiografia e l'elettrocardiografia possono essere reputati dati relativi alla salute e, pertanto, sensibili.
Con riferimento al diritto alla *privacy*, è stato posto in evidenza che dalla giurisprudenza della Corte europea dei diritti dell'uomo emerge una nozione ampia di vita privata, la quale comprende anche lo sviluppo, senza interferenze esterne, della personalità dell'individuo nelle relazioni interpersonali. Questo dovrebbe valere altresì in relazione al Metaverso e gli Stati contraenti della CEDU dovrebbero assicurarne la tutela rispetto a violazioni a opera di privati secondo la logica degli obblighi positivi. Tale

[105] M.C. Errigo, *Neuroscienze e diritto. Un punto di vista costituzionale*, Napoli, 2022, 176-177.

lettura, infine, parrebbe adottabile nell'ordinamento dell'Unione europea, in ragione del raccordo delineato dall'art. 52, par. 3, della Carta dei diritti fondamentali con il sistema CEDU.

Abstract

Nell'articolo si affronta la questione della tutela dei dati personali e della *privacy* nel Metaverso. Per farlo, si trae spunto dal dibattito sul rapporto tra neuroscienze e diritto, visto che nell'ambito di questo sono emerse indicazioni importanti per quel che riguarda la protezione dei diritti. Pertanto, dopo avere offerto una panoramica su tale tema, si delineano gli aspetti relativi alle caratteristiche e al funzionamento del Metaverso e le questioni poste da tale nuova realtà per i dati personali e il diritto alla *privacy*, cercando soluzioni nel diritto dell'Unione europea e nel sistema della Convenzione europea sui diritti dell'uomo.

The article addresses the issues of the protection of personal data and privacy in the Metaverse. To do so, it draws on the debate on the relationship between neuroscience and law, since relevant insights regarding the protection of rights have been provided in that context. Therefore, after sketching an overview of this topic, aspects related to the features and functioning of the Metaverse and the issues posed by this new reality for personal data and the right to privacy are outlined, looking for solutions in the law of the European Union and the European Convention on Human Rights.

Keywords

Metaverso – protezione dei dati personali – *privacy* – neurodiritti – diritto dell'Unione europea

Diritto alla protezione dei dati personali e dignità umana: "Profili di una pregnante correlazione"*

Antonio Vertuccio

Sommario

1. Introduzione – 2. La data driven society e il suo impatto sul diritto alla protezione dei dati personali - 3. Il riconoscimento del diritto all'autodeterminazione informativa da parte della Corte costituzionale tedesca - 4. La dignità umana e la sua correlazione con il diritto alla protezione dei dati personali - 4.1. Gli interventi legislativi europei per contrastare il microtargeting politico: "Una risposta efficace ai tentativi di manipolazione in rete"? – 5. Conclusioni

1. Introduzione

Le complesse evoluzioni sociali, caratterizzanti gli ultimi decenni, hanno avuto un forte impatto sull'ambito giuridico e, segnatamente, sulla tutela dei diritti fondamentali.

In particolare, la sempre più pervasiva digitalizzazione ha mutato il sostrato materiale sul quale si era sviluppata l'ermeneutica relativa alla tutela dei diritti fondamentali.

Il diritto alla privacy[1] è stato fortemente attinto dai mutamenti che han-

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

[1] La primordiale teorizzazione del diritto alla privacy si deve a due giuristi americani, Warren e Brandeis, che nel 1890, pubblicarono "*The right to privacy*", un contributo dottrinale per il riconoscimento del *«right to be let alone»* e per la creazione del diritto dell'*«inviolate personality»*. *The right to privacy* veniva identificato come un'estrinsecazione della proprietà privata e come una forma di possesso intangibile. Tale diritto era stato riconosciuto al fine di tutelare la sfera più emotiva degli individui. La necessità di teorizzare il diritto alla privacy nasceva dalle sofferenze morali inflitte agli individui a causa della pubblicazione sui quotidiani di vicende relative alla loro vita privata.

Al fine di inquadrare sinteticamente le fonti internazionali che hanno sancito il diritto alla privacy è possibile fare riferimento all'art. 12 della Dichiarazione Universale dei diritti dell'uomo, il quale sancisce che nessun individuo può essere sottoposto a interferenze arbitrarie nella sua vita privata, nella famiglia, nella corrispondenza né a lesione del suo onore e della sua reputazione. L'art. 17 del Patto sui diritti civili e politici del 1966 riprende il contenuto dell'art. 12 della Dichiarazione Universale dei diritti dell'uomo.

Nella medesima prospettiva si pone l'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU), il quale dispone che ogni individuo ha diritto al rispetto della propria

no cambiato il tessuto socio-economico globale, in quanto l'acquisizione dei dati personali è divenuta pervasiva e generalizzata. Invero, si potrebbe affermare che il diritto alla privacy ha assunto connotati evidentemente differenti rispetto al passato, acquisendo una portata sempre più vasta e ampia[2]. In questa prospettiva, emerge l'autonomia del diritto alla protezione dei dati personali, sancito dalla Carta dei diritti fondamentali dell'Unione europea[3].

Nell'odierno ambiente digitale i dati personali hanno assunto un importante valore economico e sono diventati il mezzo principale per alimentare perduranti tentativi di manipolazione degli "individui digitali".

L'"opacità funzionale", che colora il perimetro digitale, e la conseguente violazione del diritto alla protezione dei dati personali fanno sorgere delle riflessioni in merito alla correlazione tra «*digital right to data protection*»[4] e

vita privata e familiare, del proprio domicilio e delle sue comunicazioni. L'art. 7 della Carta dei diritti fondamentali dell'Unione europea ha il medesimo contenuto dell'art. 8 della CEDU, mentre l'art. 8 della Carta sancisce il diritto alla protezione dei dati personali, per la cui tutela assume una valenza centrale il *General Data Protection Regulation* (GDPR).

[2] In merito all'evoluzione del diritto alla privacy, S. Rodotà nel corso della Conferenza internazionale sulla protezione dei dati tenutasi a Cracovia nel 2004 affermò: «Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro. Emerge un legame profondo tra libertà, dignità e privacy, che ci impone di guardare a quest'ultima al di là della sua storica definizione come diritto ad essere lasciato solo»;
S. Rodotà, *Intervista su privacy e libertà,* Bari, 2005, 16. L'autore evidenzia che: «Nel caso della privacy, si tratta di elementi che sorreggono la libera costruzione della personalità di ciascun cittadino in un ben preciso contesto storico».

[3] Carta dei diritti fondamentali dell'Unione europea, Nizza, 2000.
In merito all'evoluzione del diritto alla protezione dei dati personali e la sua inclusione nella Carta dei diritti fondamentali dell'Unione europea e i relativi corollari si rimanda a: O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford, 2015.
L'autrice promuove un approccio olistico alla protezione dei dati personali e si sofferma anche sulla correlazione tra diritto alla protezione dei dati personali e privacy (spec. 89-129).
Per un approfondimento sull'evoluzione del diritto alla privacy e sulla protezione del diritto alla protezione dei dati personali in rete si rimanda a: O. Pollicino - M. Bassini - G. Di Gregorio, *Internet Law and protection of fundamental rights*, Milano, 2022, 169 ss. In particolare, gli autori evidenziano come privacy e protezione dei dati personali siano comunamente riconosciuti come due diritti separati. In tal senso, rileva anche la Carta dei diritti fondamentali dell'Unione europea, che tutela i medesimi diritti con due diversi articoli.

[4] In relazione all'evoluzione del diritto alla privacy si rimanda a: O. Pollicino, *Costituzionalismo, privacy e neurodiritti,* in questa *Rivista,* 2, 2021, 12 ss.; Per un approfondimento in merito al *digital right to privacy* si rimanda a: O. Pollicino, *Un digital preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain,* in *Il diritto dell'informazione e dell'informazione e dell'informatica*, 2014, 10 - 27. L'autore rileva come la direttiva 95/46/CE sia stata letta alla luce degli articoli 7 e 8 della Carta di Nizza ai fini del riconoscimento del *digital (Internet based) right to data protection.* L'autore si sofferma anche sulle pronunce della Corte di Giustizia dell'Unione europea atte a chiarire se l'art. 8 della Carta possa essere considerato autonomo, o ancillare, all'art. 7 della Carta.
In merito all'intrinseca connotazione del diritto alla protezione dei dati personali si rimanda a: F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza artificiale,* in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Torino, 2018, 37 ss. L'autore si sofferma sull'ontologica connotazione del diritto alla protezione dei dati personali, nelle sue diverse estrinsecazioni, soffermandosi in particolare sul General Data

dignità umana.
Per sviluppare un approfondimento in ordine ai profili della correlazione in questione, preliminarmente, verranno esaminate nel dettaglio le attività di profilazione e di *microtargeting*, che connotano l'ecosistema digitale.
L'analisi di queste pratiche consentirà di evidenziare come talune disposizioni del *General Data Protection Regulation(GDPR)*[5], pietra miliare per la protezione dei dati personali non solo nei confini europei, siano continuamente violate.
Prodromici alla delineazione dei termini della suddetta pregnante connessione tra diritto alla protezione dei dati personali e dignità umana saranno i cenni a una pronuncia della Corte costituzionale tedesca, attraverso la quale venne riconosciuto il diritto all'autodeterminazione informativa.
In seguito, si esaminerà la stessa dignità umana su un piano normativo, giurisprudenziale e sostanziale, nel tentativo di comprendere come sia tutelata dalle fonti internazionali e di scorgerne l'opaco contenuto.
Tale indagine permetterà di comprendere le ragioni per le quali la dignità umana viene attinta da pratiche come il *microtargeting* politico[6].
L'approfondimento dei menzionati profili di interesse è confacente alla profilazione di un'interdipendenza funzionale tra tutela del diritto alla protezione dei dati personali e diritto alla dignità umana.
L'emersione della suddetta interdipendenza funzionale imporrà il vaglio delle risposte legislative al *microtargeting* politico.

2. La *data driven society* e il suo impatto sul diritto alla protezione dei dati personali

Le riflessioni sulla connessione tra il diritto alla protezione dei dati personali e diritto alla dignità umana discendono, in primo luogo, da un'analisi fattuale dell'attuale ambiente digitale.
I dati personali hanno assunto una chiara centralità nell'odierna realtà economica e sociale. Invero, in proposito, è ormai possibile discorrere di "*data driven society*", che si sostanzia nella conversione in dati personali di qualsiasi aspetto della vita concreta[7].
La dimensione digitale, che pervade l'attuale tessuto sociale, ha portato gli

Protection Regulation (GDPR). In particolare, evidenzia come il GDPR concepisca la protezione dei dati personali in termini di controllo degli stessi dati e configuri una tutela dinamica della protezione dei dati personali, «che protegge il dato non in modo statico ma nella sua pluralità di utilizzazioni e funzioni», in questa prospettiva diviene rilevante il concetto di rischio che i trattamenti potrebbero comportare per la salvaguardia dei dati personali.

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

[6] Sul *microtargeting* politico si rimanda a: G. D'Ippolito, *Comunicazione politica online: dal messaggio politico sponsorizzato alla sponsorizzazione sui social network*, in questa *Rivista*, 1, 2020, 1, 162 ss.;
P. Villaschi, *Profilazione online e manipolazione del consenso nella bubble democracy*, in *La Rivista Gruppo di Pisa*, 3, 2021, 257 ss.

[7] Su tale trasformazione si rimanda a V. M. Schonberger - K. Cukier, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, 9 ss.

individui, in modo per lo più inconsapevole, a cedere una grande quantità di dati personali, che, come anticipato, hanno acquisito un vero e proprio valore economico[8].

L'economia corrente basa i propri *business* sui *Big Data,* dotati di un importante valore strategico. Al fine di comprendere i termini della descritta evoluzione risulta necessario fare talune precisazioni definitorie, utili a una più chiara comprensione della "datificazione" di cui si discorre.

Preliminarmente, viene in rilievo la necessità di dare una definizione dei *Big Data*.

Orbene, i *Big Data* possono essere definiti come: «*the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value*» [9]. Emerge come si tratti di una quantità elevata di dati, utilizzabili per trarre ulteriori informazioni, o meglio inferenze, attraverso la loro correlazione.

Il Parlamento europeo in una risoluzione del 2017 ha affermato che: «I *Big Data* si riferiscono alla raccolta, all'analisi, all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonte diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento, che usano sia informazioni memorizzate, sia in streaming al fine di individuare determinate correlazioni, tendenze e modelli» [10].

Il trattamento dei *Big Data* permette di trarre inferenze su fatti ignoti, utilizzabili per fini sociopolitici, strategici ed economici.

In questi termini, i processi inferenziali compiuti sui dati raccolti determinano una riqualificazione in chiave "informativa" della realtà circostante[11].

In quest'ottica, inoltre, rileva l'utilizzo di strumenti elettronici come *cookie*[12]

---

[8] Sul valore economico dei dati personali si rimanda a V. Ricciuto, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Rivista Diritto Civile*, 3, 2020, 642 ss.

[9] A. De Marco - M. Greco - M. Grimaldi, *A formal definition of Big Data based on its essential features*, in *Library Review*, 2016, 122-135.
Per un approfondimento sui *Big Data* si rimanda a: Garante Privacy - AGCOM - AGCM, Indagine conoscitiva sui Big Data, 10 febbraio 2020 (doc. web 9264297).

[10] Parlamento europeo, Risoluzione sulle implicazioni dei *Big Data* per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto, 2017.

[11] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

[12] I *cookie* sono dei piccoli file di testo necessari affinché il server del sito web che ne usufruisce possa ottenere informazioni sulla specifica attività che l'utente compie sulla pagina web. I *cookie* tecnici sono quelli strettamente essenziali per il funzionamento del sito internet, i *cookie* analitici servono per fornire al gestore del sito dati statistici, mentre i *cookies* di profilazione consentono di profilare l'utente per l'invio di messaggi pubblicitari aderenti alle tendenze emerse. In merito alla regolamentazione dell'utilizzo dei *cookie* si rimanda a: *European Data Protection Board (*EPDB), *Parere 5/2020 sul consenso ai sensi del regolamento (ue) 2016/679*, 2020, disponibile su: *epdb.europa.eu.*
L'EPDB ha chiarito che il semplice *scroll down* non può dar luogo al consenso dell'interessato all'installazione e all'utilizzo di *cookie* di profilazione. Inoltre, la predisposizione di *cookie wall,* predisposti per subordinare l'accesso al sito alla ricezione dei *cookie*, non consente di considerare il consenso libero, ai sensi dell'art. 5 del GDPR, e, dunque questo meccanismo è illecito. L'EPDB ha evidenziato come il consenso in questione debba essere informato e specifico.

e *Social Plugin*[13] per tracciare le abitudini di navigazione degli utenti.
Il suddetto monitoraggio è mirato a profilare[14] gli utenti, e, dunque, a conoscerne le insite peculiarità e al successivo *targeting*[15], che si sostanzia nella trasmissione, o nella non trasmissione, di contenuti commerciali o politici, parametrati ai profili digitali emersi.
Il *targeting* è una delle pratiche che da luogo alla disinformazione, funzionale ai tentativi di manipolazione degli individui, soprattutto in campo politico[16].
In sostanza, quindi, l'acquisizione dei dati personali è finalizzata a delineare un identikit degli individui, strumentale al tentativo di influenzarne le scelte e al condizionamento della piena e libera capacità di autodeterminazione.
La creazione di un apparato digitale, configurato in base al profilo dell'individuo, crea la c.d. *filter bubble*[17], cioè una bolla digitale, nonché informativa («infosfera») tesa a isolarlo, configurata in base agli interessi dell'individuo, con evidenti ripercussioni negative sulla sua capacità di scelta libera e informata, e non coartata, e sul pluralismo informativo[18].
In tal senso, è emblematica l'illecita acquisizione dei dati personali di 87 milioni di utenti di Facebook da parte di *Cambridge Analitica,* una società avente l'obiettivo di adottare strategie di comunicazione politica per finalità elettorali. L'illecita acquisizione dei dati personali era prodromica al *microtargeting* politico e, dunque, al tentativo di influenzare le elezioni

---

13 I *plug-in* sono programmi aggiuntivi che ampliano le funzioni delle applicazioni *web* e dei programmi desktop e consentono di acquisire informazioni relative all'indirizzo IP del visitatore del *browser*.

14 L'art. 4 del regolamento generale sulla protezione dati personali fornisce una definizione di profilazione quale: «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o per 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».

15 Per precisazioni sul *targeting* nei *social media* si rimanda a: *European Data Protection Board* (EPDB), *Parere 8/2020 sul targeting degli utenti dei social media*, 2020, disponibile su: *epdb.europa.eu*.

16 Per un approfondimento sulla disinformazione si rimanda a: O. Pollicino - P. Dunn, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione,* Milano, 2024, 125-128. In particolare, gli autori evidenziano come il termine *fake news* sia fuorviante e sia più corretto fare riferimento alla disinformazione, integrata anche dal *microtargeting*. Il concetto di disinformazione ricomprende «quelle forme di manifestazione di pensiero che si sostanziano nella diffusione di quelle informazioni false, inaccurate o fuorvianti, le quali siano presentate e diffuse con lo scopo precipuo di trarre un profitto economico, politico o ideologico, ivi inclusa l'ingerenza nei processi elettorali e democratici».

17 Per un approfondimento sul tema si rimanda a: M. Bianca, *La filter bubble e il problema dell'identità digitale*, in questa *Rivista,* 2, 2019, 39 ss.

18 In merito al modo in cui Internet abbia cambiato l'assetto dell'informazione si rimanda a: G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in G. Pitruzzella - O. Pollicino - S. Quintarelli, *Parole e potere. Libertà d'espressione, hate speech e fame news*, Milano, 2017, spec. 62-74. In particolare, vi è un riferimento all'utilizzo di sistemi di *machine learning (*sistemi di Intelligenza artificiale che si connotano per l'apprendimento automatico*)* ai fini della selezione delle informazioni da trasmettere agli individui.

presidenziali americane[19].

Più recentemente, la Corte costituzionale rumena ha annullato il risultato delle elezioni presidenziali, in quanto condizionate da una campagna di disinformazione attraverso il social network Tik Tok[20]. In particolare, la Corte ha evidenziato la fragilità dei processi democratici e come la pubblicità politica, unitamente a ingerenze terze, sia stato un «vettore di disinformazione».

Al contempo, il Garante europeo per la protezione dei dati personali ha formalmente ammonito la Commissione europea per aver posto in essere un tentativo illecito di intrusione nella campagna elettorale dei Paesi Bassi, mediante un processo di *microtargeting* e profilazione degli elettori su X. Il *microtargeting* politico sarebbe stato finalizzato a promuovere la proposta di regolamentazione (COM (2022) 209) sul controllo delle chat dei cittadini europei. Segnatamente, la campagna pubblicitaria, promossa dalla Commissione europea, avrebbe utilizzato dati particolari, come opinioni politiche e credenze religiose, per indirizzare messaggi verso specifici segmenti della popolazione, escludendo, invece, utenti con inclinazioni politiche conservatrici. La condotta in questione non ha comportato nessuna sanzione da parte del Garante europeo per la Commissione europea, ma assume un rilievo centrale nelle riflessioni circa il perdurante tentativo di condizionamento degli individui, basato sul trattamento dei dati personali.

L'intrinseca strutturazione dell'ambiente digitale fa emergere come la tutela del diritto alla protezione dei dati personali sia necessaria per salvaguardare la pluralità d'informazione e la libera autodeterminazione degli individui.

La tutela del diritto alla protezione dei dati personali è un ineludibile presupposto per garantire un effettivo e libero sviluppo della personalità umana.

Le suddette riflessioni, esplicative dell'ampia portata del diritto alla protezione dei dati personali, sono funzionali all'approfondimento circa la crescente correlazione tra diritto alla protezione dei dati personali e dignità umana.

Nella medesima prospettiva, si pone una pronuncia della Corte costituzionale tedesca del 1983, con la quale venne riconosciuto il diritto all'autodeterminazione informativa.

Infatti, la Corte tedesca iniziò a delineare una correlazione tra diritto alla protezione dei dati personali e dignità umana.

Prima di procedere alla relativa analisi, non è concesso esimersi dall'evidenziare come la *commodification*[21] dei dati personali e l'inquadramento

---

[19] L'attività di *Cambridge Analitica* fu posta in essere nel 2016 per conto della fazione politica facente capo a Donald Trump.

[20] In merito a questa significativa pronuncia si rimanda a: O. Pollicino, *Se la disinformazione condiziona i processi democratrici,* in *Il Sole 24ore*, 2025. Le emerse vicende confermano quanto affermato da: Pizzetti, La protezione dei dati personali e la sfida dell'Intelligenza artificiale, cit., 38, il quale evidenziava come « la funzione sociale colloca la protezione dei dati personali in una prospettiva che supera la sfera individuale della persona e ne fa uno degli aspetti essenziali della società democratica». «La protezione dei dati personali ha una dichiarata valenza pubblicistica legata alla tutela dei valori, dei principi e del modo di funzionamento della società nel suo complesso».

[21] In relazione alla *commodification* dei dati personali, e, dunque, sull'acquisizione di valore

dell'attuale ecosistema digitale consenta di rilevare una perdurante violazione del GDPR, a opera delle piattaforme digitali che hanno assunto un potere parastatale[22].

Ebbene, viene in rilievo un'atavica violazione dell'art. 22 del GDPR, che statuisce il diritto degli individui a non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato[23], compresa la profilazione, che produca effetti giuridici che li riguardi o che incida in modo analogo significativamente sulla loro persona.

Come visto, però, l'inosservanza di questa disposizione è costante nell'ambiente digitale, in quanto la profilazione avviene sovente attraverso trattamenti esclusivamente automatizzati. Invero, i suddetti trattamenti automatizzati, posti in essere attraverso l'uso dell'Intelligenza artificiale, sono tesi a manipolare gli individui, e, quindi, a produrre effetti giuridici sugli stessi.

Le linee guida sul processo decisionale automatizzato[24] fanno espressamente rientrare tra gli "effetti giuridici" la capacità della decisione (o, meglio, l'incidenza del contenuto trasmesso), basata sul trattamento automatizzato, di incidere sul voto nel contesto di un'elezione. Inoltre, si ritiene che l'eventuale consenso dell'interessato al trattamento automatizzato non sia connotato da un'effettiva consapevolezza circa le molteplici finalità (tra le quali il *microtargeting*) per le quali avviene il medesimo.

---

economico, si rimanda a: G. Pignataro, *Circolazione dei dati tra modelli proprietari e contrattuali*, in questa *Rivista*, 2, 2024, 1-13;

L. A. Bygrave, *Data Privacy Law: An International Perspective,* Oxford, 2014, 11, afferma: «*personal data has thus been termed the new oil*».

[22] L'assunzione di questo potere, per il cui approfondimento si rimanda a: G. De Gregorio, *Digital Constitutionalism in Europe, Refreming Rights and Power in Alghorithmic Society*, Cambridge, 2022, 80 ss., potrebbe dar luogo a delle riflessioni circa la teoria dell'efficacia orizzontale dei diritti fondamentali e il carattere multirelazionale dei diritti umani.

Sul punto si rimanda a: R. Alexy, *Teoria dei diritti fondamentali*, Bologna, 2012, 554 ss.;

P. Rescigno, *L'abuso del diritto*, Bologna, 1998, 113 ss.;

O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in questa *Rivista*, 3, 2018, 3 ss.

In relazione alla valenza dei diritti umani generali anche nei rapporti interprivati si rimanda a: M. Fasciglione, *Impresa e diritti umani*, Torino, 2024, 72 ss.

[23] Ai sensi del GDPR per decisione basata unicamente sul trattamento automatizzato si intende una decisione presa senza il coinvolgimento di un essere umano che possa influenzare ed eventualmente cambiare il risultato attraverso la sua autorità.

In relazione all'applicazione del rilevante articolo 22 del GDPR: Pizzetti, La protezione dei dati personali e la sfida dell'Intelligenza artificiale, cit., 36, chiarisce come tale articolo debba essere calato in una prospettiva atta a garantire che questa norma, anche di fronte all'espandersi delle tecnologie IA, consenta di tutelare effettivamente la sfera personale degli individui;

Si rimanda anche a L. A. Bygrave, *Article 22 Automated individual decision-making, including profiling*, in C. Kuner - L. A. Bygrave - C. Docksey (a cura di), *The Eu General Data Protection Regulation (GDPR) A Commentary,* Oxford, 2020, 522–542. L'autore afferma che l'articolo 22 riconoscerebbe un diritto, esercitabile attivamente, basandosi su un'interpretazione letterale del termine diritto. Al contempo, precisa che ai fini della configurazione di un trattamento automatizzato la raccolta delle fonti inziali non debba essere necessariamente automatizzata.

[24] Gruppo di lavoro 29 per la protezione dei dati, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, 2018.

Le sedimentate connotazioni dell'infrastruttura digitale, rispondenti a logiche economiche, volte a compromettere l'inviolabilità della sfera più intima degli individui, si pongono in netta contrapposizione con il principio di privacy *by design*[25], alla base del GDPR, che imporrebbe la trasparenza del trattamento dei dati personali e la relativa minimizzazione, come evidenziato dall'*European Data Protection Board* (EPDB).
A parere di chi scrive le violazioni del GDPR[26] inducono a soffermarsi anche sull'efficacia deterrente delle sanzioni previste dallo stesso regolamento e dalle altre fonti, quali il *Digital Service Act* (DSA)[27] e il regolamento europeo sull'intelligenza artificiale[28], al fine di non rendere convenienti, sul piano economico, le violazioni del diritto alla protezione dei dati personali.

3. Il riconoscimento del diritto all'autodeterminazione informativa da parte della Corte costituzionale tedesca

Funzionale al tentativo di identificazione della crescente portata del diritto alla protezione dei dati personali è il rinvio a una pronuncia della Corte costituzionale tedesca, con la quale è stato riconosciuto il diritto all'autodeterminazione informativa[29], quale presupposto per una collettività libera

[25] In merito al principio di privacy by design si rimanda a: *European Data Protection Board (*EPDB), *Orientamenti 4/2019 sull'articolo 25 protezione dei dati fin dalla progettazione e per impostazione predefinita*, 2020, disponibile su: *epdb.europa.eu.*
L'Organismo europeo indipendente ha evidenziato che il titolare del trattamento dovrebbe scegliere opzioni e impostazioni per il trattamento dei dati, tali da garantire che venga effettuato solo se il trattamento sia strettamente necessario per conseguire la specifica e lecita finalità. Inoltre, il titolare è tenuto a definire in anticipo per quali finalità specifiche, esplicite e legittime i dati personali vengano raccolti e trattati.
Le misure devono essere adeguate a garantire che siano trattati solo i dati necessari per ogni specifica finalità del trattamento.
Alla luce di questa enucleazione giuridica l'EPDB ha delineato i principi di trasparenza, correttezza, liceità, esattezza, minimizzazione e integrità cui i titolari del trattamento devono attenersi per tendere verso un'attuazione della *privacy by design.*

[26] Tra gli altri interventi dei Garanti europei è possibile fare riferimento alle sanzioni comminate dal Garante della privacy irlandese dell'ammontare di 390 milioni di euro a Meta. Questa sanzione è stata causata all'utilizzazione di Meta della base giuridica contrattuale per finalità di personalizzazione degli annunci su Facebook e Instagram che, in assenza di un'autorizzazione degli utenti, dovranno essere eliminati. La sanzione veniva inflitta per l'assenza di trasparenza nei confronti degli individui e per l'indebita qualificazione dell'accettazione dei termini d'uso dell'applicativo come fattispecie contrattuale, in base alla quale il trattamento dei dati personali degli interessati, finalizzato alla fornitura di servizi personalizzati, veniva indebitamente basato sull'art. 6 lett. b del GDPR.

[27] Regolamento (UE) 2022/2065, relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 200/31/CE.

[28] Regolamento (UE) 2024/1689, che stabilisce regole armonizzate sull'Intelligenza artificiale.

[29] BVerfGE , 1983, VolkszählungsurteilI. Per un approfondimento dottrinale della pronuncia si rimanda a G. Sartor, *Tutela della personalità e normativa per la protezione dei dati personali. La sentenza della Corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionali del "Datenschutz",* in *Informatica e diritto*, 3, 1986, 95-118.

e democratica.
La Corte ha rinvenuto il fondamento del diritto all'autodeterminazione informativa nell'inviolabilità della dignità umana e nel diritto al libero sviluppo della personalità, sanciti dalla Costituzione tedesca.
L'analisi di questa storica pronuncia è di fondamentale importanza perché consente di risalire alle origini del legame tra diritto alla protezione dei dati personali e dignità umana.
In prima istanza, la Corte costituzionale tedesca ha dichiarato incostituzionale la legge sul censimento della popolazione, degli impieghi e dei posti di lavoro, approvata dal Parlamento tedesco nel 1982. La predetta legge era tesa a raccogliere dettagliate informazioni sui singoli individui al fine di conoscere in modo approfondito lo stato della popolazione e la sua composizione.
In particolare, attraverso dei questionari, venivano richieste agli individui informazioni sui loro redditi, sul tipo di attività lavorativa svolta e sull'abitazione presso la quale vivevano. Il censimento, inoltre, si caratterizzava per l'assenza di un'anonimizzazione dei dati personali raccolti. Al contempo, la legge prevedeva la facoltà per le Amministrazioni di incrociare questi dati con altri dati già presenti nelle banche dati dell'anagrafe per fini non ben specificati.
I peculiari profili legislativi descritti consentivano alle autorità tedesche di porre in essere un'irragionevole e sproporzionata ingerenza nella sfera privata degli individui, contraddistinta da una penetrante acquisizione di dati personali, disancorata da una qualsivoglia anonimizzazione, non giustificata dalle ragioni censorie e foriera di incostituzionalità.
Come anticipato, la Corte ha posto alla base del riconoscimento del diritto all'autodeterminazione informativa la necessità di salvaguardare il diritto alla personalità umana, derivante dal combinato disposto tra inviolabilità della dignità umana e diritto allo sviluppo della personalità dell'individuo, entrambi sanciti dalla Costituzione tedesca.
Secondo i giudici, il diritto alla personalità umana implica la facoltà per i singoli individui di autodeterminarsi e, dunque, di stabilire autonomamente se ed entro quali limiti cedere i propri dati personali.
L'impossibilità di venire a conoscenza del modo e delle finalità per le quali venivano acquisiti i dati personali avrebbe violato il diritto all'autodeterminazione.
Ad avviso della Corte, il diritto allo sviluppo della personalità umana presuppone la salvaguardia della sfera privata degli individui da una raccolta senza limitazioni dei dati personali.
Date queste premesse, utili a comprendere la ratio sottesa alla genesi di questo diritto, è possibile rilevare come la dottrina[30] rilevi la natura bifasica del diritto all'autodeterminazione informativa, scindibile in una fase passiva, che si estrinseca nel diritto di ricevere informazioni in merito al trattamento stesso, ma anche di una "fase attiva".

[30] P. Scwarz, *The computer in German and American Constitutional law: Towards an American Right of Informational Self Determination*, in *American Journal of Comparative Law*, 4, 1989, 686 ss.; A. Palumbo, *Il diritto all'autodeterminazione informativa. L'esperienza tedesca in materia di protezione dei dati personali*, Milano, Università Bicocca, 2015, 52 ss.; A. Vivarelli, *The crisis of the right to Informational Self – Determination*, in *The Italian law journal*, 1, 2020, 303 ss.

Tale fase attiva si sostanzierebbe nel diritto dell'individuo di incidere effettivamente sul trattamento in essere dei propri dati personali, esercitando un potere di controllo continuo sul trattamento dei dati personali.
In effetti, il riconoscimento di queste facoltà attive sembra essere un corollario della fase passiva del diritto all'autodeterminazione, in quanto la scelta circa la cessione dei propri dati personali può essere effettivamente libera solo se supportata da un continuo ed effettivo controllo circa le modalità e le finalità per le quali vengono trattati i dati personali.
Appare evidente, che attraverso il riconoscimento di questo diritto, la Corte intendeva evitare che gli individui fossero "oggetto" di un opaco trattamento dei dati personali volto a perseguire finalità non ben precisate. Seppur in un contesto storico differente, questa opacità è riscontrabile anche nell'odierno ambiente digitale.
Le illuminate riflessioni della Corte sono trasponibili nell'ambiente digitale, che, come visto, si connota per l'assenza di trasparenza e per il tentativo costante di comprimere l'autodeterminazione degli individui.
La pronuncia in questione è di importante rilievo per la tutela del diritto alla protezione dei dati personali, ma è anche strumentale all'indagine in merito alla correlazione tra diritto alla protezione dei dati personali e dignità umana.
Infatti, come visto, la Corte ha evidenziato la sussistenza di un nesso tra un'estrinsecazione del diritto alla protezione dei dati personali, l'autodeterminazione informativa, e l'inviolabilità della dignità umana, individuata come fondamento del diritto alla personalità umana.
Segnatamente, la Corte ha tracciato la connessione tra diritto alla protezione dei dati personali e dignità umana, mediata dal diritto alla personalità umana, ponendo la dignità umana a fondamento del diritto all'autodeterminazione informativa.
Invero, da una prospettiva diversa e in un'ottica di interdipendenza funzionale, si ritiene che il diritto alla protezione alla protezione dei dati personali sia prodromico alla tutela della dignità umana.
Scenario già in parte desumibile dall'argomentazione della Corte, in quanto, il riconoscimento della libertà di scelta, in merito alla cessione dei propri dati personali, è una delle prerogative che derivano dalla tutela del diritto alla personalità umana, desunta, a sua volta, dall'inviolabilità della dignità umana e dal diritto allo sviluppo della personalità umana.
Dunque, la protezione della libertà di autodeterminarsi in merito alla cessione dei dati personali è necessaria per non dar luogo a una violazione del diritto alla personalità umana e della dignità umana.
L'ulteriore passaggio da effettuare per tracciare in modo più definito i termini della funzionalità del diritto alla protezione dei dati personali alla tutela della dignità umana consiste nell'approfondimento dogmatico e giurisprudenziale in merito alla dignità umana. In questa prospettiva, si cercherà di comprendere in che cosa si sostanzi la dignità umana e le intrinseche ragioni sottese alla suddetta correlazione.

4. La dignità umana e la sua correlazione con il diritto alla protezione dei dati personali

La dignità umana sembra rifuggire da una qualificazione cristallizzante, in virtù della sua natura dinamica e mutevole, riflesso delle evoluzioni sociali. La dignità, qualificabile come diritto e principio, è stata ritenuta da parte della dottrina quale fondamento dei diritti umani[31].

In un'ottica ricostruttiva, tesa a sviluppare un approfondimento in merito alla valenza della dignità umana sul piano giuridico, emerge la necessità di fare innanzitutto riferimento alle fonti normative.

Nella Costituzione della Repubblica federale tedesca la dignità umana rappresenta il diritto da cui promanano i diritti inviolabili dell'uomo, ai quali la Repubblica federale tedesca vincola i propri poteri.

Nel Preambolo della Carta delle Nazioni Unite[32], si fa riferimento alla necessità di riaffermare la fede nei diritti fondamentali, nella dignità e nel valore della persona umana. La riaffermazione di tali prerogative è funzionale alla salvaguardia dell'umanità dai conflitti bellici.

Parallelamente, nel Preambolo della Dichiarazione Universale dei diritti dell'uomo[33] la dignità umana viene identificata quale fondamento della libertà, della giustizia e della pace nel mondo. Anche in questo caso la tutela delle dignità umana assorge a presupposto per scongiurare nuovi conflitti mondiali in grado di offendere la coscienza dell'umanità.

Nel Preambolo vi è un riferimento anche alla riaffermazione della dignità nei singoli Statuti degli Stati, funzionale alla promozione del progresso sociale e della libertà.

Nella versione aggiornata della Convenzione 108[34] vi è un riferimento alla necessità di salvaguardare il diritto alla privacy in un'ottica prodromica alla tutela della dignità umana.

Inoltre, la Convenzione americana sui diritti umani[35] sancisce la tutela dell'onore degli individui, correlandola alla tutela della dignità umana.

L'art. 2 del Trattato sull'Unione europea (TUE)[36] chiarisce come l'Unione si fondi sul rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani.

Da questi "strumenti" internazionali emerge l'intima e ontologica connessione tra dignità e diritti umani.

Analogamente, l'art. 1 della Carta dei diritti fondamentali dell'Unione europea dispone che la dignità umana è inviolabile e deve essere rispettata e

---

31 C. Focarelli, *La persona umana nel diritto internazionale*, Bologna, 2013. L'autore si interroga sul fondamento dei diritti umani, rinvenendolo nella "natura umana". Al contempo, però, fa riferimento a orientamenti dottrinali tesi a rinvenire nella dignità umana il fondamento dei diritti umani. L'autore qualifica questi orientamenti come una versione moderna della tesi sulla natura umana.

32 Carta delle Nazioni Unite, San Francisco, 1945.

33 Dichiarazione Universale dei diritti dell'uomo, Parigi, 1948.

34 Consiglio d'Europa, Convenzione 108, 1981. La Convenzione è stata emendata con un Protocollo adottato nel 2018 per adeguare la Convenzione alle evoluzioni digitali.

35 Convenzione americana sui diritti umani, Costa Rica, 1969, entrata in vigore nel 1978.

36 Trattato sull'Unione europea, Maastricht, 1992

tutelata.
Nell'ambito della Carta di Nizza, la dignità umana assume un valore preminente e fondante.
La formulazione letteraria dell'art. 1 della Carta, connotata dal riferimento al termine "tutelata" induce a ritenere che gli Stati non abbiano solo un dovere di astensione, ma anche l'obbligo di porre in essere misure positive affinché sussistano le condizioni per vivere in condizioni dignitose.
Nelle spiegazioni della Carta di Nizza si afferma che: «La dignità della persona umana non è soltanto un diritto fondamentale in sé, ma costituisce la base stessa dei diritti fondamentali. Ne consegue, in particolare, che nessuno dei diritti sanciti nella presente Carta può essere usato per recare pregiudizio alla dignità altrui e che la dignità umana fa parte della sostanza stessa dei diritti sanciti nella Carta. Essa non può pertanto subire pregiudizio, neanche in caso di limitazione di un diritto»[37].
Dall'esame di questi preliminari riferimenti normativi emerge come la dignità umana sia insita negli altri diritti fondamentali. In questi termini, viene in rilievo un legame ontologico e ineludibile tra dignità e diritti fondamentali.
La dignità umana diviene un limite a potenziali violazioni dei diritti fondamentali degli individui. In quest'ottica, si potrebbe ritenere che la dignità umana possa avere una rilevanza fondamentale anche nell'identificazione del nucleo essenziale dei diritti fondamentali, o meglio, possa riempire di contenuto il nocciolo duro dei diritti non sacrificabile ai fini del bilanciamento giuridico, necessario nella districata realtà giuridica attuale[38].
Quindi, è già possibile evidenziare una correlazione ontologica tra la dignità umana e il diritto alla protezione dei dati personali. Al contempo, però, la suddetta correlazione non è dovuta alla digitalizzazione e ai profili di criticità caratterizzanti l'ambiente digitale.
Invero, l'odierno ambiente digitale darà modo di indagare sul più intenso legame tra protezione dei dati personali e dignità umana.
Sul piano giurisprudenziale, occorre rilevare come la dignità umana abbia assunto una discreta rilevanza, non corroborata, però, da un pieno tentativo di valorizzazione della stessa. Nella causa C-36/02[39], la Corte di giu-

---

[37] Spiegazioni relative alla Carta dei diritti fondamentali (2007/C 303/01). In merito al legame ontologico tra dignità umana e diritti fondamentali, e dunque anche il diritto alla privacy si rimanda a: J. Blounstein, il quale in risposta al Prosser, che criticava la dimensione unitaria del diritto alla privacy affermava in: *Privacy as an aspect of human dignity: an answer to Dean Prosser*, in F.D. Schoeman (a cura di), *Philosophical Dimension of privacy. An antology*, 1964, 156 ss., che: «An intrusion in our privacy threatens our liberty as individuals to do as well will, just as an assault, a battery or imprisonment of our person does. In all of these cases there is an interference with individuality, an intereference with right of the individual to do what he will. The man who is compelledt o live every minute of his life among othersand whose every need thought, deisre, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity ».
Sulla dignità umana nella Carta di Nizza si rimanda a: P. Grossi, *Dignità umana e libertà nella Carta dei diritti fondamentali dell'Unione europea*, in M. Siclari (a cura di), *Contributo allo studio della Carta dei diritti fondamentali dell'Unione europea,* Torino*,* 2003.

[38] In merito all'identificazione del nucleo essenziale del diritto alla protezione dei dati personali e alla rilevanza della dignità umana in questi termini si rimanda a: CGUE, C–817/19, *Ligue des droits humains* (2022).

[39] CGUE, C- 36/02, *Omega* (2004). Per un approfondimento in relazione alle pronunce

stizia dell'Unione europea (CGUE) ha riconosciuto per la prima volta alla dignità umana una reale autonomia, non prendendo in considerazione altri diritti fondamentali. In altre parole, la dignità umana è stata identificata come il diritto fondamentale da bilanciare nel caso concreto.
La controversia che dava luogo a questa causa era sostanzialmente riconducibile al divieto, sancito nell'ordinamento nazionale tedesco, di porre in essere un'attività economica avente a oggetto lo sfruttamento commerciale di giochi di simulazione di omicidi.
Nella causa in questione, la Corte ha delineato un bilanciamento tra libertà di prestazione di servizi economici e dignità umana, autonomamente considerata.
La Corte ha evidenziato come nel caso concreto prevalesse la necessità di salvaguardare l'ordine pubblico, quale fine mediato per la tutela della dignità umana.
In questa e in altre pronunce[40] della Corte, la dignità umana viene identificata come diritto fondamentale.
La dignità umana è stata anche al centro di talune pronunce della Corte europea dei diritti dell'uomo, per quanto nella Convenzione europea dei diritti dell'uomo (CEDU)[41] non vi sia alcun riferimento alla dignità umana.
Nel caso *Pretty vs. United Kingdom*[42]*,* la ricorrente rivendicava il diritto di essere assistita nel commettere il suicidio richiamando a supporto delle sue ragioni l'art. 8 della CEDU e il diritto ad autodeterminarsi.
Nella causa in questione la Corte ha affermato che: «*very essence of the Convention is respect for human dignity*». Anche in altre pronunce[43] della Corte è rinvenibile questo sfumato riferimento alla dignità umana e alla sua salvaguardia quale essenza della Convenzione.
Orbene, fatte queste premesse, atte a inquadrare la dignità umana su un piano dogmatico e giurisprudenziale, emerge la necessità di fare riferimento ai modi in cui possa essere intesa la medesima o, meglio, ai criteri di non bilanciamento della stessa[44].
Preliminarmente, su questo piano filosofico, rileva quanto affermato da Kant, il quale riteneva che la dignità umana fosse connessa alla differenza antropologica tra "*homo noumenon*" (anima) e "*homo phaenomenon" (*corpo)[45].
L'offesa alla dignità umana si concretizzerebbe allorquando si riduca una

giurisprudenziali della CGUE e della Corte EDU, relative alla dignità umana si rimanda a: M. Di Ciommo, *Dignità umana e Stato costituzionale, La dignità umana nel costituzionalismo europeo, nella Costituzione italiana e nelle giurisprudenze europee*, Firenze, 2010, 201 ss.

40 CGUE, C – 438/05**,** *International Transport Workers' Federation* (2007).

41 Convenzione europea dei diritti dell'uomo, Roma, 1950.

42 CEDU, *Pretty c. United Kingdom*, ric. 2346/02, (2002). In relazione alla valenza della dignità umana nella Convenzione si rimanda a: D. Feldman, *"Human Dignity as a Legal Value"*, parte II, in *Public Law,* 2000, 75 ss.

43 CEDU, *E. and others c. United Kingdom*, ric. 33218/96 (2002);
CEDU, *Nasr and Ghali c. Italia*, ric. 44883/09 (2016). Con questa pronuncia la Corte ha anche evidenziato come l'art. 8 della CEDU protegga anche il diritto allo sviluppo personale.

44 B. Malvestiti, *Criteri di non bilanciabilità della dignità umana*, in M. Cossutta (a cura di), *Diritti fondamentali e diritti sociali*, 2012, 113-133.

45 Sul punto si rimanda a G. Azzoni, *Dignità umana e diritto privato*, in *Ragion Pratica,* 1,

persona alla sua parte fenomenica.
In quest'ottica, è possibile fare riferimento al tratto personologico della dignità umana.
La dignità umana in questa accezione viene lesa nel caso in cui l'essere umano venga strumentalizzato e trattato come un oggetto[46].
Inoltre, la tutela della dignità umana impone il dovere di non violare l'esigenza di «fioritura» dell'essere umano e di promuoverla (tratto eudemonologico)[47].
L'esigenza di fioritura, quale piena e libera estrinsecazione dell'essere umano, è violata allorquando vi siano tentativi di condizionamento della libertà di scelta degli individui.
In questi termini, dall'esigenza di fioritura dell'individuo promana il diritto allo sviluppo della personalità.
Il legame tra dignità umana e diritto allo sviluppo della personalità è già emerso nel corso dell'approfondimento della pronuncia della Corte costituzionale tedesca sull'autodeterminazione informativa.
Si ritiene di dover evidenziare che il pieno godimento dei diritti politici-civili (attinti nel caso di specie dal *microtargeting* politico), culturali ed economici sia un presupposto essenziale per non minare il diritto allo sviluppo della personalità.
La dottrina[48] evidenzia come questa funzionalità sia desumibile anche dall'art. 22 della Dichiarazione Universale dei diritti dell'uomo, nell'ambito della quale i diritti economici, sociali e culturali vengono qualificati come indispensabili per la salvaguardia della dignità umana e del libero sviluppo della personalità dell'uomo.
In aggiunta, è possibile fare riferimento anche all'art. 1 della Dichiarazione sul diritto allo sviluppo, approvata dall'Assemblea Generale dell'Organizzazione delle Nazioni Unite (ONU)[49], che individua il godimento dei diritti politici come ineludibile presupposto per la tutela del pieno sviluppo della persona umana. In relazione all'esigenza di promuovere lo sviluppo umano e alla salvaguardia dell'individuo dalle minacce algoritmiche, operanti anche in campo politico, l'Organizzazione internazionale per l'attuazione del Programma delle Nazioni Unite per lo sviluppo ha elaborato un rap-

2012, 84.
In relazione al tentativo di calare la dignità umana in una prospettiva funzionale si rimanda a: F. Horak, *Human Dignity in Legal Argumentation: A Functional Perspective*, in *European Constitutional Law Review*, 2 , 2022, 237 ss.

[46] Ivi, 116-123.
Ai fini dell'identificazione di questo criterio l'autrice fa riferimento a Kant, il quale mise in luce il valore intrinseco dell'essere umano, che ne fa un fine in sé, che impone di non trattarlo come semplice mezzo.

[47] Ivi, 123-128. L'autrice per l'identificazione di questo tratto della dignità umana fa riferimento al Rosmini, secondo il quale il bene eudemonologico si sostanzia in ciò che è desiderato dall'individuo come bene per sé e a Hersch, il quale afferma che il tratto eudemonologico della dignità umana si sostanzia nell'esigenza assoluta dell'essere umano di essere l'artefice delle proprie scelte di vita e di valore.

[48] Ivi, 126.

[49] Assemblea Generale dell'ONU, Dichiarazione sul diritto allo sviluppo, 1986.

porto[50], avente a oggetto l'uso dell'Intelligenza artificiale. Nel rapporto l'Organizzazione sottolinea come lo sviluppo dell'IA debba essere caratterizzato da finalità inclusive e non manipolatrici.
Si ritiene che l'approfondimento in merito ai criteri di non bilanciabilità della dignità umana, utili al tentativo di identificare, almeno in parte, l'opaco contenuto della dignità umana consenta di mettere in evidenza come l'acquisizione dei dati personali ai fini della profilazione e, in particolare, i tentativi di condizionamento gli individui con il *microtargeting* politico siano in grado di violare il tratto eudemonologico della dignità umana.
Segnatamente, si ritiene che il descritto *microtargeting* politico sia in grado di incidere sull'effettiva fruizione dei diritti politici degli individui, il cui godimento rappresenta il presupposto per un pieno sviluppo della personalità, necessario a sua volta per salvaguardare l'esigenza di fioritura, e, dunque la dignità umana, la cui inviolabilità è ribadita dalla Carta.
I tentativi di coartare gli individui violano il diritto all'informazione, cui successivamente si farà riferimento, diritto funzionale alla piena esplicazione dell'essere umano, asservito a logiche arbitrarie e manipolative.
L'influenza esercitata sugli individui, attraverso la trasmissione di contenuti *ad hoc (*o la non trasmissione di determinati contenuti), selezionati in base al profilo dell'individuo digitale attraverso l'acquisizione dei dati personali, è tesa a condizionare gli utenti per comprometterne l'effettiva possibilità di autodeterminazione.
Riappare la capacità dell'«infosfera» di modellare la realtà circostante.
Pertanto, in una prospettiva di interdipendenza funzionale, emerge come la tutela del diritto alla protezione dei dati dal *microtargeting* politico, basato su trattamenti poco trasparenti ed esclusivamente automatizzati, lesivi dell'art. 22 del GDPR, sia strumentale alla tutela della dignità umana, anch'essa violata, nella sua accezione eudemonologica, da tentativi di manipolazione in ambito politico.
Al contempo, l'inviolabilità della dignità umana, attinta nel caso in questione, consente di rafforzare la protezione dei dati personali[51].

4.1. Gli interventi legislativi europei per contrastare il microtargeting politico: "Una risposta efficace ai tentativi di manipolazione in rete"?

Le riscontrate attività di *targeting* politico in rete hanno indotto le istituzioni europee ad adottare nel 2018 una Comunicazione[52], atta a contrastare la

[50] UNDP, Rapporto sullo Sviluppo Umano 2024/2025 (Capitolo 5), 2025.

[51] In questa prospettiva è possibile fare riferimento a: A. Ruggieri, *La dignità dell'uomo e il diritto di avere diritti (profili problematici e ricostruttivi)*, in *ConsultaOnLine*, 2, 2018, 398.

[52] Commissione europea, Comunicazione COM/2018/236 al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle regioni: Contrastare la disinformazione online un approccio europeo, 2018.
La Commissione europea è intervenuta su questo Codice con la Comunicazione COM/2021/262, ponendosi in un'ottica volta alla co-regolamentazione dei profili di criticità inerenti l'informazione nell'ambiente digitale.

disinformazione online.
La suddetta Comunicazione delineava dei precisi obiettivi per reprimere la disinformazione in rete, quali il miglioramento della trasparenza circa l'origine della notizia, l'implementazione della credibilità della notizia, la promozione della diversità dell'informazione. Questo strumento di *soft law,* basato sull'intervento volontario delle piattaforme, non ha consentito di contrastare effettivamente la disinformazione[53].
Successivamente, le istituzioni europee, hanno adottato una strategia legislativa differente, imponendo degli obblighi ai fornitori di piattaforme online e motori di ricerca online di grandi dimensioni[54]. Nello specifico, gli artt. 34 e 35 del DSA impongono ai suddetti attori privati l'obbligo di valutazione e attenuazione degli eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali[55].
Si potrebbe ritenere che gli obblighi in questione abbiano una valenza programmatica rispetto al *targeting* politico, in quanto recentemente è stato adottato un regolamento[56], volto a disciplinare nello specifico il *targeting* politico, imponendo precipui obblighi ai titolari del trattamento dei dati, che utilizzano i medesimi al fine di condizionare l'orientamento politico degli individui e il pluralismo informativo ("Regolamento").
Dunque, si ritiene che tale Regolamento debba essere al centro delle riflessioni relative all'efficacia della risposta legislativa al *targeting* politico.
Il Regolamento si pone in un'ottica a-territoriale[57] e si connota per dei

---

[53] O. Pollicino - P. Dunn, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione,* cit., 131-135.

[54] I servizi di intermediazione online si dividono in servizi di semplice trasporto consistono nel trasmettere su una rete di comunicazione informazioni fornite da un destinatario del servizio, il servizio di *caching* consiste nel trasmettere su di una rete di comunicazione informazioni fornite dal destinatario del servizio e comporta la memorizzazione automatica e temporanea di tali informazioni e il servizio di *hosting* consiste nella memorizzazione di informazioni fornite dal destinatario su richiesta di quest'ultimo. I motori di ricerca online sono identificati nei servizi intermediari che consentono all'utente di formulare domanda al fine di effettuare ricerche.

[55] A favore del pluralismo informativo le istituzioni europee hanno adottato anche il regolamento (UE) 2024/1083, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE. Per un approfondimento su tale regolamento si rimanda a: O. Pollicino – P. Dunn, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione,* cit., 136 – 139. Nella medesima prospettiva degli obblighi imposti dal DSA si pongono le recenti linee guida della Commissione C/2024/2121 per la salvaguardia dei processi democratici. La Commissione europea, evidenziata nuovamente la capacità manipolativa dei sistemi di raccomandazione dei fornitori di piattaforme e motori di ricerca online, evidenzia come sia necessario che i sistemi di raccomandazione siano trasparenti e programmati in modo tale da limitare la diffusione di contenuti fuorvianti.
Sulla disinformazione e nelle tornate elettorali e le risposte legislative si rimanda a: O. Pollicino – P. Dunn, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)*, in *Federalismi.it*, 12, 2024.

[56] Parlamento europeo e Consiglio, regolamento (UE) 2024/900, relativo alla trasparenza e al targeting della pubblicità politica, 2024.

[57] Il presente regolamento si applica alla pubblicità politica laddove il messaggio di pubblicità politica sia diffuso nell'Unione, sia reso di dominio pubblico in uno o più Stati membri o sia rivolto ai cittadini dell'Unione, indipendentemente dal luogo di stabilimento del prestatore di servizi di pubblicità politica o dal luogo di residenza o stabilimento dello

preliminari riferimenti al frequente uso delle tecniche di *targeting* in rete e ai conseguenti profili di pericolosità che minacciano la democrazia[58].
In prima istanza, il Regolamento impone ai prestatori di servizi di pubblicità politica[59] un generalizzato obbligo di trasparenza, che si estrinseca nell'individuazione dei servizi di pubblicità politica e nella conservazione delle informazioni[60] nell'ambito dei servizi richiesti.
D'altro canto, gli editori di pubblicità politica[61] sono tenuti a rendere edotti gli individui della natura pubblicitaria e politica del messaggio, l'elezione cui il messaggio pubblicitario si riferisce, l'identità dello sponsor[62], l'eventuale utilizzo di tecniche di *targeting*.
Invece, con precipuo riferimento al *targeting*, il Regolamento ancora la possibilità di utilizzare le tecniche di *targeting* a specifiche condizioni, quali la raccolta dei dati presso l'interessato, a seguito del suo consenso al trattamento separato dei dati personali a fini di pubblicità politica. Inoltre, ai fini della legittimità del *targeting* politico viene sancito un divieto di utilizzare i dati sensibili[63] degli individui per la profilazione[64].
In ultima istanza, i titolari del trattamento sono tenuti a comunicare all'interessato informazioni supplementari per consentirgli di comprendere la ratio sottesa alla trasmissione dei contenuti pubblicitari. Oggetto dell'obbligo di comunicazione sono anche gli obiettivi e la logica dell'eventuale *targeting*, gli specifici gruppi di destinatari presi di mira, il periodo di diffusione della pubblicità politica e il numero di persone cui è diffuso il

sponsor, e a prescindere dai mezzi utilizzati.

[58] In ottica definitoria, il Regolamento chiarisce che la pubblicità politica è identificabile nella preparazione, collocazione, promozione, pubblicazione, consegna o diffusione, con qualsiasi mezzo di un messaggio fornito dietro retribuzione o tramite attività interne o nell'ambito di una campagna di pubblicità politica di, a favore o per conto di un attore politico, salvo se di natura meramente privata o commerciale e che possa o sia inteso a influenzare l'esito di un'elezione o un referendum, un comportamento di voto o un processo regolamentare.
Inoltre, al fine di verificare se si tratti di un messaggio di pubblicità politica, il Regolamento fa riferimento a taluni indici quali: contenuto del messaggio, sponsor del messaggio, contesto in cui il messaggio è trasmesso, mezzi con cui il messaggio è preparato, i destinatari e l'obiettivo del messaggio.

[59] Definiti nel Regolamento come le persone fisiche o giuridiche impegnate nella prestazione di servizi di pubblicità politica.

[60] Tra le varie informazioni il Regolamento ricomprende il messaggio di pubblicità politica, i servizi forniti, gli importi fatturati.

[61] Definiti nel Regolamento come le persone fisiche o giuridiche che pubblica, consegna o diffonde pubblicità politica con qualsiasi mezzo.

[62] Lo sponsor viene identificato nel Regolamento come la persona fisica o giuridica per conto della quale è preparato, collocato, promosso, pubblicato un messaggio di pubblicità politica.

[63] Il Regolamento europeo per la protezione dei dati personali definisce i dati sensibili come dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

[64] Il Regolamento ha sancito il divieto di *targeting* politico se quest'ultimo implica il trattamento di dati personali di individui che, con ragionevole certezza, abbiano un anno al di sotto per l'esercizio del diritto di voto.

messaggio politico.
In quest'ottica, il titolare del trattamento è tenuto a riferire all'interessato se per l'indirizzo o la consegna del messaggio pubblicitario sia stata utilizzata l'Intelligenza artificiale.
L'intervento legislativo delle istituzioni europee, non circoscritto al contesto territoriale europeo, è di fondamentale rilievo, in quanto mira a far rientrare nel perimetro della legalità attività lesive del diritto alla protezione dei dati personali e, come visto, della dignità umana.
Al contempo, però, si ritiene di dover sviluppare talune riflessioni critiche in merito alle disposizioni analizzate.
In particolare, si ritiene che ci si debba interrogare sull'"efficacia sanante" del consenso specifico dell'interessato al trattamento dei propri dati personali ai fini della pubblicità politica. Infatti, il consenso consentirebbe comunque una profilazione, sebben limitata e meno efficace, ma comunque mirata al *targeting* e, dunque, in sostanza a una manipolazione informativa nei confronti dell'individuo. Per di più, l'importante divieto circa l'utilizzo delle categorie particolari di dati personali, ai fini della profilazione, non fuga del tutto i dubbi relativi alla possibilità di identificazione dell'utente, deducibile anche attraverso l'estrazione di inferenze, che avviene attraverso il trattamento automatizzato dei *Big Data*, basato sull'utilizzo di sistemi di Intelligenza artificiale.
In questi termini, allora, si potrebbe riflettere sull'indisponibilità del consenso alla cessione dei propri dati personali, funzionale a tutelare il pieno diritto allo sviluppo della personalità umana, quale estrinsecazione dell'inviolabilità della dignità umana (come descritto nel paragrafo 4) da salvaguardare attraverso un ambiente che, nemmeno in minima parte, minacci la democrazia e il pieno dispiegamento pluralismo informativo, necessario per non condizionare l'effettiva fruizione dei diritti politici (il cui effettivo godimento rappresenta un presupposto per non violare il diritto allo sviluppo della personalità umana).
In questa prospettiva, si ritiene che forse il Regolamento si sarebbe dovuto incentrare maggiormente sul rispristino di un ecosistema digitale effettivamente pluralista (e non basato su una selezione, o non selezione predeterminata di contenuti) più che sull'apprezzabile e comunque importante sforzo di rendere il *targeting* trasparente.
Invero, pur ammettendo la possibilità di prestare il consenso al *targeting*, l'applicazione orizzontale dei diritti fondamentali, e in particolare della dignità umana, consentirebbe di avanzare un vaglio sul consenso prestato dall'individuo in un'ottica privatistica, teso a verificare se il medesimo consenso possa incidere negativamente sulla salvaguardia della sua dignità umana, e segnatamente sul tratto eudemonologico, cui si è fatto riferimento.
Il ripristino di un ecosistema digitale pluralista consentirebbe anche di tutelare effettivamente il diritto all'informazione degli individui nella sua più ampia accezione funzionale alla democrazia, sancito dagli artt. 10 della CEDU e 11 della Carta di Nizza[65].

[65] Per un approfondimento sul diritto all'informazione e sulla sua funzionalità alla formazione di «un'opinione pubblica documentata», prodromica al pieno sviluppo della persona si rimanda a: M. Bassini, *Internet e libertà d'espressione. Prospettive costituzionali e*

Tuttavia, l'obbligo di comunicazione dell'attività di *targeting* in atto attenua l'efficacia persuasiva del contenuto trasmesso, in quanto l'individuo dovrebbe essere consapevole del meccanismo manipolativo e del fatto che sia un messaggio selezionato "*ad hoc*" per lui, ma rimane la necessità di verificare come verranno attuate tali prescrizioni.
Infatti, si scorge all'orizzonte la possibilità che i titolari del trattamento continuino a far leva sulla scarsa alfabetizzazione digitale degli utenti, servendosi della loro passiva accettazione, nonché, opacizzando il contenuto delle suddette comunicazioni.
Permane la necessità di interrogarsi sull'efficacia deterrente delle sanzioni previste dal Regolamento, pari al sei per cento dell'entrate o del bilancio annuo o del fatturato mondiale annuo dello sponsor o del prestatore di servizi di pubblicità politica.
Al contempo, però, le perplessità circa l'efficacia delle sanzioni potrebbero essere attenuate dalla riconosciuta facoltà per gli Stati di imporre sanzioni periodiche in caso di violazioni gravi e reiterate.

5. Conclusioni

L'indagine sviluppata nel presente contributo ha fatto emergere come l'odierno ecosistema digitale si serva dei dati personali per mettere in atto strategie manipolative.
Come si è cercato di evidenziare, il tentativo di condizionamento gli individui, attraverso i vari sistemi di cui si fregia l'infrastruttura digitale, anche in ambito politico, fa emergere la violazione del diritto alla protezione dei dati personali e ha fatto sorgere l'esigenza di soffermarsi sull'eventuale violazione della dignità umana.
L'approfondimento in merito alla dignità umana, introdotto dall'illuminata sentenza della Corte costituzionale tedesca, tesa a correlare la protezione dei dati personali con la dignità umana, ha consentito di comprendere come i sedimentati meccanismi manipolativi, basati su opachi trattamenti dei dati personali, siano lesivi anche della dignità umana.
In particolare, si è rilevato come il *targeting* politico sia lesivo del tratto eudemonologico della dignità umana, che si sostanzia nel diritto allo sviluppo della personalità umana, avente come suo corollario i diritti politici.
Infatti, il *targeting* politico, fonte di disinformazione, incide notevolmente sul pieno ed effettivo godimento dei diritti politici, mettendo in atto un meccanismo distorsivo capace di condizionare artificiosamente le scelte degli individui.
Tali evidenze sono un chiaro indice dal quale desumere l'intrusività della rete digitale, tesa a tentare di influenzare le scelte degli individui, asservendoli alle ragioni degli algoritmi, funzionali alla configurazione di un meccanismo condizionante, lesivo della sfera più intima degli individui con forti ricadute sull'effettiva possibilità di dispiegamento del sistema democratico.
L'analisi del regolamento europeo sul *targeting* politico porta ad accoglie-

sovranazionali, Roma, 2019, 194 ss.; N. Pica, *La tutela della libertà di informazione nel Digital Services Act tra contrasto alle "manipolazioni algoritmiche" e limiti alla content moderation*, in questa *Rivista*, 1, 2024, 13 ss.

re positivamente l'importante intervento legislativo, volto a disciplinare questo fenomeno, ma, al contempo, genera delle perplessità in merito alla possibilità di ritenere che limitare o, meglio, moderare il *targeting* sia una risposta efficace per contrastare evoluti meccanismi informatici, atti a creare disinformazione e a incidere artatamente sulla libertà di scelta degli individui.

Si ritiene che dall'inviolabilità della dignità umana, attinta nell'ambiente digitale per i profili descritti, derivino delle riflessioni sulla stessa possibilità di prestare il consenso a cedere i propri dati personali ed essere destinatari di *targeting* politico, che non si sostanzia in una semplice sponsorizzazione del proprio indirizzo politico, ma nel tentativo di plasmare una "realtà informativa", costruita *ad hoc* per l'individuo al fine di manipolarlo.

Dunque, l'inviolabilità dignità umana, ma anche la necessità di preservare la democrazia e il pluralismo informativo, fanno sorgere delle riflessioni sull'indisponibilità del consenso, seppur informato, a essere manipolato.

Abstract

L'articolata evoluzione digitale, caratterizzante il recente periodo storico, ha fatto sorgere molteplici profili di criticità concernenti la tutela dei diritti fondamentali.
La suddetta trasformazione digitale, capace di permeare l'odierno tessuto sociale, ha dato luogo a nuove forme di aggressione nella sfera personale dei consociati.
I dati personali hanno ormai assunto un rilevante valore sul piano economico e sociale, in quanto rappresentano una risorsa indispensabile per profilare i consociati e veicolare contenuti politici ed economici aderenti alle tendenze emerse.
Il sintetico inquadramento operato induce a ritenere che la tutela del diritto alla protezione dei dati personali si ponga come presupposto per la salvaguardia della dignità umana e della democrazia, minacciata dall' "infosfera", che ha quale corollario il targeting politico.

The complex digital evolution, characterizing the recent historical period, has given rise to multiple critical profiles concerning the protection of fundamental rights.
The aforementioned digital transformation, capable of permeating today's social fabric, has given rise to new forms of aggression in the personal sphere of members of society.
Personal data have now assumed a significant value on the economic and social level, as they represent an indispensable resource for profiling members of society and conveying political and economic contents adhering to emerging trends.
The synthetic framework operated leads to the belief that the protection of the right to the protection of personal data is a prerequisite for the safeguarding of human dignity and democracy, threatened by the "infosphere", which has political targeting as a corollary.

Keywords

dignità – democrazia – indisponibilità – pluralismo informativo – dati personali

Dal principio del consenso informato al *Trust-Based Consent*, una possibile traiettoria evolutiva*

Isabella de Vivo

Sommario

1. Introduzione. 2. *Il Trustworthy Ecosystem* delineato dall' AI Act. - 3. La declinazione normativa di *(Trust)worthiness:* tra "accettabilità" del rischio e standardizzazione. - 4. Il caso dei GPAI e la protezione dei dati: la *Sociological Trustworthiness* come antidoto all'irrimediabilità dell'"intrusione digitale". - 5. Le origini di un ritardo costitutivo: l'approccio dualistico alla tutela dei dati e la possibile traiettoria evolutiva: un modello decisionale per il *Trust-Based Consent*. - 6. Potenzialità e limiti del GPAI *Code of Practice* (CoP). - 7. Riflessioni conclusive.

1. Introduzione

Se da un lato il crescente "affrancamento decisionale" dei sistemi di AI dal fattore umano, aprendo la strada allo sviluppo di agenti dotati finanche di piena agentività morale *(full moral agency)*[1], ha sollevato il dibattito circa

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

[1] Stando a quanto emerge dalle riflessioni elaborate nell'ambito della *Machine Ethics (ME),* un sistema di AI può essere considerato alla stregua di un "agente morale" qualora sia in grado di analizzare una situazione in conformità a valori, elaborare le informazioni così ottenute secondo istanze valoriali, prendere delle decisioni che conducano ad atti effettivi e infine rielaborare queste stesse istanze alla luce delle sessioni passate, cfr. G. Tamburrini - F. Fossa, *Ethics of Autonomous Vehicles. From Moral Dilemmas to Social Trade-Offs*, in *Paradigmi, Rivista di critica filosofica,* 1, 2022, 79 ss. Sulla tendenza all'assottigliamento delle differenze percepite tra esseri umani e tecnologie autonome, cfr. F. Fossa, *Robot morali? Considerazioni filosofiche sulla machine ethics,* in *Sistemi intelligenti*, 2, 2020, 425 ss. Sul passaggio dall' *operational morality* come processo inferenziale di riproduzione imitativa del comportamento morale «*a host of cognitive mechanisms*» (W. Wallach, *Robot minds and human ethics: the need for a comprehensive model of decision making,* in *Ethics and Information Technology,* 12, 2010, 243 ss., spec. 249) alla *functional morality* di sistemi che presentano gradi di autonomia e sensibilità a valori che possono variare in modo indipendente, fino alla prospettiva della *full moral agency* come capacità di rendere ragione dei propri atti si veda W. Wallach - C. Allen, *Moral Machines. Teaching Robots Right from Wrong*, Oxford, 2009, 25 ss.; M. Anderson - S.L. Anderson (a cura di), *Machine Ethics,* Cambridge, 2011; J.P. Sullins, *When is a Robot a Moral Agent?* in Anderson e Anderson, 2011, 151 ss. In merito e sull'approccio «*robot-centred*» nella *Human Robot Interaction* (HRI)

l'opportunità o meno di riconoscere autonomia giuridica agli "agenti elettronici",[2] dall'altro la capacità d'impatto di tali sistemi sulla sfera sociale, etica e giuridica del soggetto umano, unitamente alla pervasività della computazione che essi sottendono - non poteva non stimolare una rinnovata riflessione sull'idoneità degli attuali strumenti di tutela a garantire la persistenza del presupposto implicito attorno al quale le categorie giuridiche sono costruite i.e. "il sé giuridico" - quale *locus* di sovranità cognitiva e libera formazione della volontà rispetto alla disposizione dei diritti[3].
Leggendo l'intersezione tra l' «ecosistema basato sulla fiducia» delineato dall'AI Act[4] e gli strumenti di protezione di privacy e dati personali apprestati dal GDPR[5], scopo di questo contributo è provare ad inquadrare le effettive potenzialità ed i limiti dello stato dell'arte della regolazione nel garantire le condizioni che, alla luce delle tradizioni costituzionali europee comuni[6], si vogliono irrinunciabili a tutela della libertà di scelta e azione, fondamento dei processi di costruzione identitaria[7], anche nell'ecosistema

si veda U. Pagallo *The laws of robots: crimes, contracts, and torts,* Dordrecht, 2013.

[2] In particolare si è discusso in seno al Parlamento europeo, a partire dalla risoluzione del 16 febbraio 2017 (c.d. Carta della Robotica) della possibilità di introdurre nel framework normativo, un inedito *tertium genus*, interposto tra persone fisiche e persone giuridiche: la c.d. "personalità elettronica" quale *fictio iuris* ultronea, necessaria ad inquadrare il peculiare status dell'"agente elettronico" nella sua capacità di comunicazione, interazione e interferenza con l'agency umana.

[3] In termini giuridici, l'erosione dell'autonomia cognitiva e la riduzione della percezione di controllo sulle proprie azioni e informazioni possono influenzare la capacità di un individuo di esprimere un valido consenso, principio fondamentale nel diritto contrattuale e nella tutela della privacy e della protezione dei dati. In generale per le implicazioni della mediazione tecnologica e del suo impatto sulla formazione dell'identità e sull'agency, si veda S. Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Othe*r, New York, 2011. Sull'erosione dell'autonomia cognitiva e della privacy individuale, derivanti dalla sorveglianza pervasiva e dalle intrusioni tecnologiche, si veda N. M. Richards, *The Dangers of Surveillance*, in *Harvard Law Review*, 126, 7, 2013, 1934 ss. Sui quattro principali rischi connessi all'AI, individuati nell' erosione di controllo, responsabilità, autodeterminazione e svalutazione delle competenze umane, si vedano L. Floridi – J. Cowls – M. Beltrametti – R. Chatila – P. Chazerand – V. Dignum – C. Luetge – R. Madelin – U. Pagallo – F. Rossi – B. Schafer – P. Valcke – E. Vayena, *AI4People – An Ethical Framework For A Good AI Society: Opportunities, Risks, Principles, And Recommendations,* in *Minds And Machines*, 28, 4, 2018, 689 ss.

[4] 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), da questo momento "AI Act".

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), da questo momento "GDPR".

[6] Sul ruolo dei valori identificati dall'art. 2 del Trattato sull'Unione europea nel delineare il concetto di identità costituzionale europea si veda Parlamento Europeo, *The notion of constitutional identity and its role in European integration,* in europarl.europa.eu, 2024. In dottrina sul patrimonio costituzionale comune europeo si veda A. Pizzorusso, *Il patrimonio costituzionale europeo,* Bologna, 2002.

[7] È implicito in quest'impostazione il riconoscimento del legame costitutivo tra processi di costruzione identitaria e libertà cognitiva. Sull'impatto delle tecnologie algoritmiche

«bioipermediale»[8].

Il quesito preliminare da cui il percorso d'analisi muove, è la misura in cui la declinazione normativa di *(Trust)worthy AI* proposta dal legislatore europeo dell'AI Act, paradigma chiave per sbloccare il potenziale tecnologico da un lato e comunicare la garanzia dei diritti fondamentali dall'altro, riesca a garantire margine di autonomia decisionale - che il concetto socio-tecnico di "affidabilità" di per sé implica - ai destinatari delle tecnologie (c.d. *Human Recipients*- HR)[9] nella negoziazione circa l'*an* ed il *quomodo* dell'ammissibilità del rischio, a partire dalla definizione dalle condizioni che legittimano il trattamento *AI-driven* dei dati (anche) personali.

Nella prima sezione del contributo, dopo aver brevemente introdotto l'ampio dibattito interdisciplinare in merito al concetto di *Trust in Technology*[10], si evidenzieranno i limiti dell'approccio "espertocratico" sposato dal legislatore europeo dell'AI Act, nel raggiungimento di un simile obiettivo. Analizzando la sovrapposizione tra standardizzazione tecnica e compliance normativa (*i.e.* accettabilità del rischio) vedremo come l' etichetta di (*Trust)worthiness* che ne deriva, non soltanto non sia sufficiente ad integrare la nozione «umano-centrica»[11] di affidabilità emergente dalle Linee Guida Etiche redatte nel 2019 dalla Commissione europea[12], ma come, al contrario, attribuendo un ruolo centrale agli organismi di normazione tecnica, quali mediatori fiduciari di ultima istanza, esautori la partecipazione ed il controllo democratico da parte degli HRs nel giudizio di conformità etico-normativa che la quantificazione del rischio "tecnico" necessariamente presuppone. Oscurando l'apparente neutralità del giudizio di standardizzazione e dunque la natura coercitiva della traduzione normativa di "fiducia ben riposta" che a tale giudizio consegue in via automatica, tale approccio non può che incrementare l'asimmetria epistemica e decisionale

sulla dimensione socio-etica nella costruzione dell'identità personale si veda S. Tiribelli, *Identità personale e algoritmi: una questione di filosofia morale*, Roma, 2023, spec.15. In tema, sia consentito rimandare anche a I. de Vivo, *Il sé allo specchio dell'algoritmo. Libertà epistemica e identità individuale,* in A. Sterpa, C. Capasso - A. Cortazzo - I. de Vivo, et al. (a cura di), *L'ordine giuridico dell'algoritmo*, Napoli, 2024, 24 ss.

[8] Sulla definizione di «*bio-hypermedia*» come dimensione costituita dall' integrazione tra biotecnologie e tecnologie dell'informazione, che influenza e modifica le capacità cognitive e fisiche umane attraverso l'interfaccia con dispositivi digitali avanzati cfr. G. Griziotti, *Neurocapitalismo, mediazioni tecnologiche e linee di fuga*, Milano, 2016.

[9] Con la locuzione, da questo momento HRs, si intende la generalità dei soggetti umani che entrano in relazione con l'AI e che in media presentano un potere limitato di resistere alle conseguenze negative dell'impatto nella loro vita quotidiana, cfr. M. Findlay - J. Seah - W. Wong, *AI and Big Data*, Cheltenham, 2023. Con *Host Communities,* da questo momento HCs si intendono le comunità, i gruppi e categorie di individui impattati da una determinata tecnologia.

[10] Per una panoramica delle diverse prospettive di indagine coinvolte si veda W.S. Volkmann - F. Linus, *Trust in technology: interlocking trust concepts for privacy respecting video surveillance*, in *Journal of Information,* in *Communication and Ethics in Society*, 19, 2021, 506 ss.

[11] In merito all'approccio umano-centrico che informa la concezione tripartita dell'AI affidabile (legalità, eticità, robustezza tecnica) di cui alle Linee Guida, si veda *infra.*

[12] Cfr. *ethics-guidelines-trustworthy-ai*, 2019, spec. 14. Le Linee Guida sono state elaborate da un gruppo di esperti: l'"*High-Level Expert Group on AI"* (AI-HLEG), nominato appositamente dalla Commissione, in merito si veda più ampiamente *infra.*

tra providers, regolatori e destinatari delle tecnologie. Se così intesa, l'idea di *Trustwhortiness*, rischia di minare *ex ante* esattamente quel principio di autodeterminazione che la regolazione umano-centrica dell'AI si prefigge di garantire.

Nella seconda parte dell'analisi, si metterà in luce come la necessità di recuperare la più ampia nozione sociale di *Trust* e *Trustworthiness,* intendendo quest'ultima come esito di "processo" decisionale orizzontale e negoziato tra regolatori, providers e HRs, diventi particolarmente urgente laddove si prenda atto di quello che sembra essere il ritardo costitutivo del taglio civilistico alla tutela dei dati - motore dello sviluppo dei sistemi di AI - nel garantire quel fascio di diritti che si irradiano dal «prisma»[13] dell'identità personale, sfera incomprimibile di autonomia e disposizione autoriale dei diritti.

Concentrando quindi specificamente l'analisi sulle sfide (apparentemente) inedite poste dalla rapidissima ascesa dei modelli Intelligenza Artificiale Generativa (Gen-AI)[14] cosiddetti "a finalità generali" (GPAI), si darà conto dei limiti che gli attuali strumenti di tutela incontrano, a partire dalla discussione del principio dicotomico che distingue tra dati personali e dati "esterni"[15] su cui il GDPR fa perno. Di fronte a quella che sembra essere l'incompatibilità ontologica tra i principi informatori della liceità del trattamento dei dati personali[16] e l'*AI-driven ecosystem* - che il lancio degli LLMs ha avuto il merito di rendere di palmare evidenza - si argomenterà come, a prescindere da specifici adeguamenti all'attuale framework normativo, ciò che primariamente appare necessario è un più radicale cambio di prospettiva che, spostando il focus dal *quid* (quali dati), all' *an* ed al *quomodo* della computazione, sia in grado di anticipare tutela di privacy e dati personali, ad un momento che precede l'irreversibilità dell'intrusione digitale nella sfera del soggetto.

Mutamento prospettico questo, che solo un ripensamento critico del ruolo della fiducia come forma di consenso dinamico, basato sulla negoziazione ed il controllo democratico del rischio tecnologico, sembra in grado di garantire.

La partecipazione orizzontale, la supervisione e la trasparenza del processo decisionale che definisce *ex ante* "l'affidabilità" di un sistema e delle sue modalità di computazione, da parte degli HRs appare, infatti, precondizione per restituire quella libertà nella disposizione dei diritti che il consenso informato al trattamento dati non può, seppur implicitamente,

---

[13] «Un diritto fondamentale è trasparente e sembra un oggetto chiaramente definito, ma appena la luce lo illumina e lo attraversa, il diritto si disperde in uno spettro di interessi, valori e persino di altri diritti (..)» J. Gerards, *The prism of fundamental rights,* in *European Constitutional Law Review*, 8, 2, 2012, 173 ss., traduzione a cura dell'autrice.

[14] Sulla definizione di Intelligenza Artificiale generativa (GenAI) e di *General-Purpose AI* (GPAI) si veda *infra.*

[15] Con la locuzione si fa riferimento ai dati giuridicamente non personali e che dunque esulano dal raggio applicativo del GDPR.

[16] Cfr. art. 5, par. 1, GDPR che stabilisce i principi fondamentali per il trattamento dei dati personali tra cui liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.

non presupporre.
Attraverso questa lente si rifletterà sul futuro ruolo del c.d. *Code of Practice,* destinato a fungere da facilitatore di compliance per i providers di modelli GPAI e attualmente in fase di redazione, analizzando criticamente le possibilità di apertura del processo di standardizzazione, ad oggi, concretamente offerte dal coinvolgimento di soggetti interessati, sviluppatori, società civile accademia e regolatori nei processi di standardizzazione del rischio.
Come si argomenterà in conclusione, sulla base di un approccio che definiamo "ecologico" volto a garantire il coinvolgimento orizzontale di soggetti interessati, comunità ospitanti (HCs) e società civile lungo tutta la catena di valore, alternativo all'approccio puramente espertocratico, è possibile tracciare le linee di azione per dare contenuto ad un'idea di consenso all'immissione degli agenti artificiali e alle relative modalità computazionali, inteso come "processo" dinamico e "*Trust Based*". Strumento normativo, questo, non solo volto ad evitare che il paradigma della fiducia si trasformi in un paradosso concettuale,[17]ma soprattutto in grado di sbloccare il ritardo ontologico di una regolazione che sembra non potersi dare se non ad "intrusione digitale" - già e irrimediabilmente - data. Affinché ciò sia realizzabile, e proprio alla luce della persistente asimmetria che continua a caratterizzare il rapporto tra le parti interessate –dimostrata dal confronto multistakeholder attualmente in corso per la redazione del *Code of Practice* – si impone la necessità di rafforzare quelle condizioni sostanziali e procedurali idonee a garantire una reale redistribuzione del potere di accesso, controllo e azione degli stakeholders, limitando l'accentramento epistemico e decisionale dei providers. Obiettivo che non può non presupporre, da un lato, la denaturalizzazione della visione dell'AI come "prodotto", dall'altro, la costruzione di un'*AI-literacy* di natura critica, che, andando oltre la dimensione meramente funzionale, renda gli HRs consapevoli della natura dei rischi posti dall'immissione degli agenti di AI e della pervasività computazionale che questi sottendono.

2. Il *Trustwhorty Ecosystem* delineato dall' AI Act

«We should ask not what our concept is, but what it ought to be, if we wish the notion to do useful conceptual work».[18]
Come affermato dalla Commissione europea nel Libro Bianco sull'intelligenza artificiale del 2020,[19] l'assenza di fiducia rappresenta uno dei princi-

[17] Parla a tal proposito di «*conceptual nonsense*» [orig. *begrifflicher Unsinn*], T. Metzinger, in *Nehmt der Industrie die Ethik weg! EU-Ethikrichtlinien für Künstliche Intelligenz.* in *Tagesspiegel.de.* 2019 tra gli esperti redattori delle linee guida per l'AI affidabile cfr. *Ethics Guidelines for Trustworthy AI*, cit. Sul paradosso comunicativo insito nell'AI Act si veda anche I. Kusche, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk,* in *Journal of Risk Research,* 2024, 1 ss.

[18] K. Jones "*Trust.*" in *International Encyclopedia of Ethics,* Hoboken, 2020.

[19] European Commission, *White Paper on Artificial Intelligence: a European approach to excellence and trust,* 19 February 2020.

pali fattori che ostacolano la diffusione dell'AI[20] e il "*Trustwhorty Ecosystem"* muove dal preciso scopo di rimuovere tale ostacolo.[21]
È chiara dunque la consapevolezza che promuovere "l'affidabilità" risponda ad un'istanza critica nell'ecosistema digitale, rappresentando, pertanto, l'opzione più promettente per regolatori e tecnologi per promuovere e sbloccare il potenziale innovativo delle tecnologie di AI[22] e, nel contempo, affrontare i rischi associati al suo utilizzo.[23] Nel nuovo framework normativo delineato dall'AI Act assurge dunque, a strategia chiave per comunicare e garantire "l'accettabilità" del livello di rischio posto dai sistemi di AI ai diritti fondamentali ed è quindi destinato a fungere da paradigma di riferimento nei processi decisionali tanto a livello di governance, quanto nella quotidiana relazione tra agenti umani ed artificiali.[24]
In considerazione della centralità del tema, il concetto di *Trust in Technology* è, del resto, da tempo al centro di un ampio dibattito interdisciplinare che ha coinvolto e coinvolge tanto la prospettiva filosofica, quanto la riflessione etico-politica concentrata a delineare contorni e significato della declinazione normativa di fiducia (*Trust*) – ed il suo correlato speculare di (*Trust)whortiness*.
Se probabilmente non è possibile fornire una definizione univoca del concetto di fiducia, in grado di integrare le diverse prospettive di indagine,[25] tuttavia, almeno per quanto attiene le concezioni normative, l'ambito originario di concettualizzazione risiede primariamente nella dimensione delle relazioni interpersonali e questo vale anche nel campo delle tecnologie digitali.[26]
La fiducia infatti è prima di tutto un'attitudine ed una proprietà del fiduciante (*Trustor)*, che deriva dall'affidabilità percepita del fiduciario (*Trustee*).[27] Per quanto frutto di un atteggiamento mentale non completamente

[20] *White Paper,* cit., 9.

[21] Ivi*,* 3.

[22] A. Drake - P. Keller - I. Pietropaoli - A. Puri - S. Maniatis - J. Tomlinson - J. Maxwell - P. Fussey - C. Pagliari - H. Smethurst - L. Edwards - S. W. Blair, *Legal contestation of artificial intelligence-related decision-making in the United Kingdom: Reflections for policy*, in *International Review of Law, Computers and Technology*, 2022, 251 ss. O. O'Neill, *A Point of View: Which comes first - trust or trustworthiness?* in *bbc.com,* 2012.

[23] Sul duplice obiettivo che muove il legislatore europeo, si veda I. Kusche, *Possible harms of artificial intelligence*, cit.

[24] Cfr. considerando 8(2) AI Act.

[25] Il concetto di "fiducia" si è sviluppato all'interno ed all'esterno del dibattito filosofico e, nonostante le riserve circa l'applicazione delle categorie ermeneutiche sviluppate primariamente nel contesto di interazioni dirette tra individui all'ambito della tecnologia, negli ultimi decenni si è assistito a un persistente interesse sul tema con il consolidamento nell'ambito della sicurezza informatica di concetti come "*trusted hardware", "roots of trust"* or "*chains of trust*", si veda M. Tehranipoor - C. Wang, *Introduction to Hardware Security and Trust*; New York, 2012; *GlobalPlatform Root of Trust Definitions and Requirements 1,* 2018.

[26] Si veda S. Weydner -Volkmann - L. Feiten, *Trust in technology: interlocking trust concepts for privacy respecting video surveillance,* in *Journal of Information, Communication and Ethics in Society,* 19, 2021, 506 ss.

[27] Nell'ambito delle teorie interpersonali, la fiducia è infatti generalmente intesa come un atteggiamento e l'affidabilità come una proprietà cfr. C. McLeod. *'Trust',* in E. N. Zalta *(ed), The Stanford Encyclopedia of Philosophy*, Metaphysics Research Lab, Stanford, 2021.

razionale, come la letteratura sull'*Algoritmic Aversion* (A.A.)[28] dimostra, è la cifra che ha il potenziale di trasformare coloro che sono soggetti a decisioni altrui in decisori a loro volta, nella misura in cui accettano o meno di accordare la loro fiducia a tali decisioni, umane o algoritmiche che siano, assumendo contestualmente il rischio e la responsabilità delle possibili conseguenze indesiderate di tale scelta.[29]

Se, dunque, la dimensione della fiducia riposa nella relazione tra controparti umane, e nonostante le iniziali riserve avanzate in dottrina sulla possibilità di estendere un simile concetto all'interazione con agenti artificiali,[30] la considerazione di una tecnologia come *trustworthy,* o "degna di fiducia", per dirsi tale non potrebbe, in ogni caso, limitarsi al campo della sicurezza informatica (*Technical Reliability*) a garanzia del rischio tecnico.[31] Questo in particolare alla luce di quanto statuito dagli «Orientamenti Etici per un'AI Affidabile» redatti dall'High-Level Expert Group on AI (AI-HLEG)[32] ove

[28] Cfr. B. J. Dietvorst - J. P. Simmons - C. Massey, *Algorithm Aversion: People Erroneously Avoid Algorithms after Seeing Them Err,* in *Journal of Experimental Psychology*, 144, 2015, 114 ss.; H. Mahmud - A.K.M. N. Islam - S. I. Ahmed - K. Smolander, *What influences algorithmic decision-making? A systematic literature review on algorithm aversion,* in *Technological Forecasting and Social Change*, 175, 2022. Si veda anche S.M. Jones-Jang - Y.J. Park, *How do people react to AI failure? Automation bias, algorithmic aversion, and perceived controllability,* in *Journal of Computer-Mediated Communication*, 28, 1, 2023.

[29] «*Anybody who trusts assumes the risk of misplacing this trust, facing the unwanted outcome after all*», cfr. P. Sztompka*, Trust: a Sociological Theory,* Cambridge, 2003.

[30] Secondo la teoria della mente la fiducia è conseguenza della capacità di ascrivere stati mentali al *trustee*, pertanto l'assenza (almeno fino ad adesso) di qualità comparabili a quelle umane come l'agency morale, ossia la capacità di determinare autonomamente le loro motivazioni, e dunque l'intenzionalità, impedirebbe di considerare i sistemi di AI *trustable*, ma al più *reliable* cfr. B. Miller – O. Freiman, *Trust and Distributed Epistemic Labor*, in J. Simon (ed.), *The Routledge Handbook of Trust and Philosophy,* London, 2019, 341 ss.; si veda anche C. McLeod, *Trust,* cit. In caso di *operational morality* infatti l'azione morale è eterodiretta, per cui i sistemi di AI possono fissare obiettivi, pianificare ed eseguire azioni per raggiungerli, sulla base di una programmazione anche morale, ma è cosa diversa dall'avere stati mentali, motivazioni o un senso di obbligo morale.

[31] In particolare nell'ambito della IT-*Security* si distingue, infatti, tra *realibility* che attiene alla robustezza interna del sistema (malfunzionamenti e danni intrinseci) e *security* - che riguarda la robustezza esterna contro gli attacchi deliberati da parte di *malicious actors.* Tuttavia, la necessità, e non solo la possibilità, di supportare empiricamente la creazione di fiducia nel contesto socio-politico dei non esperti è ampiamente condivisa in letteratura; si veda *ex multiis* S. Weydner - Volkmann - L. Feiten, *Trust in technology,* cit., in cui gli aa. andando oltre non soltanto la prospettiva della *IT-security*, ma anche la dimensione della fiducia interpersonale (tra utenti e progettisti in qualità di *trust mediators*) elaborano un concetto socio-tecnico di trust quale risultato dell'interazione tra diversi livelli e dimensioni necessariamente interconnessi e co-dipendenti.

[32] I sette requisiti chiave per l'affidabilità identificati in: *Human agency and oversight; robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; accountability,* fanno perno su quattro principi etici: rispetto dell'autonomia umana, prevenzione del danno, equità ed esplicabilità, poi confluiti nell' attuale "*ecosystem of trust"* delineato dell'AI Act; cfr. *Ethics Guidelines for Trustworthy AI,* cit. Questi si basano a loro volta, su un precedente documento redatto gruppo di esperti che individuano appunto quattro rischi principali dell'AI, ossia: (i) svalutare le competenze umane; (ii) rimuovere la responsabilità umana;(iii) ridurre il controllo umano; (iv) erodere l'autodeterminazione umana, cfr. L. Floridi et al., *AI4People – An Ethical Framework For A Good AI Society*, cit.

la robustezza tecnica emerge quale requisito *inter alias* - necessario, ma non sufficiente - ad integrare la nozione "umano-centrica di affidabilità"[33]e dei suoi principi informatori, il cui fondamento comune riposa nella tutela della dignità e dell'autodeterminazione umana.[34]

Se quindi le concezioni consolidate di fiducia nel campo della sicurezza informatica possono giustificare una valutazione di *reliability* da parte degli esperti tecnici, il concetto di «tecnologia affidabile» (*trustworthy technology*), così come promossa dall'approccio umano-centrico che informa l'AI Act, dovrebbe permettere invece di considerare la prospettiva di coloro che diventano effettivamente vulnerabili al rischio di danno derivante dall'uso (e/ o abuso) di una determinata tecnologia in un dato contesto operativo[35] quale "meta-condizione" per garantire a monte controllo, responsabilità e autodeterminazione[36] delle controparti umane.

Considerando, allora, che la possibilità di esistenza di un determinata tecnologia, così come il suo significato e il suo utilizzo non può che darsi se non all'interno di relazioni e strutture sociali preesistenti,[37] il concetto socio-tecnico di affidabilità può e deve integrare al requisito della robustezza tecnica- parametro di riferimento del processo decisionale "esperto"- i diversi livelli che attengono relazioni fiduciarie interconnesse, interpersonali e istituzionali, nella valutazione del rischio di danno - anche immateriale - posto dall'introduzione di nuove tecnologie nell'ecosistema.

La fiducia infatti, come il legislatore dell'AI Act non manca di prendere atto, è intimamente connessa al rischio,[38] concetto a sua volta prettamente moderno che - pur muovendo dall'incertezza della relazione tra presente e futuro - fa leva sul ruolo chiave svolto dai processi decisionali umani nel plasmare la direzione degli eventi.[39] Se valutare il rischio significa scegliere

---

[33] Sui limiti dell'approccio *human centered* nell' affrontare le sfide poste dalle tecnologie emergenti *ex se*, ed i relativi impatti ambientali, si veda U. Pagallo, *Dismantling Four Myths in AI & EU Law Through Legal Information 'About' Reality*, in: H. Sousa Antunes – P. M. Freitas – A. L. Oliveira – C. Martins Pereira – E. Vaz de Sequeira – L. Barreto Xavier (a cura di), *Multidisciplinary Perspectives on Artificial Intelligence and the Law. Law,* 2024, 251 ss.

[34] Cfr. *Ethics Guidelines for Trustworthy AI,* cit.

[35] Che, appunto, nella maggior parte dei casi, sono utenti non esperti, si veda S. Weydner-Volkmann – L. Feiten, *Trust in technology*, 4.

[36] Cfr. L. Floridi et al., *ibidem.*

[37] Si vedano L. Sartori – A. Theodorou, *A sociotechnical perspective for the future of AI: narratives, inequalities, and human control*, in *Ethics and Information Technology,* 24, 1, 2022.

[38] Si veda a tal proposito il considerando 64(1) dell'AI Act che si riferisce esplicitamente all'affidabilità in combinazione con la nozione di accettabilità del rischio e standardizzazione tecnica: «*In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service*». Sulla relazione intrinseca tra fiducia, affidabilità e l'accettabilità percepita dei rischi cfr. W. Poortinga – N.F. Pidgeon, *Trust in risk regulation: Cause or consequence of the acceptability of GM food*? in *Risk Analysis*, 25, 1, 2005, 199 ss. Sulla stretta relazione tra rischio e fiducia istituzionale, in particolare tra *trust, risk regulation*, e *perceived acceptability of risks* nell'AI Act si veda J. Laux, – S. Wachter, – B. Mittelstadt, *Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk*. in *Regulation & Governance*, 18, 1, 2024, 3 ss.

[39] Cfr. N. Luhmann, *What Is Communication?* in *Communication Theory*, 2, 1992, 251 ss. Id. *Trust and Power*, Hoboken, 2017, 23. Si veda anche I. Kusche*, Possible harms of artificial intelligence*, cit. Sul ruolo del rischio quale da proxy per il processo decisionale, basato sulla

di agire sulla base delle probabilità che si verifichi un determinato danno e l'entità delle conseguenze che tale danno può comportare,[40] speculare ed opposto al rischio è invece il concetto di pericolo, ossia la probabilità che un danno possa verificarsi in conseguenza ad eventi esterni su cui non si ha controllo, come accade anche nel caso di esposizione coercitiva a decisioni altrui.[41] Assumersi il rischio insito nell' affidarsi ad altri nel plasmare il proprio futuro è allora una decisione in sé che, tuttavia, per potersi dire tale, ha bisogno non soltanto di un terreno informativo su cui costruirsi, ma presuppone un processo dinamico e bidirezionale di costante negoziazione tra volontà di fidarsi da parte del *Trustor* ed esibizione di indicatori di affidabilità - individuati nella letteratura sociologica in "competenza", "benevolenza" e "integrità"[42]- da parte del *Trustee.*[43]

Se così è, il concetto di affidabilità di una tecnologia dovrebbe quindi presupporre opportuni meccanismi di controllo, comunicazione e responsabilità in grado di garantire la sussistenza e permanenza di tale relazione fiduciaria nei soggetti, organismi e istituzioni chiamati a garantirla, in qualità di *Trust Mediators.*[44] Questo è particolarmente vero laddove la "regolamentazione basata sul rischio"[45] - tesa a dare priorità e indirizzare l'azione di contrasto in modo proporzionato al pericolo effettivo, "calibrando" l'applicazione della legge sulla base di punteggi di rischio concreti[46] – come accade nell'AI Act, veda un' inedita estensione applicativa: per la prima volta infatti il paradigma del rischio è mirato all' ottimizzazione degli obiettivi costituzionali in relazione a tutti i diritti fondamentali potenzialmente coinvolti nell'uso dei sistemi di AI.[47] Tuttavia la combinazione di

previsione di eventi futuri positivi e negativi R. Gellert, *The Risk-Based Approach to Data Protectio*n, Oxford, 2020.

[40] Si veda R. Gellert, *ibidem,* spec. 27.

[41] Si veda M.G. Christoffersen, *Risk, Danger, and Trust: Refining the Relational Theory of Risk*, in *Journal of Risk Research,* 21, 2018, 1233 ss. spec. 1236-39. Si rimanda anche a N. Luhmann, *Risk: A Sociological Theory*, New York, 2002.

[42] Sugli indicatori di affidabilità percepita di veda T. Zurek – A. Wyner – T. van Engers, *The Model of Benevolence for Trust in Multi-Agent Systems*, in *Agent & Multi-Agent Systems: Technologies and Applications* (KES-AMSTA 2024), 19-21 June 2024.

[43] Si veda B. Pickering, *Trust, but Verify: Informed Consent, AI Technologies, and Public Health Emergencies*, in *Future Internet*, 13, 5, 2021.

[44] Sul ruolo dei *trust mediators* e in particolare sulla funzione di *proxy trusties* svolta da piattaforme e *sharing services* in funzione vicaria a persone e istituzioni, si veda B. Bodo', *The Commodification of Trust, in Blockchain & Society Policy Research,* in *Lab Research Nodes*, 1, 2021.

[45] Cfr. Considerando 14, AI Act. In merito e sulla differenza tra *risk based approach* e regolamentazione del rischio *strictu sensu* (*risk approach*) si vedano G. De Gregorio – P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age,* in *Common Market Law Review,* 59, 2022, 473 ss. M. E. Kaminski, *Regulating the Risks of AI,* in *Boston University Law Review*, 103, 2023, 1347 ss.

[46] C. Quelle*, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach*, in *European Journal of Risk Regulation*, 9, 3, 2018, 502 ss. spec. 509, citato in G. De Gregorio – P. Dunn, *The European Risk-Based Approaches,* cit., spec. 475.

[47] Se questo è insolito dal punto di vista della ricerca sociologica sul rischio, lo è anche dal punto di vista della regolazione. I precedenti casi di regolamentazione dei rischi delle

due approcci normativi fondamentalmente diversi, il diritto sulla sicurezza dei prodotti da un lato e la protezione dei diritti fondamentali dall'altro,[48] sembra ripercuotersi "a cascata" sul concetto normativo di *trustworthiness,* finendo con l'oscurare tanto la dimensione interpersonale, quanto quella istituzionale implicata nella più ampia accezione[49] del termine.

3. La declinazione normativa di *(Trust) worthiness*: tra "accettabilità" del rischio e standardizzazione

La descritta accezione socio-politica, alla base della concezione dinamica e negoziata del concetto di *trustworthiness* è esattamente ciò che sembra oscurato dall'approccio espertocratico[50] sposato dal legislatore europeo. In ragione, infatti, di quella che sembra essere la sovrapposizione concettuale e operativa tra i processi di standardizzazione tecnica e la valutazione - squisitamente politica- dell'accettabilità del rischio posto dai "prodotti" di AI alla categoria immateriale dei diritti fondamentali, saranno, come vedremo, gli Organismi di Standardizzazione Tecnica (SSOs), ossia le Organizzazioni europee di normazione (ESO), nella redazione delle specifiche tecnico qualitative, ad essere chiamati a svolgere il ruolo di principali *Trust Mediators,* con la conseguenza, di rendere coercitiva l'etichetta di affidabilità. Stando al dettato normativo infatti, il rispetto dei criteri di standardizzazione tecnica, *i.e.* la conformità alla normativa europea armonizzata[51]

nuove tecnologie, ad esempio energia nucleare o ingegneria genetica, si concentrano specificamente sui pericoli per salute e sicurezza di esseri umani e ambiente. Su questo ed ulteriori rilievi si veda I. Kusche, *Possible harms of artificial intelligence,* cit.*;* P. Palka, *Data Management Law for the 2020s: The Lost Origins and the New Needs,* in *Buffalo Law Review,* 68, 2020, 559 ss. Anche nel GDPR la categorizzazione del rischio è strumento emergente di regolazione in relazione specifica alla privacy e alla protezione dei dati, non quindi all'ottimizzazione generale degli obiettivi costituzionali.

[48] Sulle tensioni normative che necessariamente derivano dalla combinazione dei due approcci si vedano M. Almada - N. Petit, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?* in *Robert Schuman Centre for Advanced Studies Research Paper*, 59, 2023, che a proposito coniano la metafora *«medley»* per indicare il mix tra diritti fondamentali e sicurezza dei prodotti che caratterizza l'AI Act, spec. 12. Cfr. anche J. Laux – H. Ruschemeier, *Automation Bias in the AI Act: On the Legal Implications of Attempting to De-Bias Human Oversight of AI*, in *arXiv,* 2025.

[49] Per un'ampia trattazione delle diverse e co-implicate dimensioni della fiducia (interpersonale- istituzionale, epistemica) e su come queste siano chiamate ad interagire nell'ambito dell'AI si vedano R. Gillis – J. Laux – B. Mittelstadt, *Trust and Trustworthiness in Artificial Intelligence,* in R. Paul, E. Carmel and J. Cobbe (eds.), *Handbook on Public Policy and Artificial Intelligence,* Cheltenham, 2024, 181 ss. Per un'ulteriore ed approfondita trattazione della dimensione sociale della fiducia si rimanda anche a I. Kusche, *Possible harms of artificial intelligence,* cit.

[50] Diffusamente sull'«*expertocratic model*» nella valutazione dell'affidabilità, cfr. J. Laux - S. Wachter - B. Mittelstadt, *Trustworthy Artificial Intelligence*, cit., 18. In generale critici in relazione al tale approccio J. Smakman – M. Davies – M. Birtwistle, *Critical Mission: Lessons from Relevant Sectors for AI Safety, The Ada Lovelace Institute.org.* 2023.

[51] Ai sensi dell'art. 2, par. 1, c), del regolamento (UE) 2012 n.1025, si intende per *Harmonised Standard* «una norma tecnica europea, adottata sulla base di una richiesta

crea, una presunzione (cfr. artt. 40,1 e 43)[52] di conformità *de iure* ai requisiti dell'AI Act. La valutazione tecnico-formale del rischio funge dunque da "marchio di garanzia" del rispetto dei diritti fondamentali potenzialmente lesi dallo sviluppo ed immissione dei sistemi di AI ed in conseguenza della loro affidabilità, costruita, a sua volta, come una variabile indipendente di tale marcatura di conformità.

Se così è, laddove l'AI Act lascia margine di discrezione a chi applica le sue norme per determinare la soglia tecnica di accettabilità del rischio, delega necessariamente e in conseguenza, il bilanciamento tra diritti fondamentali che vi è sotteso. Per quanto infatti il regolamento adotti un approccio prescrittivo alla regolamentazione del rischio,[53] stabilendo *ex ante* le categorie di riferimento, a differenza di quanto avviene nel GDPR, non può e non potrebbe eliminare il carattere contestuale implicito a quello che, come visto, si risolve in un giudizio di conformità etico-politica. Il ruolo e le procedure adottate dai soggetti "delegati" a compiere il bilanciamento di diritti e valori in gioco e standardizzarlo, diventa dunque cruciale.

Se, come già chiarito dalla Commissione nelle già citate Linee Guida Eti-

della Commissione (*Standardization Request* - SR) ai fini dell'applicazione della legislazione dell'Unione sull'armonizzazione». Gli organismi coinvolti in questo caso oltre all' *European Committee for Standardization* (CEN) e l'*European Committee for Electrotechnical Standardization* (CENEC) sono gli Organismi Nazionali di Normazione (*National Standardization Bodies*-NSB, in Italia CEI e UNI); le organizzazioni europee degli stakeholders, i consulenti per le norme armonizzate. L' AI Act si basa dunque sul cosiddetto Nuovo Approccio dell'UE (oggi *New Legislative Framework* - NLF) che stabilisce i regimi di regolamentazione tecnica in base ai quali i produttori valutano la conformità dei loro prodotti ai requisiti essenziali di legge, prima di immettere il prodotto sul mercato; in merito si veda M. Veale – F. Zuiderveen Borgesius, *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*, 22, 4, 2021, 97 ss. I produttori rimangono liberi di interpretare autonomamente i requisiti essenziali, tuttavia la Commissione può incaricare le organizzazioni europee di normazione di sviluppare norme armonizzate che i produttori possono scegliere di seguire e godere di una presunzione di conformità. Si noti che mentre le norme europee del CEN e CENEC consentono la certificazione, le specifiche tecniche forniscono un documento normativo nei casi in cui una norma europea non è (ancora) realizzabile, come nel caso di tecnologie ancora in evoluzione fungendo, così, da "pre-norme". La Commissione ha dunque richiesto agli enti europei di normazione di sviluppare norme armonizzate europee a supporto dell'AI Act che saranno gli strumenti essenziali per l'attuazione del regolamento e per la presunzione di conformità. Cfr. European Commission, *Draft standardisation request amending implementing decision C(2023)3215 on a standardisation request in support of Union policy on artificial intelligence*

[52] Si veda in particolare l'art. 40, par. 1, AI Act secondo cui «*High-risk AI systems or general-purpose AI models which are in conformity with harmonised standards (..)in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements (..)*». L'obiettivo esplicito della Commissione europea è quello di sviluppare standard certificabili (art. 44 AI Act), compresa la marcatura CE per i sistemi di AI ad alto rischio (art. 49 AI Act). In merito alla «sudditanza» delle regole giuridiche nei confronti di quelle tecniche nell'AI Act si veda anche M.R. Allegri, *L'ambiguo principio (anche costituzionale?) della trasparenza algoritmica fra tecnologia, diritto e linguaggio*, in *Medialaws,* 3, 2025, 9 ss. spec. 27.

[53] Sulle diverse tecniche normative comprese nel *risk based approach* e le differenze tra GDPR, DSA e AI Act si rimanda anocora a G. De Gregorio - P. Dunn, *The European Risk-Based Approaches*, cit. Criticamente, sul mix di autoregolamentazione (*soft law)* e regolamentazione *top & down (hard law*) per i modelli ad alto rischio, adottato dal legislatore dell'AI Act, si veda U. Pagallo, *Why the AI Act Won't Trigger a Brussels Effect*, *AI Approaches to the Complexity of Legal Systems*, 2023, in papers.ssrn.com.

che per un'AI Affidabile[54] «non sempre sarà possibile individuare compromessi eticamente accettabili, poiché alcuni diritti fondamentali, come la dignità umana, sono assoluti[55] e non possono essere soggetti a un esercizio di bilanciamento»,[56] pertanto, per questi casi «lo sviluppo, il dispiegamento e l'uso del sistema di AI non dovrebbero procedere in alcun modo»,[57] sempre stando alle stesse Linee Guida, al di là delle ipotesi espressamente rientranti nelle categorie vietate, è agli sviluppatori (e in conseguenza agli organismi di standardizzazione) che è rimesso il compito di valutare se l'impatto potenziale di un fallimento del loro sistema «produca risultati socialmente inaccettabili». Ed è sempre ai *providers* che è data la possibilità, tramite autovalutazione, di attestare che il sistema, pur compreso in astratto nei casi d'uso elencati nell'Allegato III,[58] non comporti nel caso concreto un rischio significativo per la salute, la sicurezza o i diritti fondamentali, ridefinendo in tal modo i contorni della relativa categoria di (alto) rischio. Come si avrà modo di evidenziare nel prosieguo, attraverso la lettura delle sezioni delle attuali bozze del *Code of Practices* (CoP),[59] destinate ai providers di Modelli a finalità generali con rischio sistemico (GPAISR),[60] è ancora prerogativa degli sviluppatori la determinazione concreta della soglia di rischio sistemico da considerarsi inaccettabile,[61] durante le fasi cruciali del ciclo di vita dei loro modelli.

Valga altresì la pena di notare che la valutazione etico-politica non attiene soltanto all'accettabilità del potenziale danno esterno prodotto dall'agente artificiale su beni immateriali, dal momento che, come gli studi nel campo della *Machine Ethics* (ME)[62] non mancano di rilevare, la crescente autonomia decisionale dei sistemi di AI richiederebbe la messa a punto di strumenti atti a garantire la "verificabilità" della riproduzione algoritmica dell'esperienza morale. Detto in altri termini, un sistema eticamente affida-

[54] *Ethics Guidelines for Trustworthy AI*, cit.

[55] Il termine "assoluto" è utilizzato nel contesto delle line guida in denso a tecnico- inteso appunto come non suscettibile di bilanciamento.

[56] *Ethics Guidelines*, cit., 13.

[57] Ivi, 20.

[58] Si tratta della sostanziale eccezione che l'art. 6, par. 3, AI Act, introduce all'elenco, altrimenti mandatorio, dei sistemi ad alto rischio.

[59] Cfr. *code-of-practice.ai*

[60] *General-Purpose AI* with *Systemic Risk* (GPAISR) or *Systemic Risks* (GPAISRs) cfr. *Third draft general purpose AI code practice published-written-independent-experts*

[61] Stando alla seconda bozza, tale soglia sarebbe dovuta fungere da parametro di riferimento nella definizione dei *Key Performance Indicators* (KPI) ossia indicatori chiave di prestazione quantitativi e qualitativi, su cui misurare l'effettiva compliance al Codice. cfr. *Second draft general purpose AI code practice published-written-independent-experts*. Stando anche al rapporto l'ISO/IEC TR 24028 *Overview of trustworthiness in artificial intelligence ISO/IEC TR, 2020 (E). (n 89) 16-17,* l'affidabilità risulterebbe migliorabile attraverso «un processo organizzativo con risultati specifici misurabili e indicatori chiave di prestazione» (KPI). Ciò nonostante, nel passaggio alla terza bozza ogni riferimento ai KPI, così come altre metriche formalizzate di valutazione, è stato rimosso, per prediligere logiche di valutazione se in forma descrittiva, non più tecnico- numerica. Sulle critiche espresse dagli stakeholders in merito a tale indebolimento del codice si veda più ampiamente *infra.*

[62] In generale sul concetto e la missione della *Machine Ethics* si veda F. Fossa, *Robot morali?* cit.

bile, dovrebbe essere grado di determinare quali siano e da dove provengano le informazioni significative per il giudizio morale che è chiamato a computare: «dovrà quindi essere dotato di apparati percettivi in grado di catturare simili informazioni e inserirle nel processo decisionale, nonché di tutte le istruzioni relative a ciò che i suoi utenti ritengono, o in linea di massima dovrebbero ritenere, moralmente e normativamente accettabile».[63] Se così è, lo stesso discusso concetto di *reliability* di una determinata tecnologia autonoma, dovrebbe essere in grado di per sé di comprendere la convergenza del funzionamento dell'agente artificiale non solo con il fine ad esso preposto, ma anche con i valori morali in gioco nelle situazioni in cui il sistema si trova ad operare,[64] considerati meritevoli di tutela.

Tuttavia il linguaggio della formalizzazione tecnica, del diritto e dell'etica sono diversi. Se la protezione dei diritti fondamentali si basa su valutazioni di proporzionalità, con l'obiettivo di garantire il massimo livello di tutela possibile rispetto ai rischi che possono minacciare i diritti individuali, la sicurezza dei prodotti, invece, parte dal presupposto che il danno possa essere misurato quantitativamente e si affida a una logica di valutazione formalizzata, basata su una soglia di rischio accettabile.[65]

Sembra improbabile allora che gli organismi europei di standardizzazione (SSOs) possano rispondere ai citati indicatori chiave di affidabilità, intesa nel senso socio-politico del termine di cui si è dato conto. Guardando al primo indicatore, la *competenza - i.e.* la percepita capacità del *trustee* di eseguire un compito delegato - se, come emerso dalla trattazione finora svolta, in virtù del descritto automatismo sono i diritti fondamentali ad essere assunti direttamente come parametri immateriali nel processo decisionale,[66] è evidente come quella che dovrebbe essere una valutazione tecnico formale del rischio relativo alla sicurezza del prodotto, trasli in un vero e

---

[63] Cfr. G. Tamburrini - F. Fossa, *Ethics of Autonomous Vehicles,* cit. 432. L'e*xplicit moral agency* o la *functional morality* (su cui cfr. *supra* nota 1) è il risultato infatti della programmazione il cui scopo è rendere il sistema in grado di svolgere ragionamenti e prendere decisioni conformi a istanze morali, si veda J.H. Moor, *The Nature, Importance, and Difficulty of Machine Ethics*, in *IEEE Intelligent Systems*, 2006, 18 ss.

[64] Cfr. G. Tamburrini - F. Fossa, *ibidem,* 428; gli A.A. sottolineano infatti «la necessità di dotare le tecnologie autonome di un intero nuovo insieme di capacità: rilevare quali valori siano in gioco in quali contesti pratici, risolvere contrasti tra i criteri strumentali della conformità a scopo e i criteri morali della conformità a valore, gerarchizzare i diversi valori morali di cui si ha contezza, e così via». *ibidem*, 429. Sulla necessità di un approccio onto-centrico che includa i principi della bioetica cioè la beneficenza, la non maleficenza, l'autonomia e la giustizia – nel concetto di "spiegabilità" principio a sua volta deve includere 'intelligibilità, comprensione, controllo dei sistemi di AI e responsabilità per i suoi usi si veda L. Floridi et al., *AI4People – An Ethical Framework For A Good AI Society*, cit.; U. Pagallo*, Dismantling Four Myths in AI & EU*, cit., spec. 257.

[65] In merito si rimanda a M. Almada - N. Petit, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?,* cit.

[66] Come detto, il rischio diviene dunque vera e propria proxy traslativa del livello di garanzia dei diritti fondamentali assumendo una sorta di funzione pan-costituzionale .Come è stato notato la circostanza nasconde un implicito paradosso nella misura in cui i valori che dovrebbero essere l'oggetto della protezione sono, contestualmente, anche il punto di riferimento che, implicitamente o esplicitamente, giustifica le decisioni sull'inclusione di determinate tipologie di sistemi di AI nella categoria ad alto rischio, cfr. I. Kusche *Possible harms of artificial intelligence,* cit.

proprio *ethical assessment* normalmente estraneo all'expertise delle SSOs. Circostanza, questa, che sembra del resto emergere dal rapporto tecnico l'ISO/IEC[67] *Overview of trustworthiness in artificial intelligence*[68] in cui, nella consapevolezza che «visioni diverse dell'AI affidabile possono derivare da diverse visioni morali del mondo o sistemi di valori»[69] si lascia alle parti interessate il compito di enucleare e sostenere i valori derivanti dalla «propria visione etica del mondo»[70] nella definizione delle misure di mitigazione in tema di privacy.

Se, da un lato, le SSOs sono prive di quella legittimazione politica necessaria a svolgere un compito normalmente proprio degli organi giurisdizionali e di deliberazione democratica,[71] è anche vero, come non si è mancato di rilevare,[72]che qualora non siano loro a compiere scelte normativamente difficili[73] o a risolvere veri e propri *ethical dilemmas,* in mancanza di idonei meccanismi compensativi, saranno verosimilmente gli sviluppatori a supplire, con le conseguenti asimmetrie di potere che a livello economico, sociale e politico, questo implica.[74] Se così fosse, oscurare la natura tutt'altro che neutrale della definizione degli standard dietro l'etichetta di affidabilità finirebbe per agevolare l'ulteriore accentramento dell'«autorità epistemica» negli AI providers che, determinando compromessi e soglie etiche soggettive senza il coinvolgimento diretto degli stakeholders esterni,[75] sono, e continueranno ad essere, i principali detentori del potere di indirizzo tecnico e politico delle traiettorie di sviluppo AI.[76]

---

[67] Rispettivamente: Organizzazione internazionale per la standardizzazione e Commissione elettrotecnica internazionale.

[68] Cfr. *Information Technology -Artificial Intelligence - Overview of Trustworthiness in Artificial Intelligence,* cit. Si tratta di uno dei rapporti tecnici pubblicati a febbraio 2024 dal SC-42, un sottocomitato istituito all'interno dell'ISO il cui scopo è creare «*an ethical AI-enabled society*», cfr. *Enabling an AI-Ready Culture,* 2021.

[69] *Ibidem,* 13.

[70] *Ibidem,* 23.

[71] M. Veale - F. Z. Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, cit.

[72] Cfr. J. Laux – S. Wachter – B. Mittelstadt, *Three pathways for standardisation and ethical disclosure by default under the European Union Artificial Intelligence Act*, in *Computer Law & Security Review*, 53, 2024.

[73] Si pensi a concetti intrinsecamente normativi ed altamente contestuali come l'equità, su cui non è pensabile un consenso globale che possa essere facilmente standardizzato, come rilevato dal citato rapporto ISO *Enabling an AI-Ready Culture*.

[74] Onde scongiurare questo rischio, gli SSOs dovrebbero creare standard che richiedano una «divulgazione etica di default» definendo requisiti minimi di documentazione e rendicontazione pubblica allo scopo di trasferire il processo decisionale etico agli stakeholder locali, a cui andrebbe rimesso il compito di stabilire requisiti normativi in modo proceduralmente coerente, limitando in questo modo la discrezionalità dei fornitori nel rispondere a «domande normative difficili» nello sviluppo dei loro prodotti e servizi di AI ,.così J. Laux – S. Wachter – B. Mittelstadt, *Three pathways for standardisation*, cit., 11.

[75] Si ricorda peraltro che in virtù della sostanziale eccezione prevista dall'art. 6, par. 3, AI Act, se a seguito di un 'autovalutazione da parte del fornitore si ritiene che un sistema non comporti un rischio significativo per la salute, la sicurezza o i diritti fondamentali non sarà ritenuto ad alto rischio e quindi escluso dalla relativa regolamentazione, anche qualora rientri nei casi d'uso elencati nell'Allegato III (art. 6, par. 2).

[76] Sui pericoli dell'accentramento autorità epistemica nelle piattaforme, nella veste di

Non può poi tacersi dell'ulteriore effetto che una tale asimmetria epistemica, anche a livello psicologico, può andare ad implicare, a partire dalla normalizzazione di potenziali *bias* e discriminazioni sistemiche insiti nei processi decisionali artificiali. Se, come suggeriscono le recenti ricerche empiriche, la discriminazione e l'errore nel giudizio algoritmico sembrano essere percepiti come più facilmente giustificabili rispetto al parallelo umano,[77] esattamente per l'assenza di intenzionalità nell'azione dell'agente artificiale,[78] una simile tendenza, potrebbe essere facilmente incrementata dalla standardizzazione e successiva "etichettatura" di pratiche *"unfair".*[79]
Passando all'analisi degli altri due indicatori, *l'integrità,* intesa come l' accettabilità dei principi e dei valori che ispirano/guidano le azioni del fiduciario e la *benevolenza,* ossia la percepita disposizione dello stesso ad adeguare eventualmente i suoi obiettivi iniziali nell'interesse del *Trustor,* non può non rilevarsi l'ovvia circostanza per cui la protezione dei diritti o il sostegno di valori pubblici non sempre trovi facile allineamento con le priorità di organizzazioni private – istituite da, e per gli stakeholders, naturalmente più vicini alla massimizzazione del profitto. Per quanto l'intero processo di armonizzazione ruoti attorno ai principi riconosciuti dall'Organizzazione Mondiale del Commercio (OMC) nel campo della normazione, ovvero coerenza, trasparenza, apertura, consenso, applicazione volontaria, indipendenza da interessi particolari ed efficienza, è evidente che tali organismi sono normalmente chiamati ad operare al di fuori dei normali circuiti di partecipazione, trasparenza, controllo democratico e responsabilità pubblica.[80] È noto, del resto, come la delega dell'autorità normativa alle SSOs abbia sollevato importanti questioni relative tanto alla legittimità degli input, in considerazione appunto dell'assenza di partecipazione della società civile e dei non esperti alla produzione di norme, quanto alla legittimità

AI-providers e la depoliticizzazione di questioni fondamentali che questo implica, si veda D. Leslie et al. *Frontier AI, Power and the Public Interest: Who Benefits, Who Decides?* in *Harvard Data Science Review*, 5, 9, 2024, 6 ss. Nello stesso senso, sul trasferimento del potere di decidere cosa costituisca un'AI affidabile dai regolatori agli AI-providers e agli organismi di standardizzazione cfr. N. Helberger, *FutureNewsCorp*, *or how the AI Act changed the future of news,* in *Computer Law* & *Security Review*, 52, 2024, 9 ss.

[77] Y. E. Bigman - D. Wilson - M. N. Arnestad - A. Waytz - K. Gray*, Algorithmic discrimination causes less moral outrage than human discrimination,* in *Journal of Experimental Psychology: General,* 152, 1, 2023, 4 ss.

[78] D. Acemoglu, *Harms of AI*, in J.B. Bullock, et al. (eds), *The Oxford Handbook of AI Governance,* Oxford, 2022, spec. 44 e 47.

[79] A. Bonezzi - M. Ostinelli, *Can algorithms legitimize discrimination*? in *Journal of Experimental Psychology: Applied*, 27, 2021, 447 ss. G. Yalcin Williams - S. Lim*, Psychology of AI: How AI impacts the way people feel, think, and behave, in Current Opinion* in *Psychology*, 58, 2024, 1018 ss. In egual modo può dirsi, in riferimento all' *Automation Bias* (AB) ossia la tendenza psicologica a fare eccessivo affidamento sull'automazione nei processi decisionali su cui K. Goddard – A. Roudsari – J. C. Wyatt, *Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators*, in *Journal of the American Medical Informatics Association*, 19, 1, 2012, 121 ss.; J. Laux - H. Ruschemeier, *Automation Bias in the AI Act: On the Legal Implications of Attempting to De-Bias Human Oversight of AI*, in *arXiv,* 2025, 12.

[80] Sulle questioni relative all'assenza di legittimazione democratica, cfr M. Ebers, *Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act,* in *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, 2021, in *ssrn.com.*

degli output, data la carenza di trasparenza e *accountability* dei processi decisionali istituzionali di attuazione di tali norme.[81] Difficilmente, dunque, l'operato delle SSOs potrà fornire la base per la costruzione di un consenso democratico e partecipativo allo sviluppo e implementazione dei sistemi di AI, almeno non senza lo sviluppo di nuovi quadri istituzionali e di pratiche procedurali necessarie ad abilitare la deliberazione collettiva sui modi e le condizioni in cui i sistemi computazionali entrino nell'ecosistema e modellino la vita sociale.[82]

In conclusione, la descritta sovrapposizione "a cascata" tra standardizzazione, accettabilità politica del rischio e *trustworthiness,* sembra svuotare di significato quella che dovrebbe essere la funzione di quest'ultima, ossia assurgere a condizione di legittimazione (democratica) *ex ante* dell'immissione e lo sviluppo di sistemi di AI potenzialmente lesivi dei diritti fondamentali e con cui l'individuo, volontariamente o meno, è destinato ad interagire.

Se è vero, infatti, che l'asimmetria epistemica tra providers ed esperti da un lato, e destinatari delle tecnologie (HRs) dall'altro, fa sì che questi ultimi non possano essere chiamati a valutare autonomamente le prove a garanzia della *trustworthiness* di un sistema, esattamente in ragione di ciò, devono poter riporre la loro fiducia nelle organizzazioni e nelle istituzioni che, in qualità di *Proxy Trusties,* sono chiamate a garantirla.[83] Detto in altri termini, il giudizio esperto deve poter essere *trustworthy* affinchè l'AI lo sia a sua volta.[84]

4. Il caso dei GPAI e la protezione dei dati: la *Sociological Trustworthiness* come antidoto all'irrimediabilità dell'"intrusione digitale"

La descritta necessità di promuovere la partecipazione democratica dei destinatari delle tecnologie (HRs) nella valutazione di ammissibilità *ex ante* di un determinato sistema, restituendo loro quell'autonomia decisionale alla base del discusso concetto *trustworthiness,* è del resto resa di palmare evidenza dalle sfide (apparentemente) inedite poste dalla rapidissima asce-

[81] Si veda *ex multiis* L. Senden, *Towards a More Holistic Legitimacy Approach to Technical Standardisation in the EU*, in M. Eliantonio - C. Cauffman, (a cura di) *The Legitimacy of Standardisation as a Regulatory Technique*, *A Cross-disciplinary and Multi-level Analysis,* Cheltenham, 2020; C. Cauffman - M. Gérardy, *Competition Law as a Tool to Ensure the Legitimacy of Standard-Setting by European Standardisation Organisations?* Ibidem. H. Schepel, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets*, Oxford, 2005.

[82] In merito sia consentito rimandare anche I. de Vivo, *La ricerca di un modello per regolare le nuove tecnologie,* in M.E. Bucalo, M. Caporale, A. Sterpa (a cura di) *Diritto Pubblico di Internet,* Napoli 2024, 79 ss., 105 ss.

[83] Esattamente in ragione della difficoltà per l'individuo di sviluppare una conoscenza tecnica tale per poter parlare di consenso informato, un consenso basato sull'*Institutional Trustworthiness.* svolge un ruolo chiave, così C. Wilson - M. van der Velden, *Sustainable AI: An integrated model to guide public sector decision-making', Technology in Society,* 68, 2022.

[84] Cfr. O. O'Neill, *A Point of View: Which comes first - trust or trustworthiness?,* cit., traduzione a cura dell'autrice.

sa, storicamente senza precedenti,[85] dei cosiddetti sistemi di «intelligenza generativa (GenAI)[86] a finalità generali» (GPAI).
L'inserimento "last minute" della categoria dei GPAI[87] nel sistema di classificazione dell'allora non prevista «categoria del rischio sistemico» è infatti emblema della necessità di superare l'asimmetria epistemica e decisionale tra sviluppatori da un lato, regolatori e utenti dall'altro, nella definizione delle condizioni di ammissibilità di una tecnologia che - discorsivamente legittimata da un contestuale e strategico «*public interest-washing*»[88] da parte delle big-tech - continua a muoversi sovrascrivendo le sue regole dall'interno dei laboratori di ricerca.[89] Il coinvolgimento circa l'*an* ed il *quomodo*

[85] Si veda N. Helberger – N. Diakopoulos, *ChatGPT and the AI Act* in *Internet Policy Review*, 12, 1, 2023.

[86] L'Intelligenza Artificiale Generativa (GenAI) è una branca dell'intelligenza artificiale la cui caratteristica è la capacità di creazione di contenuti nuovi e originali, come testi, immagini, video, musica o codice, utilizzando modelli di *deep learning* addestrati su vasti set di dati.

[87] Comunemente noti anche come modelli fondativi (*Foundation models*- FM) i GPAI sono progettati per svolgere una vasta gamma di compiti non specificamente limitati ad un singolo dominio o applicazione. Possono essere dunque applicati in molteplici contesti e integrati in vari sistemi o applicazioni a valle -fungendo da fondamento per lo sviluppo di applicativi AI per scopi specifici (cfr. R. Bommasani - P. Liang, P. *Reflections on Foundation Models. Human-Centered ArtificialIntelligence*, 2021, in hai.stanford.edu. La sfida regolatoria sta appunto nell'impossibilità di determinarne aprioristicamente l'utilizzo e dunque il rischio. L'AI-Act, a tal proposito, dopo aver fornito la definizione di GPAI all' art. 3 n. 63, distingue la sottocategoria di «GPAI con rischio sistemico» (art.3 n.65) per indicare e sottoporre a specifica regolazione quei modelli che a causa delle loro capacità e dell'ampio impiego previsto, potrebbero avere «un impatto significativo sul mercato dell'Unione a causa della loro diffusione o a causa di effetti negativi reali o ragionevolmente prevedibili sulla salute pubblica, sicurezza, diritti fondamentali o sulla società nel suo complesso»; in merito si veda *infra*. La previsione è stata inserita a seguito degli emendamenti parlamentari proposti nelle more del trilogo che ha condotto all'approvazione del testo definitivo dell'AI-Act, in concomitanza al lancio di Chat-GPT. In argomento si veda I. Kusche, *Possible harms of artificial intelligence,* cit.; N. Helberger – N. Diakopoulos, *ChatGPT and the AI Act*, cit. Per una visione critica dell'inserimento della categoria dei GPAI in parziale sovrapposizione ai modelli GenAI si veda U. Pagallo, *Why the AI Act Won't Trigger a Brussels Effect,* cit. In particolare, l'integrazione di pezzi di legislazione verticale, attraverso la serie di misure normative proposte dagli emendamenti parlamentari per gli usi dei GPAI, avrebbe alterato l'approccio orizzontale della Commissione, con l'effetto di sommare gli svantaggi di entrambe le tecniche di governance; cfr. *ibidem,* 7.

[88] Anche nel settore privato, infatti, le aziende hanno riconosciuto il ruolo chiave della fiducia nei loro sistemi di AI e adottato iniziative per rafforzarla, come la sottoscrizione di impegni etici, lo sviluppo di principi guida e l'adesione a reti per un'AI responsabile, come gli *Ethics-based Auditing*, cfr. J. Mökander – L. Floridi, *Ethics-Based Auditing to Develop Trustworthy AI in Minds and Machines,* 31, 2, 2021, 323 ss. L' effettività di tali misure di *self-regulation*, tuttavia, come già rilevato, non va esente da critiche, si veda *ex multiis* B. Mittelstadt, *Principles alone cannot guarantee ethical AI,* in *Nature Machine Intelligence,* 1, 11, 2019, 501 ss.; Leslie et al., *Frontier AI, Power and the Public Interest,* cit., 7, che appunto parlano di «*public interest washing*» riflettendo criticamente su come l'inizio della «*GenAI age of competition*» sia stata legittimata da quella stessa retorica di apertura e democratizzazione degli albori di Internet, che fatta propria dalle big tech, ha permesso loro il consolidamento del potere finanziario e tecno-scientifico necessario a monopolizzare le infrastrutture critiche di dati, *condicio sine qua non* per sviluppo delle tecnologie GenAI di «frontiera».

[89] Sul rischio di obsolescenza normativa, incrementato dalla moltiplicazione delle fattispecie in relazione alla GenAI si veda ancora U. Pagallo, *Why the AI Act Won't Trigger a Brussels Effect,* cit.

dell'implementazione e dell'immissione nell'ecosistema di nuovi agenti in cui l'alta velocità, l'impatto asimmetrico ed il *cascade effect* rappresentano le caratteristiche distintive,[90] appare infatti l'antidoto per pensare a strumenti di regolazione non solo reattivi, ma dinamici ed adattivi, in grado di colmare quel ritardo ontologico di una regolazione che sembra non potersi dare se non ad "intrusione digitale" - già e irrimediabilmente - data.
Ciò è particolarmente vero se si guarda all' incompatibilità strutturale tra la prospettiva di tutela apprestata dal GDPR, con cui il regolamento sull'Intelligenza artificiale necessita di armonizzazione,[91] e le condizioni costitutive di sviluppo e addestramento dei *Large Language Models* (LLMs)[92] che il caso pilota di Chat-GPT[93] sembra aver reso di palmare evidenza.
In particolare la dubbia legittimità del *modus operandi* di tali sistemi che in Italia ha condotto alla temporanea sospensione del trattamento dei dati personali da parte di OpenAI prima, e della cinese Deep-Seek poi, a seguito di due provvedimenti di simile tenore emessi dall' Autorità Garante della Privacy (GPDP),[94] sembra essere conseguenza delle incertezze in-

[90] I dubbi di legittimità dell'immissione in massa dei sistemi GenAI hanno riguardato rischi per i diritti fondamentali coinvolgendo i più svariati settori, dalla proprietà intellettuale, alla manipolazione informativa, dalla *cybersecurity* ai costi ambientali. Per i potenziali impatti negativi e gli effetti trasformativi sulla società nel suo complesso si veda il report del *Center for Research on Foundation Models* (CRFM) dello Stanford Institute for Human-Centered Artificial Intelligence (HAI) in R. Bommasani, et al. *On the Opportunities and Risks of Foundation Models,* in *ArXiv.org.,* 2021.

[91] Sui problemi relativi alla "tenuta" del GDPR in particolare in relazione all'AI generativa si vedano M. Eberns - K. Sein, *Data-driven Technologies: Challenges for Privacy and EU Data Protection Law* in id. (a cura di), *Privacy, Data Protection and Data-driven Technologies,* Londra, 2024, 3 ss. In particolare sulle questioni relative al coordinamento con l'AI-Act. cfr. A. Lombardi, *Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra GDPR e AI Act,* in *EJPLT,* 2, 2023, 240 ss, spec. 244.

[92] Gli LLMs sono una sottoclasse di GPAI, con un focus specifico sul linguaggio naturale. Tramite l'utilizzo di tecniche come il *deep learning* e l'apprendimento non supervisionato sono in grado di acquisire competenze linguistiche complesse. La versatilità e capacità di simulazione è tale da rendere l'applicazione possibile ad una gamma di settori pressoché indefinita, trasformando il modo costitutivo il paradigma dell'interazione machine-human a partire dalla gestione cognitiva e informativa.

[93] ChatGPT (*Generative Pre-trained Transformer)* è un modello di AI c.d. *transformer,* basato cioè su meccanismi di ottimizzazione dell'attenzione, che sostituisce le reti neurali ricorrenti o convoluzionali tradizionalmente impiegate negli encoder e decoder dei modelli di traduzione automatica e di elaborazione del linguaggio naturale. Cfr. A. Vaswani et al., A*ttention Is All You Need*, in *arxiv.org*, 2017.

[94] Con il provvedimento emesso in via d'urgenza dall'Autorità Garante della Privacy, di poco successivo all'immissione del sistema sul mercato europeo da parte di OpenAI, è stata infatti disposta la temporanea sospensione del trattamento dei dati personali degli interessati stabiliti nel territorio italiano Cfr. Prov. 30 marzo 2023, n. 9870832. Il Garante ha poi concluso l'istruttoria il 20 dicembre 2024, imponendo a OpenAI una sanzione di 15 milioni di euro e l'obbligo di realizzare una campagna informativa di sei mesi. Il secondo e più recente provvedimento di limitazione del trattamento è stato emesso dal Garante nei confronti della compagnia cinese *DeepSeek*, cfr. prov. 30 gennaio, 2025, n. 10097450, in *garanteprivacy.it*. caso che ha indotto azioni simili sia a livello europeo (si veda l'indagine aperta dalla *Data Protection Authority* (AP) olandese sui trasferimenti di dati di DeepSeek verso la Cina), sia a livello internazionale, in particolare negli USA, dove a seguito di «prove profondamente inquietanti» della raccolta di dati sensibili di cittadini statunitensi e la minaccia alla sicurezza nazionale che DeepSeek rappresenta

terpretative dovute tanto all'oggettiva difficoltà di delineare l'ambito di applicabilità del GDPR, quanto del "ritardo costitutivo" degli strumenti di tutela di privacy e dati personali ivi previsti.

In relazione al primo aspetto, preso atto che il regolamento non esclude dal suo ambito di applicazione i dati personali resi pubblicamente disponibili on line[95] e che un consenso da parte degli interessati all'operazione di "raschiamento" (potenzialmente inclusivo di dati anche sensibili) che l'addestramento presuppone, non era e non è ragionevolmente ipotizzabile,[96] non era chiaro quale potesse essere la base giuridica idonea a legittimare il trattamento.[97] Ora lo scopo perseguito dal provider allo sviluppo dei sistemi, affinché possa integrare l'interesse legittimo,[98] non soltanto presupporrebbe un test di bilanciamento caso per caso, ma per potersi dire tale, richiederebbe la conformità ai principi fondamentali stabiliti dall'art. 5 GDPR, tra cui la conoscibilità e la sufficiente specificità delle circostanze e finalità trattamento,[99] condizioni, queste, ontologicamente incompatibili con l'addestramento di modelli di GenAI per finalità generali. Quanto ai requisiti di trasparenza e affidamento, è evidente come non fosse ragionevolmente prevedibile per nessun utente la modalità attraverso cui i dati originariamente immessi online sarebbero stati utilizzati, trattandosi di modelli non ancora esistenti. Non può poi tacersi l'ulteriore circostanza per cui, come spesso avviene con i grandi database, la possibilità di dedurre dati sensibili nella fase di *data scraping*, farebbe potenzialmente rientrare il trattamento, nel raggio di applicazione dell'articolo 9 del GDPR. Ciò in

per gli Stati Uniti, diverse agenzie federali, inclusi la NASA e la Marina degli Stati Uniti, hanno proceduto a bloccare l'app, sulla base del bipartisan *No DeepSeek on Government Devices Act*. Un simile divieto è stato introdotto in Australia, mentre l'Agenzia Digitale del Giappone ha reso obbligatoria l'approvazione da parte del *Cabinet Cyber Security Center* per qualsiasi uso governativo del servizio, unendosi al divieto esistente di Taiwan sull'uso della piattaforma da parte delle agenzie governative.

95 Art. 29 *Working Party, Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation*, 679, 2016.

96 Si vedano F. Z. Borgesius – S. Kruikemeier – S. Boerman – N. Helberger, *Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation,* in *European Data Protection Law Review* 3, 2018, 353 ss.

97 In merito all'estensione da accordare al requisito dell'interesse legittimo è utile ricordare la sentenza della CGUE che chiamata a pronunciarsi su un caso di *behavioral advertising*, all'attenzione dell'autorità antitrust tedesca (CGUE, 4 luglio 2023, C-252/21, *Meta Platforms Inc. and Ors v Bundeskartellamt*) afferma che il trattamento di dati *ulteriori* per finalità come appunto la profilazione comportamentale, non possa fondarsi sulla mera esecuzione del contratto tra utente e piattaforma, né sul *legittimo interesse* della piattaforma, né sul consenso degli utenti, che non sarebbe libero in quanto condizionato dall'erogazione del servizio (Corsivi dell'A.). La raccolta, dunque, per dirsi legittima, dovrà essere strettamente necessaria al servizio richiesto e proporzionale agli scopi perseguiti. In merito si veda anche il Comitato Europeo Per La Protezione Dei Dati (EDPB) che ribadisce l'interpretazione restrittiva delle singole condizioni di liceità del trattamento, cfr. EDPB *Urgent Binding Decision*, n. 01/2023, in *edpb.europa.eu*

98 Cfr. art. 6, par., 1., lett. *f),* GDPR.

99 Cfr. art. 5, par., 1, GDPR che stabilisce i principi fondamentali per il trattamento dei dati personali tra cui liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.

particolare alla luce dell'ampia interpretazione del concetto di dato sensibile resa dalla Sentenza della CGUE[100] nel recente caso che ha coinvolto Meta. Stando a quanto affermato dalla Corte, per aversi dato sensibile non è, infatti, necessario che i dati personali si riferiscano direttamente a categorie protette, come l'origine etnica o razziale, la religione, l'età o la salute, ma è sufficiente che «il trattamento dei dati consenta di rivelare informazioni che rientrano in una di queste categorie».[101] Ciò che risulta decisivo è quindi la possibilità di dedurre tratti sensibili sulla base dei dati disponibili*,* come accade sempre più spesso tramite le tecniche di apprendimento automatico[102] e questo indipendentemente da ciò che l'operatore intenda fare di tale deduzione. Se così è, non potendo trovare applicazione in questo caso l'esenzione di cui all'articolo 9, par. 2, lett. *j),* limitata alla costruzione di modelli che siano strumentali alla ricerca,[103] poco o nessun margine di manovra rimarrebbe per il trattamento di queste categorie di dati al di fuori del consenso informato ed esplicito dell'interessato, salvo prevedere una nuova eccezione, questa volta specifica, per l'addestramento dei sistemi GenAI.[104]

Il *data scraping* peraltro non rappresenta l'unico momento in cui i dati personali, potenzialmente anche sensibili, entrano nel ciclo di vita di un LLM. La successiva fase è quella dell'interazione *human -machine* tramite i c.d. *prompt*, dove l'utente con le sue richieste può, volontariamente o meno, rivelare dati personali anche sensibili, propri o di terzi. Sebbene in questa fase si possa invocare il consenso dato al momento della registrazione, come base giuridica per la liceità del trattamento dei dati, tuttavia l'inconoscibilità delle finalità e la difficile compatibilità con il principio di minimizzazione[105] che, come noto, richiede che il trattamento non vada oltre quanto strettamente necessario per il conseguimento delle finalità legittime specificate, rende difficile ipotizzare l'espressione di un valido consenso da parte dell'utente e che, in ogni caso, non potrebbe coprire la cessione di dati personali di terzi eventualmente coinvolti. Emblematico a questo riguardo è l'appello alla consapevolezza e alla responsabilità circa le conse-

---

100 CGUE, C-252/21, *Meta vs. Bundeskartellamt,* ECLI:EU:C:2023:537.

101 CGUE, C-252/21 par. 73.

102 Cfr. *ex multiis* R. Chaturvedi – S. Chaturvedi, *It's All in the Name: A Character-Based Approach to Infer Religion,* in *Political Analysis*, 32, 1, 2024, 34 ss; M. Veale – R. Binns – L. Edwards, *Algorithms that remember: Model inversion attacks and data protection law,* in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376, 2018.

103 Esenzione che dunque non potrebbe essere utilizzata per l'addestramento di modelli a scopi commerciali, cfr. Considerando 159 e 162, GDPR.

104 In questo senso, C. Novelli – F. Casolari – P. Hacker – G. Spedicato – L. Floridi, *Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity* in *Computer Law & Security Revien,* 55*,* 2024. Una simile eccezione del resto farebbe eco a quanto già previsto dall'art. 10, par. 5 dell'AI-Act che si occupa specificamente delle condizioni sotto le quali i fornitori di sistemi di AI ad alto rischio possono eccezionalmente trattare categorie particolari di dati personali. Il trattamento è permesso nella misura in cui sia strettamente necessario per scopi di rilevamento e correzione dei *bias*, ed è soggetto alle garanzie di cui al GDPR, al regolamento (UE) 2018 n. 1725, nonché alla direttiva (UE) 2016 n. 680.

105 Art. 5, par. 1, l. c) GDPR. In merito si vedano R. Bommasani *et al., On the Opportunities and Risks of Foundation Models,* cit.

guenze della condivisione dei dati personali rivolto dall' autorità olandese direttamente agli utenti, in relazione al più recente modello DeepSeek: «quando carichi un documento come un CV nel chatbot di DeepSeek, i tuoi dati personali possono essere registrati su un server in Cina. Lo stesso vale per tutte le domande che si avviano nel chatbot. Sii consapevole di questo. Pensa solo a questo. Il sistema vive sulle informazioni che hai inserito. Renditi conto che puoi persino caricare - intenzionalmente o involontariamente - informazioni su altre persone in quel chatbot, senza che quell'altra persona lo sappia, o possa esprimere il suo consenso. Un tale trasferimento illegale ti rende responsabile».[106] Se la responsabilizzazione individuale su cui l'Autorità fa leva è da sola insufficiente alla tutela dei diritti in gioco, tuttavia l'appello è particolarmente significativo nella misura in cui rende evidente l'impellente esigenza di un'alfabetizzazione all'AI di natura critica che, come si argomenterà, assurge a pre-condizione di successo di qualsiasi tentativo di effettivo coinvolgimento democratico dell' *human recipient* sulle scelte cruciali relative ai sistemi con cui, volontariamente o meno, è destinato ad entrare in relazione.

Venendo al secondo profilo, non era e non è tuttora chiaro quali siano e come possano essere tecnicamente implementati gli strumenti di tutela previsti dal GDPR, come opposizione, revoca del consenso, rettifica e cancellazione. Si tratta infatti di rimedi *ex post* e che intervengono a raccolta già avvenuta, come vedremo, difficilmente applicabile ai dati di output, e il cui esercizio in concreto si complica ulteriormente se applicato ai sistemi generativi. Il risultato di un eventuale *opt-out,*[107]a livello tecnico, si è risolto, almeno inizialmente infatti, nell'apposizione di un filtro auto-censorio per cui il sistema si astiene dal riferire determinate informazioni che tuttavia, una volta entrate a far parte del bagaglio "cognitivo" del modello, continuano ad esistere- alimentando e plasmando il suo *modus cogitandi*. Se questo è vero, è vero anche che la cancellazione di determinate informazioni da un set di addestramento non può che essere una soluzione superficiale dal momento che il bagaglio "esperienziale", le connessioni e relazioni tra concetti, permangono ed evolvono a prescindere dall'"amnesia" relativa al singolo dato o informazione. A livello tecnico questo significa che i dati rimossi continuano a plasmare i parametri del modello,[108] potendo trapelare negli output, inavvertitamente, o a seguito di operazioni di *reverse engineering* capaci di sfidare anche più sofisticate operazioni di *Machine Unlearning* (MU).[109]Anche attraverso gli algoritmi di MU non sembra infatti

---

[106] Cfr. Autoriteit Persoonsgegevens, *AP: pas op met gebruik chatbot DeepSeek*, 3 febbraio 2025, traduzione a cura dell'autrice. In maniera simile per affrontare le sfide relative alla sicurezza e all'etica, l'Organizzazione Mondiale della Proprietà Intellettuale (WIPO) raccomanda di utilizzare strumenti su cloud privati e di formare i dipendenti affinché evitino di includere informazioni riservate nei prompt, mentre l'accesso agli strumenti AI dovrebbe essere limitato e controllato qualora i *prompt* contengano materiale coperto da copyright, segreti commerciali o dati personali.

[107] Il primo caso di *opt-out* è stato quello di un componente del Garante Privacy, Guido Scorza, che in qualità di privato cittadino, ha esercitato il diritto di opposizione al trattamento dei propri dati *ex* art. 21.

[108] Si veda E. De Cristofaro, *An Overview of Privacy in Machine Learning,* in *arXiv.org,* 2020.

[109] I cd. algoritmi di *unlearning* si concentrano sulla cancellazione dell'influenza specifica di alcuni punti di dati sul modello. L'output finale *l'Unlearned Model* è il modello ottenuto

che il sistema "disimpari" definitivamente e l'*Unlearned Model* oltre a poter inficiare l'accuratezza degli output, resta, al momento vulnerabile ad attacchi di *adversarial machine Learning*.[110]

5. Le origini di un ritardo costitutivo: l'approccio dualistico del GDPR e la possibile traiettoria evolutiva: un modello decisionale per il *Trust-Based Consent*

Come anticipato in premessa, i dubbi e le incertezze interpretative sollevate dall'immissione degli LLMs nel mercato europeo non fanno altro che rendere evidenti quelli che sono i limiti intrinseci dell'approccio duale alla tutela dei dati che informa l'architettura del GDPR di fronte al livello di saturazione raggiunto dalla computazione. Non solo il *discrimen* tra ciò che è personale e ciò che non lo è sembra destinato inevitabilmente a venir meno,[111] ma è la scissione tra dato quale «bene oggetto» - suscettibile di rivendicazione di diritti- e soggetto cui inerisce, presupposto ontologico della tutela civilistica, a dover esser messa in discussione. Se questa scissione duale tra dati "bene prodotto" e "soggetto produttore" è ciò che ha reso possibile lo sviluppo dell'economia *data-driven,* è in questo stesso sistema che tale dicotomia tende a sfumare, fino a scomparire del tutto, nell'equivalenza tra flusso identitario e flusso di dati.[112]
Ciò che sfugge alle maglie di una tutela operante sulla base del "nesso di prossimità" che legando la persona ai suoi segnerebbe per converso il *discrimen* tra un "interno" ed un "esterno" - sono esattamente infatti i «dati profilati»[113]o tecnicamente gli *inferred data*[114] dati in cui, seppur tale nesso

rimuovendo dall' addestramento le informazioni che il modello deve "dimenticare" (c.d. *Forget Set*) così che non influenzino più il suo comportamento. Al momento, però, questo metodo richiede molto tempo e potrebbe avere un impatto negativo in termini *performance* e *accuracy*.

[110] Si vedano C. Novelli – F. Casolari – P. Hacker – G. Spedicato – L. Floridi, *Machine Unlearning: Its Nature, Scope, and Importance for a "Delete Culture"*, in *Philosophy & Technology,* 36, 2, 2023, 1 ss. Sull'esigenza di rimedi più solidi si vedano E. Hine – C. Novelli – M. Taddeo – L. Floridi, *Supporting Trustworthy AI Through Machine Unlearning,* in *Science and Engineering Ethics*, 30, 5, 2024.

[111] Sull'insufficienza di tale paradigma dicotomico nell'ambito del machine learning, che si fonda prevalentemente su dati non personali e su meccanismi inferenziali ed il correlato approccio individuale alla tutela basato sul principio del consenso, si veda G. M. Ruotolo*, Intelligenza Artificiale e trattamento dei dati tra diritto internazionale e ordinamenti interni*, in *AI Law - International Review of Artificial Intelligence Law,* 2025.

[112] J. Van Den Hoven, *Information Technology, Privacy, and the Protection of Personal Data*, in J. Van Den Hoven - J. Weckert (a cura di*), Information Technology and Moral Philosophy*, in *Philosophy and Public Policy*, Cambridge, 2008, 301 ss.; L. Floridi, *The Informational Nature of Personal Identity*, in *Minds and Machines,* 21, 4, 2011, 549 ss.

[113] A. Nicita, *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,* 2019*,* 1165 ss.

[114] La categoria si basa sulla tripartizione del *World Economic Forum* (cfr. World Economic Forum, *Personal data: The emergence of a new asset class*, 2011, 7) ripresa dalle indicazioni del WP-29, *Guidelines on the right to data portability* (rev. 01), 2017, 9-10. Si veda in merito A.

sembrerebbe reciso,-nella misura in cui viene meno il requisito dell'identificabilità della traccia informativa- restano in grado di incidere direttamente ed indirettamente sulla sfera personale, sociale e giuridica dell'interessato (a livello individuale o sistemico), influenzando gli output dei sistemi automatizzati con cui egli entra in relazione. È il tipico caso della profilazione di gruppo e i possibili *bias* e discriminazioni categoriali che questa implica.[115]Salvo dunque voler riconoscere a questa particolare categoria di dati statuto giuridico autonomo e quindi la titolarità di diritti alla privacy a gruppi *ad hoc,*[116] il trattamento automatizzato dei dati con cui gli individui vengono "stoccati" in classi (in base al loro comportamento, alle loro preferenze e ad altre caratteristiche) ha creato e crea una lacuna nella regolazione[117] che l'approccio personalistico non sembra in grado di colmare.[118] Se da un lato è vero, come è stato rilevato, che nessuna previsione, anche implicita del sistema, garantisce un diritto (di esclusiva) al trattamento di questa categoria di dati, risultanti dall'elaborazione di dati ceduti volontariamente dall'utente *(volunteer data)* e dai dati osservati dal comportamento online *(observed data)*, automaticamente esercitabile dalle imprese catalizzatrici della loro raccolta,[119] per cui nulla impedirebbe, in astratto, l'esercizio

Pentland - L. Shirer - T. Hardon - I. W. Berger, *Trusted Data: A New Framework for Identity and Data Sharing*, Cambridge, 2019.

[115] I dati statistici su cui si basa la profilazione comportamentale possono essere utilizzati in modo generico, si pensi al c.d. miglioramento dei servizi come può essere la riconfigurazione delle interfacce di piattaforma che per quanto interesse legittimo del fornitore può avere come effetto, intenzionale o meno, l'incremento della dipendenza con danno per la salute mentale degli utenti, si veda P. Palka, *Harmed While Anonymous*, in *Technology and Regulation*, 2023, 22 ss.

[116] Il concetto di «*Categorial Privacy*» ormai piuttosto risalente, si basa in gran parte sul concetto di privacy individuale, estendendola alle informazioni non più riferibili a persone identificabili, ma il cui trattamento inferenziale ha conseguenze negative per i membri di una determinata categoria, cfr. A. Vedder, *Medical Data, New Information Technologies And The Need For Normative Principles Other Than Privacy Rules,* in M. Freeman, A. Lewis (a cura di), *Law And Medicine*, Oxford, 2000, 441 ss. Si veda anche L. Floridi, *Group Privacy: A Defence And An Interpretation*, in L. Taylor – L. Floridi – B. van der Sloot (a cura di), *Group Privacy: New Challenges of Data Technologies*, Cham, 2017. R. Mühlhoff, *Predictive privacy: Collective data protection in the context of artificial intelligence and big data,* in *Big data and society,* 2023, 1 ss.

[117] M. Ebers, *Regulating AI and robotics: Ethical and legal challenges,* in M. Ebers, S. Navas (a cura di), *Algorithms and Law*, Cambridge, 2020, 37 ss.

[118] In questo senso si veda G.M. Ruotolo, *Intelligenza Artificiale e trattamento dei dati*, cit. secondo cui si potrebbe pensare di applicare le norme sul trattamento dei dati non già, e non solo, ai dati forniti dall'utente e a lui immediatamente riferibili, ma a quelli che i sistemi di AI gli attribuiscono, sulla base del meccanismo di *co-patterning* (appunto *inferred data)*, in forma collettiva sulla base dei modelli previsti dal diritto internazionale e, in particolare, nella forma dei reclami di cui al Protocollo addizionale alla Carta Sociale Europea del 1995.

[119] Cfr. F. Mezzanotte, *I poteri privati nell'odierno diritto dello sviluppo economico*, in *Pol. dir.,* 2018, 507 ss. spec. 523. L'A. rileva come dietro l'apparente logica redistributiva e gli obblighi di disclosure imposti ai *data holders* si celi l'implicita accettazione di una premessa priva *de iure condito* di alcun fondamento giuridico ossia la sussistenza di un diritto di esclusiva sui dati inferiti o profilati, automaticamente esercitabile dalle imprese catalizzatrici della loro raccolta. In merito si veda anche S. Eskens, *A right to reset your user profile and more GDPR rights for personalized news consumers*, in *International Data Privacy Law,* 9, 3, 2019, 153 ss.

dei diritti cancellazione (art. 17) e rettifica (art.16),[120] il loro esercizio in concreto troverebbe ridotto margine di manovra laddove, come è questo il caso, il trattamento determini un mutamento (irreversibile) di «materia prima». Difficilmente la cancellazione dei dati personali raccolti dal titolare del trattamento, potrà incidere rispetto al "prodotto" di tale trattamento, ossia sull'interpretazione e le valutazioni che ne derivano e il conseguente surplus informativo. Del resto, il diritto di revocare il consenso di per sé «non pregiudica la liceità del trattamento basata sul consenso prima della revoca»,[121] ma si limita a sottrarre i dati personali a futuri sfruttamenti economici, non potendo incidere su quanto è stato fatto, sui trattamenti che sono stati già effettuati e sui risultati che questi hanno prodotto, rispetto ai quali l'interessato non ha più alcun potere di controllo. Dunque, la relazione di natura prettamente personalistica, che per scelta del sistema insiste tra consumatore e dati personali, è destinata a interrompersi nel momento in cui chi esercita «questa attività d'impresa computazionale»[122]ottiene il valido consenso al trattamento o operi su un'altra base giuridica. Per quanto riguarda il diritto di rettifica,[123] resterebbe aperta la questione se "l'inaccuratezza" dei dati che da origine a siffatto diritto debba essere oggettiva (dati inesatti), o possa estendersi alla sindacabilità della valutazione soggettiva[124] a prescindere dalla pretesa oggettività dei dati su cui si basa e, quindi, estendersi in concreto anche agli *inferred data* che rappresenta-

[120] Come del resto suggerito dal WP-29, i diritti cancellazione (art 17) e rettifica (art.16), in principio dovrebbero potersi applicare per contestare l'accuratezza o cancellare qualsiasi categoria di dati, dunque sia i dati personali di input (i dati personali utilizzati per creare il profilo) sia i dati di output (il profilo stesso o "punteggio" assegnato alla persona), cfr. WP Art. 29, *Guidelines on Automated Decision-Making and Profiling,* 2018, spec. 18, traduzione a cura dell'autrice.
Cfr art. 7, GDPR.

[121] Cfr. art. 7, GDPR.

[122] Cfr, A. Ottolia, *Big Data E Innovazione Computazionale*, Torino, 2017; F. Bravo, *Il "Diritto" A Trattare Dati Personali nello svolgimento dell'attività economica*, Padova, 2018; C. Irti, *Consenso negoziato e circolazione dei dati personali,* Torino, 2021, spec. 47.

[123] Ancora, secondo quanto espresso dal WP29 in riferimento all'art. 16 «i dati personali utilizzati per creare il profilo dovrebbero includere sia i dati volontari che i dati osservati, poiché il GDPR stabilisce che ogni persona ha il diritto di rettificare «i dati personali che la riguardano». Cfr. WP Art. 29, *Guidelines on Automated Decision-Making,* cit., traduzione a cura dell'autrice.

[124] Precedentemente,il WP29 aveva ritenuto che il termine"accurato" dovesse riferirisi ad un dato di fatto, per cui solo i dati oggettivamente inesatti sarebbero suscettibili di rettifica e cancellazione dai risultati di ricerca. Cfr. WP29. *Orientamenti sull'attuazione della sentenza della Corte di giustizia dell'Unione europea relativa a "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, 2014, spec. 15. Tuttavia nel caso di specie una lettura ristretta del termine era giustificata dal contesto – ie la cancellazione e la deindicizzazione della notizia dal motore di ricerca. Lo scopo di una simile lettura era minimizzare le implicazioni della rimozione di informazioni per altri diritti fondamentali, come il diritto alla libertà di espressione e all'informazione, esigenza che non dovrebbe darsi in caso di memorizzazione dei dati in back-end necessari alla profilazione. Per una discussione critica del principio di accuratezza, si veda J. Chen, *The dangers of accuracy: Exploring the other side of the data quality principle*, in *European Data Protection Law Review*, 4,1, 2018, 36 ss. T. Gillespie, *The Relevance of Algorithms*, in T. Gillespie – P. J. Boczkowski – K. A. Foot (a cura di), *Media Technologies: Essays on Communication, Materiality, and Society*, Cambridge, 2014, 167 ss.

no appunto una valutazione non suscettibile di verificazione in termini di verità o falsità. Anche il fondamentale divieto di profilazione[125] ossia il divieto di esser sottoposti a decisione «esclusivamente»[126]automatizzata ha qui un margine di applicazione limitato venendo in rilievo solo laddove la decisione produca effetti giuridici o incida significativamente sulla sfera giuridica della persona- circostanza questa non facilmente dimostrabile in caso di *group-profiling* e in generale in tutti casi personalizzazione informativa, di pubblicità comportamentale (OBA), addestramento e interazioni con gli LLMs.[127]

Quello che dunque emerge dall'analisi finora condotta è che la tutela di matrice civilistica, come quella apprestata dal GDPR, operando in via successiva all'estrazione dei dati, nel migliore dei casi, sembra poter solamente arginare alcune delle intrusioni digitali "minori" nella sfera del soggetto che si sono già verificate. Il diritto alla privacy inteso come limite all' utilizzo e commercializzazione dei dati[128] una volta astratti dalla materia a cui ineriscono e reificati in "frammenti identitari", va ad avvicinarsi solo in superficie alla sfida più fondamentale che l'economia digitale pone, e che *in primis* sta nella tutela dello spazio identitario minimo che è garanzia di uno sviluppo che possa dirsi moralmente libero della personalità individuale, e che la tutela civilistica, non può seppur implicitamente non dare per scontata.[129] Preso atto dell'ontologica porosità dei confini tra ambienti interni ed esterni,[130] così come della natura relazionale di dati e identi-

[125] Cfr. art. 22 GDPR, disposizione considerata una delle massime espressioni di quell'approccio alla privacy e alla data protection fondata sui valori democratici e costituzionali intimamente connessi alla dignità umana, cfr. E. Celeste – G. De Gregorio, *Digital Humanism: The Constitutional Message of the GDPR*, in *Global Privacy Law Review,* 3, 1, 2022, 4 ss. Si veda anche M. Rotenberg, *Artificial Intelligence and Democratic Values, The Role of Data Protection. European*, in *Data Protection Law Review,* 7, 4, 2021, 496 ss. spec. 498, secondo cui: «*It is regarded as the very expression of the right to algorithmic transparency*».

[126] Si noti che nella recente sentenza Schufa, la Corte di giustizia europea ha interpretato l'espressione "decisione basata esclusivamente su un trattamento automatizzato" in modo molto ampio. Secondo la Corte, la disposizione non riguarda solo le operazioni che hanno effetti legali diretti nei confronti dell'interessato senza alcun intervento umano, ma l'art. 22, par. 1, GDPR coprirebbe anche le previsioni automatizzate precedenti (come il credit scoring) fatte da una particolare società (Schufa), a condizione che una terza società successivamente «si basi *fortemente* su tale valore di probabilità per stabilire, attuare o terminare un rapporto contrattuale con tale persona», cfr. CGUE Causa C-634/21 OQ contro Land Hessen ECLI:EU:C:2023:957. par. 73. In merito si vedano anche E. Hine – C. Novelli – M. Taddeo – L. Floridi, *Supporting Trustworthy AI Through Machine Unlearning,* in *Science and Engineering Ethics*, 30, 5, 2024.

[127] Si vedano F. Galli – G. Sartor, *The Mismatch Between GDPR and Behavioural Advertising: What Way Forward*? in M. Ebers – K. Sein (a cura di), *Privacy, Data Protection and Data-driven Technologies,* Londra, 2024, 287 ss. Peraltro il diritto di opposizione alla profilazione automatizzata, stando a quanto previsto dall'art. 21 par.1. del GDPR (diversamente dalla disciplina contenuta nel precedente Codice della Privacy), non è riconosciuto nei casi in cui il trattamento sia fondato sul consenso- e come visto in ogni caso opererebbe limitandosi ad impedire irretroattivamente l'ulteriore trattamento dei dati.

[128] Su tale approccio si veda F. Bravo, *Il "Diritto" A Trattare Dati Personali,* cit., 195 ss.

[129] R. Esposito, *Le persone e le cose*, Torino, 2014.

[130] Il concetto di «porosità computazionale» descrive l'interpenetrazione tra agency umana e artificiale come conseguenza della permeabilità tecnica dei sistemi computazionali cfr. M. Berry, *Porosity and Computation*, in stunlaw.blogspot.com, 2024.

tà - fenomeno in costante divenire e fortemente dipendente dai rapporti (*human-human; machine-human*) che gli individui sono messi nelle condizioni di intrecciare[131]- a venire in discussione sono invece ,primariamente, le condizioni necessarie a garantire la centralità dell'agency e dell'autonomia cognitiva dell'individuo – e ciò indipendentemente dalla natura umana o artificiale delle controparti di queste relazioni. Un tale cambio di prospettiva implica allora una più ampia riflessione circa gli strumenti necessari a restituire margini di autonomia decisionale all'individuo nel determinare la soglia di interferenza (calibrata in termini di rischio) che si è disposti ad accettare e, dunque, alla soglia di fiducia che si è disposti ad accordare, ad un agente artificiale, non diversamente da quanto accadrebbe in una relazione con controparti umane.

Se, come abbiamo visto, all'approccio espertocratico che informa l'AI Act consegue l'esclusione dei destinatari "non esperti", tanto nei processi decisionali iniziali, quanto nelle fasi successive di implementazione dei sistemi di AI, l'ideazione e la messa a disposizione di nuovi modi per rendere effettivo il coinvolgimento democratico dei soggetti destinati ad essere impattati da tali tecnologie, a livello locale, regionale e globale, rappresenta il cuore della sfida.

Un modello decisionale di stampo "ecologico" complementare all'accentramento tecnocratico,[132]che colleghi dinamicamente le scelte progettazione e l'implementazione dei sistemi con norme, valori e standard specifici delle comunità ospitanti (HCs) è ciò che può dare contenuto ad un'idea di consenso *Trust-Based*: un processo orizzontale che, facendo perno sulla natura dinamica e negoziata della "fiducia in senso ampio", sia in grado di recuperare la centralità del coinvolgimento dei destinatari di una data tecnologia nel giudizio etico sotteso alla definizione di ammissibilità del rischio posto dai sistemi di AI.

Se così inteso il paradigma della *(Trustworthiness* può assurgere effettivamente a strumento d'elezione per porre al centro il momento dell'autodeterminazione degli HRs, tanto sull'*an* quanto sul il *quomodo* dell'implementazione dei sistemi di AI, enfatizzando la libertà di scelta e la natura negoziata dei principi e valori che tali tecnologie per definizione non neutrali, dovrebbero essere in grado di interiorizzare.

---

131 Pionieri, sono gli studi antropologici di E. Goffman, *The Presentation of Self in Everyday Life*, University of Edinburgh, *Social Sciences Research Centre*, 1956, trad. it. di E. Goffman, *La vita quotidiana come rappresentazione,* Bologna, 1969. Nella dottrina italiana si veda Rodotà secondo cui «È solo nel momento in cui l'identità si specifica come concetto relazionale che la protezione dei dati cambia di significato (..) e l'identità si fa comunicazione» cfr. S. Rodotà, *Il diritto di avere diritti,* Roma-Bari, 2012, spec. 322.

132 Come già suggerito in dottrina, potrebbe prevedersi un obbligo di «*disclosure by default*» volto a fornire informazioni essenziali per gli attori locali responsabili della definizione di requisiti etici specifici, come le organizzazioni in qualità di deployers o le autorità nazionali competenti di coordinamento e supervisione Cfr. J. Laux – S. Wachter – B. Mittelstadt, *Three pathways for standardisation*, cit., 51. In particolare, tra le parti interessate a livello locale dovrebbero esserci le organizzazioni che utilizzano l'AI fornita da terzi, gli individui soggetti al suo utilizzo o comunque interessati, le organizzazioni della società civile che agiscono per conto di tali individui, nonché le autorità di regolamentazione, le organizzazioni governative e intergovernative, *ibidem.*

6. Potenzialità e limiti del GPAI *Code of Practice* (CoP)

Un ruolo chiave in questa sfida, che avrebbe in astratto il potenziale di fungere da valvola di apertura orizzontale del processo decisionale, è il lavoro attualmente svolto dai quattro gruppi *multi-stakeholders*[133] istituiti presso la Commissione europea il cui scopo, con la redazione di un *Code of Practice*[134] è fornire gli strumenti tecnico operativi per concettualizzare, prevenire e rispondere adattivamente al rischio sistemico[135] posto da alcune categorie di modelli a finalità generali (GPAISR).[136] In particolare basandosi su criteri quantitativi e qualitativi l'obiettivo è dare concretizzazione e attuazione pratica ai principi generali contro specificazioni errate o tentativi di elusione, pur rimanendo «*future proof*».[137]

Se l'adesione al Codice, ad oggi in stato di bozza,[138] non costituirà prova conclusiva della conformità dei sistemi all'AI Act, tuttavia, come espresso nei considerando di apertura del documento, l'obiettivo è quello di fungere da ponte fino all'adozione di standard UE armonizzati per i modelli di AI di uso generale.[139]

Sebbene si tratti del risultato di uno sforzo collaborativo che ha già coinvolto centinaia di partecipanti provenienti dall'industria, dal mondo acca-

[133] La procedura di consultazione e la redazione delle misure è suddivisa tra quattro *Working Groups* che lavorano in parallelo: Wp 1 per la «Trasparenza e norme relative al copyright»; Wp 2 per la «Valutazione del rischio sistemico» Wp 3 per «l'attenuazione del rischio tecnico» Wp 4 per «la governance del rischio sistemico». Solo le misure in tema di Trasparenza e copyright (WP1) si applicheranno a tutti i modelli di AI di uso generale, ad eccezione di quelli rilasciati con licenza libera e open-source che soddisfano le condizioni specificate nell'art. 53, par. 2, AI Act e che non sono classificati come modelli con rischio sistemico. Le misure di cui ai WPP 2, 3 e 4 e la corrispondente Sezione III troveranno applicazione invece solo per i fornitori di modelli di uso generale con rischio sistemico (GPAISR) di cui all'art. 51, AI Act.

[134] Cfr. *Codice di buone pratiche dell'IA per finalità generali*; Code of practice, third draft.

[135] Cfr. Art.3, par. 65 che definisce il rischio sistemico come «un rischio specifico delle capacità ad alto impatto dei modelli di AI generici, che ha un impatto significativo sul mercato dell'Unione a causa della loro portata, o a causa di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, la pubblica sicurezza, i diritti fondamentali o la società nel suo complesso, che possono essere propagati su scala attraverso la catena del valore». Come detto in precedenza, per i *General Purpose Models,* la considerazione del rischio sistemico, è stata innescata esattamente in ragione dalla loro improvvisa e rapidissima diffusione seguito dal lancio di ChatGPT nelle more del trilogo tra Parlamento Commissione e Consiglio.

[136] Come detto, eccezion fatta per le regole redatte in tema di trasparenza e copyright il cui raggio si estende a tutti i modelli di AI di uso generale, il CoP troverà dunque applicazione per i fornitori di GPAI classificati con rischio sistemico (GPAISR) *ex* art. 51, AI Act.

[137] Cfr. *Second Draft General-Purpose AI Code of Practice*, cit.,1; *Third Draft*, cit., 4.

[138] La pubblicazione del testo definitivo è prevista nel mese di agosto 2025. Alla pubblicazione seguirà la valutazione dell'Ufficio e del Comitato AI, e dunque la procedura di approvazione da parte della Commissione.

[139] In particolare dettando ai providers criteri concreti e di dettaglio necessari a dimostrare la conformità agli standard e, al contempo, fornendo orientamenti dall'Ufficio AI su come valutare tale conformità per i firmatari ai sensi degli articoli 53, par. 4 e 55, par. 2, AI-Act.

demico e dalla società civile e che, dunque, avrebbe il potenziale per dare voce concreta a interessi, valori e priorità "altre" rispetto a quello delle piattaforme in veste di AI providers, tuttavia, molto dipenderà da un gioco di equilibrio in continua evoluzione, il cui esito sarà determinato non solo dall'effettiva capacità di raggiungere un assetto di interessi condiviso, ma anche dagli strumenti procedurali e sostanziali effettivamente offerti per la partecipazione e supervisione di un processo in costante riscrittura. In attesa della pubblicazione del testo finale, ciò che al momento sembra emergere dalla comparazione delle tre bozze ad oggi pubblicate è, infatti, la progressiva riaffermazione del ruolo centrale del provider, nella definizione delle condizioni di sviluppo e implementazione dei modelli che intende immettere sul mercato.

Se è vero infatti che la tassonomia (non esaustiva)[140] dei rischi sistemici contenuta nella sezione III[141] che costituirà la base immediata per l'identificazione del rischio, è il risultato di uno sforzo coordinato teso a trovare un compromesso tra i feedback di tutti gli stakeholders (fornitori, società civile e accademia) è anche vero che tale sforzo definitorio si trova ad affrontare sfide epistemologiche e tecniche prima di tutto legate al focus della legge sulle capacità tecnologiche dei modelli, piuttosto che sui contesti di impiego.[142] Circostanza questa che, oltre a rendere di per sé centrale l'expertise dei providers, da sola non risolve la sfida fondamentale che vi è sottesa, ossia il tentativo di modellare democraticamente gli impatti sociali all'interno di sistemi dinamici.[143]

L'ultima versione del Codice sembra essere il risultato, infatti, di un'interpretazione restrittiva delle disposizioni dell'AI Act che richiedono una relazione causa-effetto tra le «capacità ad alto impatto» di in modello - concetto definito come capacità che corrispondono o superano le capacità registrate nel modello di GPAI più avanzato[144] - e i rischi sistemici, in modo tale che i rischi non direttamente derivanti da tali capacità siano esclusi dalla tassonomia quelli «selezionati», *alias* resi obbligatori dal codice. Detto in altri termini questo significa che i rischi sistemici per i diritti fondamentali che non derivano dai vantaggi comparativi di questi modelli, in termini di sofisticazione o sviluppo, saranno completamente esclusi

[140] Cfr. Considerando h) e da interpretarsi in buona fede in casi dubbi (Considerando g).

[141] Redatta ai sensi dell'art. 56 AI-Act e basata sull'individuazione della natura, tipologia e fonti (i.e. capacità e propensioni del modello).

[142] In merito e sull'approccio parzialmente diverso della definizione di rischio sistemico nel DSA, si veda M. Loi – M. Fabbri – A. Ferrario, *Regulating the Undefined: Addressing Systemic Risks in the Digital Services Act (with an Appendix on the AI Act),* in *SSRN Working Paper,* 2024. Le prescrizioni tecniche nell'AI Act sono orientate verso obiettivi procedurali e standard che consentono al sistema di essere immesso sul mercato (o di rimanervi), mentre al contrario, gli obblighi tecnici nel GDPR e nel DSA mirano alla garanzia sostanziale di valori e obiettivi specifici, si veda M. Almada, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?* cit., 12.

[143] Lo stesso dicasi per le recenti tassonomie elaborate in letteratura che categorizzano tali rischi (ad esempio, controllo, democrazia, discriminazione) in relazione a fonti e capacità, cfr. R. Uuk – C. I. Gutierrez – D. Guppy – L. Lauwaert – A. Kasirzadeh – L. Velasco – P. Slattery – C. Prunkl, *A Taxonomy of Systemic Risks from General-Purpose AI,* in *arXiv preprint* 2024.

[144] Cfr. art.3, par. 64 AI Act.

dagli obblighi previsti dal Codice, riducendo drasticamente le possibilità di controllo e trasparenza. Nel passaggio dalla II alla III bozza viene riaffermata, peraltro, la netta distinzione tra «*Selected Systemic Risks*»[145] che i firmatari sono tenuti obbligatoriamente considerare e i c.d. «*Optional Systemic Risks*»[146] la cui rilevazione, gestione e mitigazione è rimessa all'iniziativa dei providers attraverso «*Voluntary Measures*». L'effetto è quello di rendere meramente "opzionale" il seguente elenco di rischi: a.) rischi per i diritti fondamentali, quali, libertà di espressione non discriminazione; rischio per la privacy e la protezione dei dati personali; materiale pedopornografico (CSAM) e le immagini intime non consensuali (NCII); b.) rischi per la salute, la sicurezza o la protezione pubblica; c.) rischi per la società nel suo complesso (tra cui ambiente; benessere dei non umani; rischio per la stabilità del sistema finanziario; rischio per i processi democratici; rischio di contenuti illegali, violenti, di odio, radicalizzanti o falsi), ad oggi, tutti testualmente ricondotti sotto l'etichetta di «Altre tipologie di rischio da considerare *potenzialmente* nella selezione dei rischi sistemici».[147] Il paradossale risultato di un simile approccio è quello di delegare alla discrezionalità (e alla buona volontà) dei providers la valutazione di rischi che l'AI Act considera come obbligatoria,[148] sostanzialmente delegando ai fornitori a valle dei sistemi di AI in cui tali modelli vengono integrati la loro identificazione e le procedure di valutazione e mitigazione.[149]

---

[145] I rischi sistemici obbligatori di cui all' Impegno II.3 sono individuati dall'*Appendix* 1.1. in: 1. Cibercriminalità: 2. Rischi chimici, biologici, radiologici e nucleari: 3. Manipolazione dannosa; 4. perdita di controllo umano, cfr. *Appendix 1.1., III Draft*, cit., 56.

[146] Cfr. *Appendix 1.2*., *ibidem,* 57.

[147] *Ibid.*

[148] Peraltro, in deroga agli approcci internazionali che il Codice dichiara di rispettare come il *Rapporto internazionale sulla sicurezza dell'AI 2025* che riconosce esplicitamente come rischi sistemici quelli legati alla privacy e all'ambiente. Sulle preoccupazioni e le critiche di un simile approccio si veda la lettera aperta inviata dai co-legislatori dell'AI Act alla Vicepresidente della Commissione Europea: *Open letter to Executive Vice-President Virkkunen on the treatment of fundamental rights risks in the Code of Practice for GPAI*, in *cdt.org/wp*. In merito alle preoccupazioni sollevate dagli stakeholders si veda *ex multiis* il position paper di BEUC *Feedback to third draft of the AI Act's Code of Practice for General-Purpose AI*, 1 April 2025; nonché CdD Europe, *Third Draft of the General-Purpose AI Code of Practice Misses the Mark on Fundamental Rights*, 18 March 2025.

[149] Il Codice giustifica le modifiche osservando che questi rischi sarebbero meglio affrontati attraverso altre parti dell'AI Act, nonché dal GDPR dal DSA e dal DMA. Tuttavia l'AI Act si applica principalmente ai "sistemi di AI", e non anche ai "modelli GPAI". Questo significa che gli obblighi relativi ai diritti fondamentali si attivano solo se un modello viene integrato in un sistema, ma non in via automatica. La valutazione del rischio in questo caso è condotta infatti a livello di sistema, in modo indipendente dal profilo di rischio del modello sottostante. Se il sistema non è da considerarsi ad alto rischio, l'AI Act non dispiega effetti regolatori aggiuntivi, lasciando potenzialmente scoperti determinati rischi legati al modello. Quanto al GDPR l'ambito di applicazione ai modelli GPAI, come noto, non è ancora chiaro. Il parere n. 28/2024 dell'EDPB ha stabilito i criteri per determinare quando un modello configuri un trattamento di dati personali, suggerendo misure di mitigazione potenzialmente idonee ad anonimizzarlo ed escluderlo dal perimetro normativo. Tuttavia, chiarisce anche che la valutazione di effettiva anonimizzazione deve essere resa caso per caso, e che le mitigazioni proposte sono non vincolanti né esaustive. In assenza di prescrizioni uniformi, spetta ai fornitori determinare in autonomia le misure necessarie alla compliance rispetto a quelle

In relazione ai rischi sistemici considerati "obbligatori" i providers di GPAISR, in adempimento a quanto previsto dal regolamento,[150] saranno tenuti ad adottare, pubblicare e trasmettere all'AI Office un *Safety and Security Framework (c.d. Model Report)* aggiornato periodicamente, che specificherà le misure e le procedure di valutazione, di mitigazione e governance del rischio sistemico[151] che i firmatari intendono adottare nei momenti chiave dell'intero ciclo di vita del modello (ie. progettazione e prototipazione, l'allenamento, pre-implementazione e distribuzione). Tuttavia, anche in questo caso, resta prerogativa dei firmatari, la definizione dei criteri in base ai quali decideranno se il rischio sistemico derivante dai loro GPAISR è accettabile.[152] Giudizio in cui la discrezionalità aumenta, a seguito dell'eliminazione nella terza bozza del Codice, della precedentemente prevista necessità di redigere una «scala fissa e comparabile tra i firmatari».[153] Peraltro la trasmissione formale all'ufficio AI e la pubblicazione del *Model Report*, come la seconda bozza si premurava di chiarire espressamente, fugando le preoccupazioni espresse dai provider in sede di prima consultazione, è ben lungi dal voler rappresentare una "pre-approvazione di fatto"[154] all'immissione del modello sul mercato, che del resto sarebbe esorbitante il dettato normativo. A ciò si aggiunga[155] il carattere non mandatorio della valutazione esterna del rischio (salvo specifiche eccezioni in ogni caso superabili dai providers)[156] anche questo chiaramente disambiguato

meramente raccomandate. L'inclusione del diritto alla privacy e alla protezione dei dati nella tassonomia dei rischi sistemici presentati dai modelli, avrebbe chiaramente facilitato l'armonizzazione degli approcci, rendendo obbligatorie le misure per ridurre al minimo l'uso dei dati personali nell'addestramento, ad oggi adottabili, stando al CoP, se «pertinenti e applicabili».

150 Cfr. art. 55(1) AI Act che stabilisce gli obblighi specifici a cui i fornitori di GPAI con rischio sistemico sono tenuti ad adeguarsi tra cui la valutazione del modello, la valutazione e la riduzione del rischio a livello dell'Unione, la documentazione degli incidenti e delle misure correttive e la protezione della sicurezza informatica.

151 In particolare Identificazione (Imp. II.3); Analisi (II.4); Valutazione (II.5) e Sviluppo; cfr. *III Draft,* cit., 8.

152 Cfr. III *Draft*, cit., 4, ove si fornisce un quadro di riferimento esplicativo suddiviso in sezioni potenziali: 1. Criteri di accettazione del rischio sistemico (Misure II.1.2-II.1.3) 2. Valutazione del rischio sistemico e decisione di procedere (Imp. II.2-II.5) 3; Attenuazioni tecniche del rischio sistemico (Imp. II.6-II.7); 4. Attenuazione del rischio di governance (Imp. I.8-II.16).

153 Cfr. *III Draft*, cit., 7, ove si argomenta che tale requisito, previsto invece in II bozza, avrebbe contraddetto la flessibilità concessa ai firmatari dal provvedimento di definire i livelli di rischio sistemico in modi diversi.

154 Come riportato nella II bozza, i provider erano preoccupati che l'invio del Model Report all'AI Office potesse suggerire la necessità di approvazione prima dell'implementazione. Per risolvere questo problema, si chiariva dunque che questo è dovuto al momento dell'immissione sul mercato, non prima.

155 In ossequio a quanto stabilito dall'art. 114, AI-Act.

156 A partire dal 2 novembre 2025, la valutazione esterna è necessaria, infatti (a condizione che il valutatore esterno indipendente abbia accettato di proteggere le informazioni commercialmente riservate, qualora necessiti di accedere a tali informazioni) esclusivamente per i rischi sistemici "obbligatori" *ie* quelli individuati ai sensi dell'Impegno II.3 (su cui si veda nota *supra)* ed in particolare quando non vi sono prove sufficienti che il modello non comporti un rischio aggiuntivo rispetto ai modelli di AI di uso generale

nel passaggio dalla prima alla seconda bozza, nonostante gli sforzi dei rappresentanti di società civile e accademia nel sottolineare l'importanza dell'obbligatorietà di test esterni pre-implementazione.

Se così è, ed ove lo scopo perseguito sia rendere verificabile e contestabile la definizione concreta del livello di tutela accordato a valori per definizione non neutrali, impliciti nella valutazione di accettabilità del rischio, il *Model Report* - per quanto strumento fondamentale - non è da solo sufficiente a garantire il raggiungimento dell'obiettivo. Sebbene la trasparenza,[157]a cui il Report è funzionale, sia precondizione per poter parlare di *accountability*[158] da sola non è in grado di determinare automaticamente l'accettabilità del rischio e dunque la *(trust)whortiness* di un sistema.

Va tenuto, peraltro, presente che nella terza versione del Codice, si afferma esplicitamente che il testo finale non conterrà più riferimenti ai *Key Performance Indicators* (KPI), previsti invece nella seconda bozza, ossia metriche numeriche di performance, con la conseguenza che stakeholder esterni e autorità non avranno strumenti analitici per verificare la conformità nel tempo.[159]A minare ulteriormente la possibilità di riequilibrio, è l'assenza

già presenti sul mercato dell'UE. (Secondo la Mis. II.11.1 della III bozza, sono esclusi i modelli derivati in modo sicuro ai sensi della Mis. II.4.2 o i modelli che presentano un livello di sicurezza uguale o maggiore di altri GPAISR che rispettino i requisiti ivi indicati). È inoltre richiesta quando il fornitore non dispone delle competenze o delle informazioni interne necessarie per condurre efficacemente la valutazione del rischio, come nei casi in cui tale valutazione richiederebbe l'accesso a informazioni sensibili rilevanti per la sicurezza nazionale. Tuttavia, l'obbligo di ricorrere alla valutazione esterna può essere superato qualora non sia possibile trovare valutatori esterni indipendenti, qualificati secondo i criteri della Mis. II.11.1, nonostante sforzi adeguati, tempestivi e in buona fede. In questo caso, i «Firmatari tengono conto del potenziale rischio aggiuntivo e dell'incertezza dei rischi sistemici derivanti dall'assenza di valutazione esterna nel determinare l'accettabilità dei rischi sistemici ai sensi dell'Impegno II.5.» cfr. *III draft,* cit., 40. Si specifica peraltro, in accoglimento delle preoccupazioni dei providers, che l'Ufficio AI, indicato in precedenza come potenziale valutatore, non debba obbligatoriamente svolgere un ruolo nella valutazione del rischio prima del collocamento sul mercato. Quanto alle valutazioni successive all'immissione sul mercato, se nella seconda bozza si chiedeva ai Firmatari di fornire «un accesso non restrittivo ai modelli utilizzati» (II.11.2) si chiarisce ora che: «(1) l'accesso alle API è sufficiente per soddisfare questa misura; (2) i Firmatari possono specificare criteri per l'accesso dei ricercatori più restrittivi per i modelli più sensibili». cfr. *ibidem*, 43. Traduzioni a cura dell'autrice.

[157] Quanto alla trasparenza pubblica (Impegno II.16) si noti che l'obbligo in base al quale i providers erano tenuti a pubblicare (in versione ridotta) i loro Model Report (o equivalenti) per favorire la consapevolezza e la conoscenza da parte del pubblico dei rischi sistemici derivanti dal modello, è stato limitato solo ai casi in cui sia strettamente necessario per valutare e mitigare il rischio, cfr. *III Draft,* 50, cit.

[158] La trasparenza è infatti un requisito procedurale che facilita il coinvolgimento dei non esperti nel garantire la responsabilità degli sviluppatori, la quale tuttavia come nota de Bruijn non ne è una conseguenza automatica cfr. H. de Bruijn – M. Warnier – M. Janssen, *The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making,* in *Government Information Quarterly,* 39, 2, 2022. Se si considera la fiducia ben riposta come dipendente dalla possibilità di esigere *accountability* nel processo decisionale basato sull'AI, è fondamentale che questa possibilità venga effettivamente esercitata. La possibilità astratta che gli sviluppatori siano chiamati a rispondere delle loro scelte non è sufficiente a giustificare la fiducia.

[159] Tra le preoccupazioni e le critiche espresse in merito alla direzione "peggiorativa" della terza bozza espressa dagli stakeholders, si veda *ex multiis* in cui, nella generale critica, CEPIC rileva come la rimozione dei KPI renda «quasi impossibile misurare se i providers

per i fornitori di GPAISR di obblighi effettivi di trasparenza in merito alla legalità dei set di dati di addestramento,[160]alla *compliance* alle richieste di *opt-out* a tutela di copyright e privacy, così come la mancata previsione di strumenti di *enforcement* di tali diritti. Oltre al generale obbligo di introduzione di procedure di reclamo, non c'è alcuna disposizione concreta circa le misure che i fornitori dovrebbero adottare in conseguenza di denunce di violazioni del Codice. Circostanza questa, che non può che limitare drasticamente la partecipazione attiva al controllo e alla negoziazione dell'affidabilità dei sistemi, creando, peraltro, disallineamento tra pratiche volontarie e obblighi normativi, dal momento che il diritto di reclamo per i sistemi ad alto rischio, così come il diritto alla spiegazione dei singoli processi decisionali, sono previsti rispettivamente dagli artt. 85 e 86 del regolamento.[161]

In conclusione la conformità in concreto alle soglie di rischio che, come ampiamente argomentato, significa anche accettabilità etico-politica dei modelli, dovrà essere valutato e dimostrato caso per caso: valutazione questa, che stando al CoP, spetta ai providers nel momento in cui, seguendo le *best practices,* gli approcci internazionali e le linee guida dell'AI Office, sono chiamati a "quantificare" quella soglia oltre la quale il rischio è da considerarsi inaccettabile. In ultima analisi è agli sviluppatori e ai fornitori di sistemi a valle che è rimessa la definizione di quel limite invalicabile da cui dipende l'ingresso di un agente artificiale nell'ecosistema.

Se così è, come è stato opportunamente rilevato, per superare le asimmetrie politiche, strutturali derivanti dall'accentramento dell'autorità epistemica in provider e tecnocrati, ciò che probabilmente è necessario è un cambio di prospettiva che –denaturalizzando la visione dell'AI come "prodotto" alla base dell'attuale quadro regolatorio,[162] la inquadri come ecosistema pubblico immanente e globale.[163]

Il modello consultazione multistakeholder necessiterebbe allora dell'ulteriore messa a punto di procedure idonee a garantire il coinvolgimento

---

stiano rispettando gli impegni».

[160] I fornitori di GPAI potranno conformarsi aderendo a misure tecniche di controllo dell'accesso, combinate con «sforzi ragionevoli» per escludere dall'addestramento dati soggetti a copyright.

[161] Si veda in merito il *Joint statement* del 28/03/2025, in cui 37 organizzazioni che rappresentano autori, performer, giornalisti, musicisti, editori, industrie audiovisive e giornalistiche ritirano il loro appoggio alla III bozza e ai lavori della Commissione in quanto «(„) *undermines the objectives of the AI Act, contravenes EU law and ignores the intention of the EU legislator*» in *Joint statement by a coalition of authors, performers and other rightsholders active across the EU's cultural and creative sectors regarding the third draft of the EU AI Act's GPAI Code of Practice Summary,* Bruxelles, 28 March 2025. In particolare, sulle preoccupazioni in merito al futuro della libertà di informazione si veda ancora il comunicato CEPIC «Il lavoro dei giornalisti continuerà a essere estratto, riutilizzato e monetizzato dalle aziende di intelligenza artificiale, senza licenze né trasparenza, e con rischi crescenti di disinformazione a causa delle allucinazioni dell'AI»: CEPIC, *From Bad to Worse: CEPIC Strongly Opposes the Third Draft of the EU Code of Practice under the AI Act,* 28 March 2025, traduzione a cura dell'autrice.

[162] In merito e sulle ragioni della scelta si rimanda a M. Almada - N. Petit, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?* cit.

[163] Cfr D. Leslie et al. *Frontier AI, Power and the Public Interest,* cit.

politico necessario a dare contenuto concreto ai valori impliciti alla nozione di eticità e di bene pubblico che, in quanto tale, necessita di essere articolato e declinato in obiettivi condivisi localmente per orientare i progetti.[164]Questo significa non soltanto integrare procedure di reclamo *ex post* adeguatamente strutturate, ma andare oltre modelli "blindati" di buone pratiche incentrati unicamente su interessi e "sforzi ragionevoli" dei providers.

7. Riflessioni conclusive

Ai fini di rendere la risposta regolatoria non solo reattiva, ma dinamica e adattiva e ove lo scopo della tutela sia la resilienza della sfera incomprimibile dell'individuo da quelle che sono da considerarsi "rischi digitali" inammissibili, l'anticipazione del momento della tutela di diritti fondamentali, come privacy e protezione dei dati ad un momento che precede l'intrusione digitale, a nostro avviso, è precondizione per potersi parlare "affidabilità" di un sistema di AI. Si è dunque individuata una possibile traiettoria evolutiva che prendendo le mosse dall'analisi del concetto *Trust in technology* nel senso sociale, interpersonale ed epistemico del termine, sia in grado di dare contenuto a un' idea di consenso come processo negoziato ed iterativo volto a garantire margini di autonomia decisionale ai individui e "comunità ospitanti" circa la soglia di interferenza (calibrata in termini di rischio ai diritti fondamentali) che si è disposti ad accettare e, dunque, alla soglia di fiducia che si è disposti ad accordare, ad un agente artificiale. IL cambio di prospettiva che il modello di *Trust Based Consent* implicherebbe, è infatti, a nostro avviso essenziale, non soltanto per leggere criticamente le limitazioni ontologico strutturali insite all'approccio dualistico alla tutela dei dati che informa l'architettura del GDPR, ma lente critico-operativa per riflettere sulla natura degli strumenti normativi necessari *de iure condito* e *de iure condendo* per il recupero della centralità dell'autodeterminazione dell'individuo nella definizione del proprio percorso di esistenziale ed identitario, di cui la pervasiva relazione con l'agency artificiale è elemento co-determinante. Rendere partecipi gli *human recipients* delle decisioni destinate a plasmare la fisionomia ed il *modus operandi* degli agenti artificiali con cui andranno ad interagire, significa anche restituire controllo sui termini di quelle relazioni che, per quanto a controparte non umana, sono co-determinanti dei processi di costruzione identitaria. Se l'autodeterminazione è costitutiva dell'idea di persona e la libertà di costruzione identitaria - ne è presupposto e conseguenza,[165] è prima di tutto necessario far sì che l'individuo sia posto davvero nelle condizioni di creare il proprio percorso esistenziale e tutelarlo nel suo evolversi, scongiurando forme di etero-regolamentazione tanto umana, quanto algoritmica.

Un modello decisionale alternativo all'approccio puramente espertocratico, di natura orizzontale, volto a garantire la possibilità di comprendere e

[164] *Ibidem.*.

[165] «Costruzione della sfera privata, sovranità su di sé e determinazione dei legami sociali si congiungono» cfr. S. Rodotà, *Persona, riservatezza, identità, Prime note sistematiche sulla protezione dei dati personali,* in *Riv. Crit. del Dir. Priv.,* 15, 1997, 603.

co-definire le condizioni giustificano l'*an* ed il *quomodo* dell' immissione ed evoluzione degli agenti di AI nell'ecosistema, è allora un passo fondamentale, non solo per limitare l'ulteriore accentramento dell'autorità epistemica negli AI providers, ma anche e soprattutto per scongiurare il rischio che l'interazione tra agency umana e artificiale non assuma le forme di una colonizzazione dello spazio che vogliamo costitutivo dell'idea di individuo e delle sue possibilità identitarie. Affinché un tale modello "ecologico" sia concretamente realizzabile, il primo passo è, allora, cominciare a trattare le esternalità negative dei sistemi di AI, non solo come un problema tecnico da risolvere, attraverso una migliore documentazione o interfacce, ma come una questione politica che impone, da un lato, la necessità di rafforzare quelle condizioni sostanziali e procedurali idonee a garantire una reale redistribuzione del potere decisionale, dall'altro richiede, in uno sforzo prospettico, l'impegno a creare "confini porosi" tra conoscenza esperta e pubblica.[166]

Se si vuole realmente evitare che l'asimmetria epistemica tra non esperti ed esperti si traduca in un'asimmetria politica,[167] funzionale all'obiettivo è anche la creazione delle condizioni sostanziali e procedurali per pensare ad un'*AI Literacy* di natura critica,[168] che rendendo gli individui consapevoli delle sfide etiche, sociali e politiche sottese al percorso che da vita ad un sistema di AI e alla datificazione che sottende, fornisca gli strumenti epistemici necessari affinché le relazioni *machine-human* non traslitterino in intrusioni, in particolare in ciò che più profondamente definisce il senso il sé: l' autonomia cognitiva e la libertà di scelta e azione nei processi di costruzione identitaria.

---

166 In merito si veda ancora M. Berry, *Porosity and Computation*, cit.

167 Sull' equità democratica nella gestione collettiva del rischio, si veda M. Kusch, *Towards a Political Philosophy of Risk: Experts and publics in deliberative democracy*, in *Risk: Philosophical Perspectives* 131, 2007.

168 Dove l'alfabetizzazione funzionale all'AI è condizione sicuramente necessaria, ma non sufficiente. Su questo tema cfr. D. Monett - G. Bogdan, *Deconstructing the AI Myth: Fallacies and Harms of Algorithmification,* 2024 secondo cui «*involve people affected directly by AI in all phases of its lifecycle; that is the best way to design, develop, test, deploy, and use, i.e. deal with AI*» spec. 7. Sulla necessità di iniziative di educazione e consultazione pubblica, supportate da un'adeguata regolamentazione della privacy e da una regolamentazione delle procedure volte a migliorare la fiducia si veda anche G. L. Gilbert, C. Degeling - J. Johnson, *Communicable Disease Surveillance Ethics in the Age of Big Data and New Technology*, in *Asian Bioethics Review*, 11, 2, 2019, 173 ss.

Abstract

Obiettivo di questo contributo è analizzare la misura in cui l'attuale declinazione "espertocratica" di *(Trust)worthiness* delineata dall'AI Act, riesca a garantire, oltre che a "comunicare" il rispetto di un principio cardine della visione umano-centrica dell' AI: la sovranità della decisione umana, intesa (anche) come autonomia decisionale degli *Human Recipients* (HRs) nella definizione dell' *an* e del *quomodo* dello sviluppo di determinati sistemi di AI e delle relative modalità computazionali, in determinati contesti d'uso. Dopo aver condotto una parallela analisi degli strumenti di tutela *ex post* previsti dal GDPR, nonché delle criticità dell'attuale processo di redazione del *GPAI-Code of Practice,* si argomenterà come, la denaturalizzazione della visione dell'AI come prodotto, sia precondizione per la costruzione di quello che definiamo «*Trust Based Consent*»: un modello decisionale, alternativo all'approccio espertocratico, che, recuperando il ruolo chiave della "fiducia" come processo bidirezionale e iterativo, riconosca il coinvolgimento democratico degli HRs nella definizione *ex ante* dell'ammissibilità in concreto del rischio per i diritti fondamentali che si è disposti ad accettare, collegando le scelte di progettazione sviluppo ed implementazione ai valori e agli standard specifici delle "comunità ospitanti".

With the aim of tracing an evolutionary pathway from informed consent to a broader notion of "Trust-Based Consent", this paper examines the limits of the current "expertocratic" framing of (Trust)worthiness in the AI Act. It asks whether, and to what extent, such a framework can genuinely guarantee, rather than merely "communicate", the normative foundations of a human-centric approach to AI. At its core lies the principle of human decision-making sovereignty, understood also as the autonomy of Human Recipients (HRs) to take part in decisions on the concrete admissibility of risks to fundamental rights posed by the AI systems with which they are expected, willingly or not, to interact, as well as by the associated computational configurations. Through a parallel analysis of the *ex post* safeguards under the GDPR and the critical issues of the GPAI Code of Practice drafting process, the paper argues that de-naturalizing the view of AI as a product is crucial to enabling an alternative governance model, grounded in democratic participation of HRs. Such a model should reclaim trust as a bidirectional and iterative process, linking the design and implementation of AI systems to the specific norms, values, and standards of host communities across the entire AI value chain.

Keywords

Trust & Trustwhortiness – AI Act Trustworthy Framework – GPAI Code of Practice – Data Protection – Human Agency - Machine Agency

Riflessioni sull'impatto dell'intelligenza artificiale sul rispetto del diritto internazionale umanitario e il ruolo del principio di umanità*

Alice Civitella

Sommario

1. Introduzione. – 2. L'intelligenza artificiale nei conflitti armati: sistemi d'arma autonoma e sistemi di supporto alle decisioni. – 3. Problemi relativi al rispetto del diritto internazionale umanitario: principi di distinzione, proporzionalità e precauzione. – 4. Tra etica e diritto: Clausola Martens e principio di umanità. – 5. Conclusioni.

1. Introduzione

Per transizione digitale, generalmente, si intende il fenomeno per il quale individui, imprese e servizi pubblici si dotano di nuove tecnologie, creando così nuove occasioni ed opportunità[1]. Tale transizione è stata resa particolarmente evidente dal sempre più pervasivo ruolo dell'intelligenza artificiale (IA)[2] in vari ambiti della nostra vita quotidiana: dal campo medico e giudiziario, fino ai sistemi di guida autonomi delle automobili. Come testimoniato dalla proliferazione a livello nazionale, regionale ed internazionale di normative, standard e linee guida[3], tale fenomeno ha generato

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1 Parlamento dell'Unione europea, *Plasmare la trasformazione digitale: spiegazione della strategia dell'UE*, in europarl.europa.eu

2 Ai fini di questa analisi, si prenderà come riferimento la definizione di intelligenza artificiale fornita all'art. 3 del c.d. *EU AI Act*: «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». V. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale, Gazzetta Ufficiale dell'Unione europea, 2024/1689

3 Ad esempio v.: Governo italiano, *Strategia italiana per l'intelligenza artificiale 2024- 2026*, in *gov.it;* Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno, cit.; Nazioni Unite, *AI Advisory Body*, in *un.org*; Consiglio d'Europa, *The Framework*

nuovi quesiti giuridici per i quali, tuttavia, non sempre vi sono risposte certe.

La transizione digitale, tuttavia, non è limitata al solo ambito civile. Negli ultimi anni si è assistito all'espansione dell'applicazione dell'IA anche in ambito militare. Sebbene le potenzialità di tale tecnologia comincino solo ora ad essere esplorate, essa già rappresenta una vera e propria rivoluzione nella condotta delle ostilità[4]. Gli algoritmi di IA – e quelli di *machine learning* in particolare – vengono impiegati per diverse finalità: dalla logistica, alla raccolta ed analisi di informazioni di intelligence, fino ad arrivare al supporto diretto e indiretto nella condotta delle ostilità. Vi sono due applicazioni di tale tecnologia che hanno particolarmente destato l'interesse della comunità internazionale: i sistemi d'arma autonomi in grado di esercitare una forza di tipo letale (*Lethal Autonomous Weapon Systems*, d'ora in avanti "armi autonome") e, più recentemente, i sistemi autonomi di supporto alle decisioni (*Decision Support Systems*, d'ora in avanti "DSS"). In tali casi più che in altri, l'elevato livello di autonomia nel processo decisionale che porta all'impiego della forza armata, e la conseguente progressiva erosione della decisione umana, hanno suscitato preoccupazioni ed interrogativi di natura etica e giuridica più volte espressi da Stati, società civile ed organizzazioni internazionali, *in primis* le Nazioni Unite[5].

A fronte di ciò, il presente contributo si prefigge l'obbiettivo di indagare le sfide che le suddette applicazioni dell'IA nei conflitti armati pongono per il rispetto del diritto ivi applicabile, il diritto internazionale umanitario (DIU). Tale indagine vuole in particolar modo rispondere alla necessità di ricostruire in modo sistematico le comunanze e differenze in merito all'applicazione di tale tecnologia nei DSS e nelle armi autonome e le sfide che essa pone al fine del rispetto del DIU. Muovendo, infatti, dalla constatazione di una trattazione spesso e volentieri settoriale delle diverse applicazioni dell'IA nei conflitti armati, il presente contributo intende da un lato fornire una panoramica delle principali difficoltà poste da questa tecnologia ai fini del rispetto dei principi fondamentali del DIU applicabili al processo del *targeting*; dall'altro vuole investigare il ruolo che il principio di umanità, quale principio fondamentale del DIU, assume di fronte all'impiego di nuove tecnologie nei conflitti armati.

A tal fine, nel secondo paragrafo verrà effettuata un'analisi introduttiva sull'impiego dell'IA all'interno delle armi autonome e dei DSS, descriven-

---

Convention on Artificial Intelligence and human rights, democracy and rule of law, in *coe.int*

[4] Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach,* in *International Review of the Red Cross*, 102-913, 2020, 465. Per un approfondimento, v. Y. Zhang - Z. Dai - L. Zhang - L. Wang - Y. Zhou, *Application of Artificial Intelligence in Military: From Projects View,* in *6th International Conference on Big Data and Information Analysis*, 2020; N. Masuhr, *AI in Military Enabling Applications*, in *CSS Analyses in Security Policy*, 251, 2019

[5] Ad esempio, v.: Comitato Internazionale della Croce Rossa, *Artificial Intelligence*, in *icrc.org*; Assemblea generale delle Nazioni Unite, *Current developments in science and technology and their potential impact on international security and disarmament efforts Report of the Secretary-General*, A/79/224, 23 luglio 2024; Assemblea generale delle Nazioni Unite, *General and complete disarmament Report of the First Committee,* draft XX e XLIII A/79/408*, 15 novembre 2024; Nazioni Unite, *Security Council Debates Use of Artificial Intelligence in Conflicts, Hears Calls for UN Framework to Avoid Fragmented Governance*, SC/15946, in *press.un.org*, 19 dicembre 2024

done le particolari caratteristiche, comunanze e differenze. Nel terzo paragrafo, invece, si descriveranno i principali problemi che l'impiego di algoritmi di IA nelle suddette applicazioni fa sorgere in relazione al rispetto del DIU e, specificatamente, dei principi di distinzione, precauzione e proporzionalità. A conclusione dell'analisi giuridica, il quarto paragrafo sarà incentrato sull'analisi del principio di umanità come espresso all'interno della Clausola Martens ed alle sue potenzialità in merito alla regolamentazione di armi autonome e DSS. Infine, verranno tratte alcune considerazioni conclusive in merito all'analisi effettuata.

2. L'intelligenza artificiale nei conflitti armati: sistemi d'arma autonoma e sistemi di supporto alle decisioni

L'IA trova ormai ampia applicazione all'interno dei conflitti armati. Pur non essendo in grado, almeno per il momento, di replicare la flessibilità e l'adattamento tipici dell'intelligenza umana, essa può essere addestrata al fine di svolgere compiti specifici[6]. È in questo senso che ci si riferisce all'IA come ad una *enabling technology*, ossia come ad una tecnologia nata e sviluppata allo scopo di aiutare l'essere umano nello svolgimento di particolari attività[7].

Oggigiorno essa viene applicata al fine di rendere automatizzati e più efficienti diverse mansioni legate all'ambito militare come, ad esempio, logistica e rifornimenti; addestramento delle forze armate attraverso la creazione di simulazioni e *wargaming*[8]; condotta di operazioni cibernetiche e dell'*information warfare*[9]; assistenza nelle operazioni finalizzate a fornire assistenza umanitaria[10]; supporto al decisore umano nelle varie fasi che compongono il processo del *targeting*[11]; finanche, la potenziale "sostituzione" dell'operatore umano nel caso delle armi autonome. Tra queste, solamente le applicazioni dell'IA con un impatto diretto sulla condotta delle ostilità saranno di interesse ai fini del rispetto del DIU, specialmente qualora considerate

[6] In questo senso ci si riferisce all'impiego odierno di *narrow AI* contrapposta alla *general* o *strong AI* la quale si prevede sarà in grado di svolgere una vasta gamma di compiti complessi meglio di un essere umano anche in situazioni mai incontrate prima, nonché di immaginare e creare. Sul punto: P. Scharre, *Military Applications of Artificial Intelligence: Potential Risks to International peace and Security*, in *Report the Militarization of Artificial Intelligence,* Stanley Centre for peace and Security, 2019, 12; W. Boothby, *AI Warfare and the Law*, in *International Law Studies,* 104, 2025, 33-34

[7] P. Scharre, *Military Applications of Artificial Intelligence: Potential Risks to International peace and Security*, cit., 11

[8] A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, Comitato Internazionale della Croce Rossa, 2024, 20

[9] Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach,* cit., 467

[10] Ivi, 469-470

[11] Processo volto alla distruzione o neutralizzazione delle forze ed equipaggiamenti delle forze armate avversarie

parte dei mezzi e metodi di guerra[12]. Come già sottolineato, tra queste vi sono due applicazioni che rilevano in particolar modo: le armi autonome e la più ampia categoria dei DSS impiegati nel processo del *targeting*. Nel caso delle prime, ci si riferisce a sistemi d'arma in grado di arrivare "autonomamente" all'impiego della forza armata. Nel caso dei secondi, invece, si intendono sistemi il cui compito si "limita" ad una fase di analisi e informativa, i quali, quindi, non si configurano come "armi" in senso stretto. In generale, l'impiego dell'IA all'interno delle armi autonome e dei DSS comporta l'ottimizzazione – in termini di riduzione dei tempi e contestuale aumento dell'efficienza – dello svolgimento del c.d. *OODA loop* (*Observe, Orient, Decide, Act*)[13]. Se l'impiego dei DSS, come vedremo, si concentrerebbe nelle prime due fasi[14], le armi autonome, invece, sono potenzialmente in grado di effettuare l'intero *loop* autonomamente[15]. A ciò si deve aggiungere che, tra i diversi tipi di IA, il *machine learning* si prevede sarà quello maggiormente utilizzato nelle applicazioni militari[16]. Esso, infatti, creando dei modelli dai dati fornitigli nella fase di addestramento, è in grado di effettuare delle generalizzazioni quando messo davanti ad elementi sconosciuti[17]. In tal senso, si suole dire che il *machine learning* è in grado di

[12] Con il termine "mezzi e metodi di guerra" si considerano le armi ed i sistemi d'arma da un lato, e le modalità in cui essi vengono impiegati e le tattiche militari dall'altro. Sul punto v., C. Pilloud- J. De Preux- Y. Sandoz et al., *Commentary on the Additional Protocols to the Geneva Conventions of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Ginevra, 1987, para 1402, 398; J. McClelland, *The review of weapons in accordance with Article 36 of Additional Protocol I*, in *International Review of the Red Cross*, 85-850, 2003, 404. Per un approfondimento sulle applicazioni che non hanno un impatto diretto sulla condotta delle ostilità v. S. Grand-Clément, *Artificial Intelligence Beyond Weapons. Application and Impact of AI in the Military Domain*, Istituto di ricerca delle Nazioni Unite sul disarmo, Ginevra, 2023

[13] Processo decisionale sviluppato dal Colonnello John Boyd degli Stati Uniti da utilizzare durante le operazioni militari. V.: J. Boyd, *A Discourse on Winning and Losing, Edited and Compiled by Dr Grant T Hammond*, Maxwell AFB, 2018. Sul punto v. J. Johnson, *Automating the OODA loop in the age of intelligence machines: re-affirming the role of humans in command-and-control decision-making in the digital age,* in *Defence Studies*, 23-1, 2023, 43 ss.; O. Daniels, *Speeding Up the OODA Loop with AI. A Helpful or Limiting Framework,* in japcc. org, maggio 2021; T. McFarland, *Autonomous Weapon Systems and the Law of Armed Conflict. Compatibility with International Humanitarian Law*, Cambridge, 2020, 35-36; A. Backstrom - I. Henderson, *New Capabilities in Warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons review,* in *International Review of the Red Cross*, 94-886, 2012, 491

[14] V., Comitato Internazionale della Croce Rossa e Geneva Academy of International Humanitarian law and Human Rights, *Artificial Intelligence and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts Current Developments and Potential Implications*, Ginevra, 2024, 11-13

[15] T. McFarland, *Autonomous Weapon Systems and the Law of Armed Conflict. Compatibility with International Humanitarian Law*, cit., 35-36; A. Backstrom - I. Henderson, *New Capabilities in Warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons review,* cit., 491; O. Daniels, *Speeding Up the OODA Loop with AI. A Helpful or Limiting Framework,* cit.

[16] A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, cit., 1

[17] Per un approfondimento v. W. Burgard, *Artificial Intelligence. Key Technologies and Opportunities*, in S. Voeneky - P. Kellmeyer - O. Mueller - W. Burgard (eds.), *The Cambridge Handbook of Responsible Artificial Intelligence. Interdisciplinary Perspectives*, Cambridge, 2022, 1

"imparare" e di "adattarsi" a seconda delle circostanze incontrate durante il suo impiego e senza l'intervento di un operatore umano, consentendogli di svolgere compiti dalla crescente complessità in tempi ridotti[18]. Vi sono, tuttavia, delle differenze tra queste due applicazioni che meritano di essere sottolineate.

Nello specifico, le armi autonome si distinguono da altre tipologie di armi più "tradizionali" [19]per la capacità di svolgere autonomamente e, potenzialmente, in assenza di supervisione umana, le c.d. funzioni "critiche" del processo del *targeting*. In altri termini, esse sono in grado di identificare, ingaggiare ed attaccare potenziali obiettivi militari[20]. Un'arma autonoma, più nel dettaglio, una volta attivata e avvalendosi dell'uso di varie tipologie di sensori, analizza l'ambiente operativo, si orienta in esso, e sfruttando i dati e le informazioni pervenutegli dai sensori, identifica potenziali obiettivi militari. Infine, essa "decide" qualora attaccare l'obiettivo e le modalità migliori per farlo. L'elemento cruciale di tali armi, dunque, si realizza nella potenziale "sostituzione" dell'essere umano nelle decisioni inerenti all'impiego della forza, delegandole ad un *controller*, ossia un hardware o un software[21]. Per quanto spesso descritte come armi del futuro, si è assistito a recenti impieghi di armi autonome in alcuni conflitti armati. Alcuni esempi sono rappresentati dall'impiego di sistemi di difesa aerea quali Iron Dome e Arrow 2 e 3 da parte di Israele in difesa da attacchi missilistici proveniente da Hamas e dallo Stato iraniano[22], o, ancora, dall'impiego di *loitering munitions* quali i missili Harpy, Horep e Harpy-2, durante il conflitto tra Azerbaigian e Armenia nella regione del Nagorno-Karabakh del 2020[23]. Quest'ultime, in particolare, sono programmate al fine di sorvolare

---

ss.

[18] M. A. Visger, *Garbage In, Garbage Out. Data Poisoning Attacks and Their Legal Implications*, in L.A Dickinson -E. W. Berg (eds.), *Big Data and Armed Conflict Legal Issues Above and Below the Armed Conflict Threshold,* New York, 2024, 182

[19] Da notare che al momento non esiste una definizione condivisa di "arma autonoma" o "arma letale autonoma". Si prenderà dunque qui come riferimento la definizione adottata dal Comitato Internazionale della Croce Rossa, che definisce queste armi come sistemi che *«[…] select and apply force to targets without human intervention. After initial activation or launch by a person, an autonomous weapon system self-initiates or triggers a strike in response to information from the environment received through sensors and on the basis of a generalized "target profile". This means that the user does not choose, or even know, the specific target(s) and the precise timing and/or location of the resulting application(s) of force».* Disponibile presso: Comitato internazionale della Croce Rossa, *ICRC position on autonomous weapon systems,* in *icrc.org*, 12 maggio 2021

[20] Più nel dettaglio, le funzioni critiche riguardano la selezione degli obiettivi (cercare o rilevare, identificare, seguire, selezionare) e la fase di attacco (usare la forza contro, neutralizzare, danneggiare o distruggere). Per un approfondimento su questo concetto v., D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* Cheltenham, Northampton, 2022, 36

[21] Per una disamina sulle funzionalità tecniche delle armi autonome, v. T. McFarland, *Autonomous Weapon Systems and the Law of Armed Conflict. Compatibility with International Humanitarian Law*, cit., 32 ss.

[22] G. Doyle - M. Zafra – A. Arranz - J. Chowdhury, *Israel's Iron Dome*, in *reuters.com*, 18 aprile 2024; BBC, *What are Israel's iron Dome, Arrow and Thaad missile defences?,* in *bbc.com*, 16 ottobre 2024

[23] F. Ancona, *AI in warfare: Loitering Munitions-Current Applications and Legal Challenges*, in *mondointernazionale.org*, 26 febbraio 2024

una determinata area per un predeterminato periodo di tempo al fine di "cercare" potenziali obiettivi da ingaggiare autonomamente, qualora corrispondenti ai parametri prestabiliti[24].

Tale autonomia è sovente conferita dall'uso di algoritmi di IA[25]. Sebbene divergenze di opinioni esistano in merito alla necessità dell'IA per far sì un'arma sia definita come "autonoma"[26], è certo che l'impiego di questa tecnologia sta assumendo un ruolo centrale nello sviluppo ed utilizzo di tale tipologia di armamenti[27]. Essa, infatti, basandosi sulla raccolta e il processo di un'enorme mole di dati, incrementa le capacità autonome di queste armi nelle funzioni critiche, ad esempio, conferendo maggiore precisione nell'identificazione di obiettivi tramite un calcolo di tipo stocastico e, più in generale, rendendole più affidabili nello svolgimento di specifiche attività[28]. Tuttavia, la capacità di adattamento conferita dal *machine learning*, come vedremo, rende spesso e volentieri imprevedibili tali sistemi, specialmente qualora messi di fronte a condizioni diverse da quelle di addestramento.

---

[24] Per un approfondimento v., M. Voskuijil, *Performance Analysis and the Design of Loitering Munitions: a comprehensive technical survey of recent developments*, in *Defence Technology*,18-3, 2022

[25] Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach*, cit., 466

[26] Infatti, spesso e volentieri vi è una sovrapposizione di significati tra "autonomia" ed "intelligenza artificiale". Il riferimento alle capacità autonome rimane generico, incentrato più su ciò che l'arma è in grado di fare rispetto a quelle che sono le effettive caratteristiche tecniche di tale autonomia. Poca chiarezza esiste in merito all'effettivo impiego di algoritmi di intelligenza artificiale nelle armi autonome esistenti, e, conseguentemente, a quale tecnologia conferisce in realtà l'autonomia. Ad esempio, H. Nurbanu*, Defining Weapon Systems with Autonomy: The Critical Functions in Theory and Practice*, in *Groningen Journal of International Law*, 9-2, 2022, considera l'autonomia come il risultato dell'impiego dell'intelligenza artificiale, e, quindi, si può intendere che le esistenti armi autonome ne siano dotate; T. McFarland - Z. Assaad, *Legal review of in situ learning in autonomous weapons*, in *Ethics and Information Technology*, 25-9, 2023 considerano le crescenti problematiche che l'impiego di intelligenza artificiale nelle armi autonome avrà in futuro, senza specificare se le attuali armi autonome ne siano provviste; J-F Caron, *Defining semi-autonomous, automated and autonomous weapon systems in order to understand their ethical challenges*, in *Digital War,* 1, 2020 sottolinea che non tutte le armi autonome hanno, in realtà, vere capacità di autonomia e che l'impiego di intelligenza artificiale aiuterà in future lo sviluppo di vere capacità autonome, lasciando intendere che le attuali armi autonome ne siano sprovviste; Taddeo - A. Blanchard, *A Comparative Analysis of the Definitions of Autonomous Weapons Systems*, in *Science and Engineering Ethics*, 28-37, 2022 parlano di armi autonome basate su *autonomous artificial agents*, sottolineando, allo stesso tempo, che alcune definizioni di armi autonome menzionano capacità che solo l'intelligenza artificiale potrà conferire in futuro. Infine, l'ufficio delle Nazione Unite sugli affari per il disarmo sostiene che non tutte le armi autonome impiegano intelligenza artificiale, in quanto essa viene impiegata per aumentare l'autonomia di tali armi: v. UNODA, *Lethal Autonomous Weapon Systems (LAWS),* in disarmament.unoda.org. Tale mancanza di chiarezza è illustrata molto bene da A. Seixas-Nunes, *The Legality and Accountability of Autonomous Weapons Systems. A Humanitarian Law Perspective*, Cambridge, 2022, 100 ss.

[27] Per un approfondimento v., E. M. Forrest - B. Boudreau - A. J. Lohn - M. Ashby - C. Curriden - K. Klima -D. Grossman, *Military Applications of Artificial Intelligence. Ethical Concerns in an Uncertain World,* RAND Corporations, 2020

[28] Il riferimento è alla capacità dell'intelligenza artificiale di aumentare la *reliability* di tali armi. Sul punto v., W. Boothby, *AI Warfare and the Law*, cit., 42-43; T. McFarland - Z. Assaad, *Legal review of in situ learning in autonomous weapons*, cit., 9

Somiglianze e differenze vi sono in relazione ai *Decision Support Systems*. Essi possono essere definiti come strumenti informatici progettati per assistere gli operatori umani nel prendere decisioni complesse a diversi livelli della catena di comando. Il loro impiego risponde, dunque alla *need for speed* dei conflitti armati odierni, aiutando il comandante a completare in modo veloce ed efficiente il processo decisionale[29]. Sebbene i DSS siano da tempo impiegati nei conflitti armati, il ricorso all'IA in questi sistemi rappresenta un'assoluta novità. Essa permette a questi sistemi di raccogliere, processare ed analizzare diverse tipologie di dati provenienti da svariate fonti[30] e di restituirli all'operatore umano sotto forma di analisi, predizioni o raccomandazioni[31]. Diventa così possibile non solo comprendere meglio l'ambiente operativo in cui ci si trova ad operare, ma anche prendere delle decisioni in un tempo drasticamente ridotto[32]. I DSS sono impiegati nella condotta delle ostilità per svolgere svariate mansioni*:* dalla raccolta ed elaborazione di informazioni di intelligence e identificazione e prioritizzazione di obiettivi militari, fino alla determinazione del tempo e delle modalità migliori per effettuare un attacco, inclusa la scelta dei mezzi e metodi di guerra più indicati[33]. Come nel caso delle armi autonome, anche i DSS vengono utilizzati in diversi conflitti armati contemporanei. Ad esempio, nel contesto del conflitto armato israelo-palestinese è noto l'impiego di sistemi quali The Gospel e Lavender, addestrati ed impiegati al fine di fornire agli operatori umani "liste" di potenziali obiettivi militari. Se nel caso del primo gli obiettivi segnalati rientravano tra la più ampia categoria degli "oggetti" usati ai fini militari, nel caso del secondo, invece, gli obiettivi identificati erano individui potenzialmente affiliati di Hamas e delle Jihad Islamica per la Palestina[34]. Ancora, nel contesto del conflitto tra la Federazione Russa e l'Ucraina, è stato riportato l impiego alcuni DSS

[29] A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, cit., 17; Comitato Internazionale della Croce Rossa e Geneva Academy of International Humanitarian law and Human Rights, *Artificial Intelligence and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts Current Developments and Potential Implications*, cit., 8

[30] Quali, ad esempio, immagini satellitari, dati rilevati da sensori, immagini audio-video, frequenze e segnali di cellulari

[31] Comitato Internazionale della Croce Rossa e Geneva Academy of International Humanitarian law and Human Rights, *Artificial Intelligence and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts Current Developments and Potential Implications*, cit., 9; Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach*, cit., 468-469

[32] A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, cit., 18

[33] Ivi, 55 ss.; Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach*, cit., 468; Comitato Internazionale della Croce Rossa e Geneva Academy of International Humanitarian law and Human Rights, *Artificial Intelligence and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts Current Developments and Potential Implications*, cit.,9

[34] Y. Abraham, *'Lavender': The AI machine directing Israel's bombing spree in Gaza,* in *972mag.com*, 3 aprile 2014**;** M. N. Schmitt, *Israel – Hamas 2024 Symposium – The Gospel, Lavender, and the Law of Armed Conflict*, in *liber.westpoint.edu,* 28 giugno 2024; T. Mimran - M. Pacholska - G. Dahan - L. Trabucco, *Israel – Hamas 2024 Symposium – Beyond the Headlines: Combat Deployment of Military AI-Based Systems by the IDF,* in *liber.westpoint.edu*, 2 febbraio 2024

prodotti da Palantir nonché di altri sistemi di produzione ucraina, come Kropyva e GISA Arta, al fine, ad esempio, di svolgere funzioni quali la raccolta e il processo di dati, fino all'esecuzioni di compiti legati alle fasi più critiche del processo del *targeting*.[35]

3. Problemi relativi al rispetto del diritto internazionale umanitario: principi di distinzione, proporzionalità e precauzione

L' IA pone delle sfide peculiari per il rispetto del DIU che accomunano armi autonome e DSS. A rischio di semplificare, esse riguardano: l'imprevedibilità dell'IA; i rischi legati alla mancanza di accuratezza, rappresentatività, veridicità ed integrità dei dati; i *bias* cognitivi che scaturiscono dalla relazione uomo-sistema autonomo; e infine, il pericolo che l'IA, pur partendo da condizioni e presupposti ottimali, commetta degli errori imprevedibili per l'essere umano. Tutti questi elementi, singolarmente o cumulativamente, possono inficiare l'*output* del sistema autonomo. In altri termini, a causa delle sue caratteristiche intrinseche, un sistema dotato di IA potrà agire, o portare l'essere umano ad agire, in modo non conforme al DIU. Partendo da queste premesse, in questo paragrafo si fornirà un'analisi introduttiva sui problemi posti dall'impiego dell'IA nelle applicazioni sopra descritte per il rispetto dei principi fondamentali DIU che governano il processo del *targeting*: distinzione, proporzionalità e precauzione.

L'impiego di nuove innovazioni tecnologiche nella condotta delle ostilità ha da sempre caratterizzato i conflitti armati[36]. Non a caso, già nella Dichiarazione di San Pietroburgo del 1868 gli Stati avevano espresso la necessità di regolare, tramite i principi generali del DIU, i nuovi mezzi e metodi di guerra quali derivanti dal progresso tecnologico[37]. Si può perciò affermare che l'IA rappresenti l'ultima sfida posta nello sviluppo dei mezzi e metodi di guerra cui il DIU deve rispondere. È d'uopo evidenziare, a tale riguardo, come al momento non esista alcuna regolamentazione internazionale giuridicamente vincolante sull'impiego di tale tecnologia nei conflitti armati o, ancor più nel dettaglio, nei mezzi e metodi di guerra. L'unica parziale eccezione, non avendo valore vincolante, la si ritrova nella *Political Declaration on Responsible Military use of Artificial Intelligence and Autonomy (*d'ora in avanti "la *Declaration*"*)*[38]. Dapprima proposta al Summit *Responsible AI in the Military Domain*, tenutosi all'Aja nel febbraio 2023, oggi la *Declaration* è stata adottata da più di 50 Stati con lo scopo di creare una rete di principi comuni su cui basare lo sviluppo e l'impiego dell'IA nei contesti

[35] A. Nadibaidze - I. Bode - Q. Zang, *AI in Military Decision Support Systems: a Review of Developments and Debates*, Centre for War Studies, 2024, 16

[36] Si pensi, ad esempio, all'impiego di armi chimiche o batteriologiche e lo sviluppo di mezzi cibernetici. Per un approfondimento v. I. Bode - H. Huelss, *Autonomous Weapons Systems and International Norms*, Londra, Chicago, 2022, 60 ss.

[37] Dichiarazione sulla rinuncia all'uso, in tempo di guerra, di proiettili esplosivi di peso inferiore a 400 grammi (S. Pietroburgo, 29 novembre-11 dicembre 1868)

[38] U.S. Department of State, *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, in *state.gov*, 9 novembre 2023

di conflitto armato. Va, inoltre, sottolineato che recentemente le Nazioni Unite si sono interessate più direttamente alla questione specifica delle armi autonome, nonché della militarizzazione dell'intelligenza artificiale, come testimoniato dal rapporto del Segretario generale *Lethal Autonomous Weapons Systems* del 1° luglio 2024 e dalla risoluzione dell'Assemblea Generale *Artificial intelligence in the Military Domain and its Implications for International Peace and Security*, adottata il 24 dicembre 2024[39]. Cionondimeno, non trattandosi anche in questi casi di strumenti giuridicamente vincolanti, è necessario indagare le norme che specificatamente possono applicarsi al caso dell'impiego dell'IA nei conflitti armati.

La convenzione di riferimento in tal senso è il Primo protocollo addizionale alle Convenzioni di Ginevra del 12 agosto 1949, adottato nel 1977, e concernente la regolamentazione del DIU applicabile nei conflitti armati internazionali[40]. Sebbene l'ambito di applicazione del Protocollo sia limitato ai soli conflitti armati internazionali[41], è bene sottolineare che i principi qui descritti sono considerati di natura consuetudinaria e, in quanto tali, applicabili anche nei conflitti armati non internazionali[42]. Prima di procedere, si rende necessaria una precisazione in merito all'applicabilità di tali principi alle nuove tecnologie, mezzi e metodi di guerra. È generalmente accettato che le norme inerenti alla regolamentazione dei mezzi e metodi di guerra, siano esse di natura pattizia o consuetudinaria, continuino ad applicarsi anche nel caso di nuovi mezzi e metodi[43]. Ciò deriva dal principio espresso all'art. 35(1) del Primo protocollo, e considerato di natura con-

---

[39] Assemblea generale delle Nazioni Unite, *Seventy-ninth session, Item 98 (ss) of the preliminary list* General and complete disarmament: lethal autonomous weapons systems*, *Lethal autonomous weapons systems, Report of the Secretary-General*, A/79/88, 1 luglio 2024; Risoluzione dell'Assemblea generale delle Nazioni Unite*, Artificial intelligence in the military domain and its implications for international peace and security*, A/RES/79/239 approvata con una maggioranza di 159 Stati, tra cui l'Italia, e 2 voti contrari, e 5 astenuti.

[40] Protocollo addizionale alle Convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime dei conflitti armati internazionali, United Nations Treaty Series 1125- 3, 1977

[41] L'art. 1(3) e (4) del Protocollo, infatti, dispone che:
«3. Il presente Protocollo, che completa le Convenzioni di Ginevra del 12 agosto 1949 per la protezione delle vittime della guerra, si applicherà nelle situazioni previste nell'art. 2 comune a dette Convenzioni
4. Le situazioni indicate nel paragrafo precedente comprendono i conflitti armati nei quali i popoli lottano contro la dominazione coloniale e l'occupazione straniera e contro i regimi razzisti, nell'esercizio del diritto dei popoli di disporre di sé stessi, consacrato nella Carta delle Nazioni Unite e nella Dichiarazione relativa ai principi di diritto internazionale concernenti le relazioni amichevoli e la cooperazione fra gli Stati in conformità della Carta delle Nazioni»

[42] Si veda, come riferimento, J-M. Henackaerts - L. Doswald-Beck, *Customary International Humanitarian Law Volume I: Rules*, Comitato Internazionale della Croce Rossa, Cambridge, 2009, Regole dalla 1 alla 10 (principio di distinzione); regola 14 (principio di proporzionalità); regole dalla 15 alla 24 (principio di precauzione); Tribunale penale internazionale per l'ex Jugoslavia, *The Prosecutor v. Tadić*, Appeals Chamber, Jurisdiction, 1995, para 110-128

[43] A. Cassese, *Means of Warfare: the traditional and the new law,* in *Journal of Criminal International Justice*, 21-5, 2023, 1159; S. Haines, *Weapons, Means and Methods of Warfare*, in S. Wilmshurst - S. Breau (eds.), *Perspectives on the ICRC Study on Customary International Humanitarian Law*, Cambridge, 2007, 260

suetudinaria, in base al quale le parti in conflitto non godono di un diritto illimitato nella scelta dei mezzi e metodi di guerra[44]. Come si analizzerà nel paragrafo 4, secondo l'interpretazione più restrittiva della c.d. Clausola Martens[45], inoltre, tutto ciò che non è esplicitamente proibito da norme specifiche del DIU deve comunque sottostare ai dettami dei principi di umanità, del diritto consuetudinario e della coscienza pubblica[46]. Necessariamente, dunque, anche nell'impiego di nuove tecnologie che, come l'IA, non sono soggette ad esplicita regolamentazione, vigerà l'obbligo di rispettare le norme del DIU[47].

Nel caso delle armi autonome, ciò è stato reso esplicito nel primo degli undici principi sviluppati dal *Group of Governamental Experts of the High Contracting Parties related to emerging technologies in the area of lethal autonomous weapons system*[48], in base al quale:

«International humanitarian law continues to apply fully to all weapons systems, including the potential development and use of lethal autonomous weapons systems»[49]

Per quanto ciò sia esplicitamente riferito al caso specifico delle armi auto-

---

[44] Sulla natura consuetudinaria del principio v. CIG, Parere consultivo dell'8 luglio 1996, *Legality of the Threat or Use of Nuclear Weapons*, 78

[45] *Infra* nota 107

[46] A. Cassese, *The Martens Clause: Half a Loaf or Simply Pie in the Sky?,* in *European Journal of International Law*, 11-1, 2000, 189-190 ; T. Meron, *The Humanization of Humanitarian Law*, in *The American Journal of International Law*, 94-2, 2000, 87; M. Salter, *Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause*, in *Journal of Conflict and Security Law* , 17-3, 2012, 408 ss.; I. Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I,* Leiden, 2009, 40; M. N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, in *Virginia Journal of International Law*, 50-4, 2010, 400

[47] Sul ruolo della Clausola Martens in tal senso v.: CIG, Parere consultivo dell'8 luglio 1996, *Legality of the Threat or Use of Nuclear Weapons*, cit., 86

[48] Gruppo di esperti stabilito in seno alla Convenzione su talune armi convenzionali durante la quinta conferenza di revisione della convenzione, tenutasi a Ginevra tra il 12 e il 16 dicembre 2016. V., CCW/CONF.V/10, d'ora in avanti GGE

[49] GGE, *Annex III Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System*, CCW/MSP/2019/9, 2019. Da notare che tale interpretazione e supportata dalla maggioranza degli Stati e della dottrina. Ad esempio, v. CCW, *Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Submitted by the Chairperson of the Informal Meeting of Experts*, 2016; GGE, *Areas of Convergence on LAWS, Submitted by Brazil,* CCW/GGE.2/2018/WP.5, 28 agosto 2018; CCW, *Final Document of the Sixth Review Conference Part I*, CCW/CONF.VI/11, 10 gennaio 2022; GGE, *Existing International Humanitarian Law applicable to Lethal Autonomous Weapon Systems*, CCW/GGE.1/2024/CRP.3, 27 maggio 2024
Sul punto *inter alia*, v. T. Chengeta, *Measuring Autonomous Weapon Systems against international humanitarian law rules*, in *Journal of Law and Cyber Warfare,* 5-1(c), 2016; B. Kastan, *Autonomous Weapon Systems: a Coming Legal Singularity?*, in *Journal of Law, Technology and Policy*, 45, 2013; A. Szpak, *Legality of Use and Challenges of New Technologies in Warfare – the Use of Autonomous Weapons in Contemporary or Future Wars*, in *European Review*, 28-1, 2020; M. Brenneke, *Lethal Autonomous Weapon Systems and their Compatibility with International Humanitarian Law: a Primer to the debate*, in T. D. Gill et al. (eds.), *Yearbook of International Humanitarian law*, l'Aja, 2018; M. Sassóli, *Autonomous Weapons and International Humanitarian law: Advantages, open technical questions and legal issues to be clarified*, in *International Law Studies,* 90, 2014

nome, la continuità dell'applicazione del DIU anche al caso dell'impiego dei DSS quali parte dei mezzi e metodi di guerra è stata sovente ribadita[50]. Ne consegue che, per quanto il diritto applicabile al processo del *targeting* non abbia subito cambiamenti a livello convenzionale dal 1977, i principi che verranno descritti nelle pagine seguenti rimangono applicabili anche alle nuove tecnologie e, nel caso di specie, a IA, DSS e armi autonome[51].

Il principio di distinzione

Nella pianificazione ed esecuzione di un attacco, il primo passo da compiere riguarda l'identificazione dei potenziali obiettivi militari, ovvero degli individui e gli oggetti che possono essere legittimamente oggetto di attacco[52]. È a tal fine che le parti in conflitto saranno chiamate a rispettare il c.d. principio di distinzione, ossia l'imperativo di distinguere in ogni momento tra civili e beni civili[53] da un lato, e combattenti ed obiettivi militare dall'altro, laddove solo gli ultimi possono essere attaccati. Tale principio, disciplinato per la prima volta agli articoli 48 e 51(2) del Primo protocollo addizionale, è stato definito dalla Corte internazionale di giustizia (CIG) come un «*cardinal principle*»[54] del DIU, nonché nel Commentario del 1987 al Primo protocollo come la base su cui si fondano i principi e le regole del DIU[55].

L'impiego dell'IA in armi autonome e DSS può coadiuvare (o sostituire) l'essere umano nell'effettuare le valutazioni imposte dal suddetto principio. Ciò, inevitabilmente, fa emergere problemi inediti. Le armi autonome, come visto, sono in grado di identificare autonomamente potenziali obiettivi militari; gli algoritmi di IA, conseguentemente, devono essere addestrati in modo tale da distinguere correttamente tra civili/beni civili e combattenti/obiettivi militari. Diversi dubbi sono emersi in merito all'effettiva capacità di queste armi e dell'IA in generale di effettuare questa

---

[50] A. Backstrom - I. Henderson, *New Capabilities in Warfare: an Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36*, cit., 490 ss.; T. McFarland, *Factors shaping the legal implications of increasingly autonomous military system,* in *International Review of the Red Cross*, 97-900, 1315; W. Boothby, *Some legal challenges posed by remote attack*, in *International Review of the Red Cross*, 94-886, 2012, 585; W. Boothby, *AI Warfare and the Law,* cit., 138. Sul punto v.; D. Amoroso, *Sistemi di supporto alle decisioni basati sull'IA e crimini di guerra: alcune riflessioni alla luce di una recente inchiesta giornalistica,* in *Diritti umani e diritto internazionale*, 2, 2024; D. Mauri*, Numeri, persone, umanità. Sistemi di Supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, in *Diritti umani e diritto internazionale*, 2, 2024

[51] W. Boothby, *Does the Law of Targeting Meet Twenty-First-Century Needs?*, in C. Harvey - J. Summers - N. D. White (eds.), *Contemporary Challenges to the Laws of War: Essays in Honour of Professor Peter Rowe*, Cambridge, 2014, 232

[52] Per una definizione di obiettivo militare, v. Articolo 52 Primo protocollo addizionale

[53] Per "civili" si intendono tutti coloro che non possono essere considerati come combattenti, mentre per "popolazione civile", si intende l'insieme di civili. V., Articolo 50 Primo protocollo addizionale

[54] CIG, Parere consultivo dell'8 luglio 1996, *Legality of the Threat or Use of Nuclear Weapons*, cit., 78

[55] C. Pilloud – J. De Preux- Y. Sandoz et al., *Commentary on the Additional Protocols to the Geneva Conventions of 8 June 1977 to the Geneva Conventions of 12 August 1949*, cit., para. 1683, 598

distinzione[56]. Ciò è ancora più evidente nel caso di obiettivi militari considerati tali non per natura, ma per scopo, ubicazione, o uso[57]. Una valutazione di questo tipo è inevitabilmente contestuale e da effettuarsi caso per caso. In tal senso, la dubbia capacità delle armi autonome di raggiungere un tale livello di consapevolezza situazionale ha destato non poche preoccupazioni[58]. Considerazioni simili possono farsi in merito alla corretta identificazione di combattenti/civili, nei casi in cui questi ultimi partecipino direttamente alle ostilità o, ancora, nel caso di attacco a beni duali, per i quali è necessaria una comprensione delle intenzioni e dei comportamenti degli individui che, al momento, sembra essere impossibile per un'IA [59]. Altre considerazioni devono farsi in merito a quelli che sono i limiti tipici dell'IA in sé, di cui si è accennato sopra. Ad esempio, un'IA addestrata su dati poco rappresentativi o viziati genererà un *output* che riflette tali elementi. Dati viziati, infatti, inevitabilmente influenzeranno gli *output* del sistema compromettendo l'effettiva capacità di distinguere e classificare correttamente individui ed oggetti[60]. Anche qualora addestrata su dati del tutto adeguati, l'IA può ugualmente commettere degli errori in base ad una percentuale nota, c.d. margine di errore. Anche in tali situazioni, vi è il rischio di compromettere l'*output*, creando un possibile effetto a cascata[61]. Questi rischi sono intrinsechi anche dei DSS, come è diventato evidente dall'impiego di tali sistemi nel conflitto israelo-palestinese. Sebbene i DSS, come osservato, si limitino a fornire dei suggerimenti all'operatore umano, nel caso del conflitto israelo-palestinese è risultato evidente come la

[56] Ad esempio, v., W. Boothby, *AI Warfare and the Law*, cit., spec. 151 e 159; D. Amoroso, *Autonomous Weapons Systems and International Law. A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains,* Napoli, 2020, 60-75; S. Gutan, *"Terminator Factor"- AI Targeting Decision-Making and the Law*, in *International Conference Knowledge-based Organization*, XXX- 2, 2024, 4; A. Roberts - A. Venables*, The Role of Artificial Intelligence in Kinetic Targeting from the Perspective of International Humanitarian Law,* in *13th International Conference on Cyber Conflict*, 2021, 49

[57] Art. 52 Primo protocollo addizionale

[58] D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit., 144. Per un approfondimento v. T. Chengeta, *Measuring Autonomous Weapon Systems against International Humanitarian Law Rules,* cit.; A. Blanchard - M. Taddeo, *Predictability, Distinction & Due Care in the use of Autonomous Weapon Systems*, 3 maggio 2022

[59] D. Amoroso, *Autonomous Weapons Systems and International Law,* cit., 47-56; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit., 146 ss. Per un approfondimento su partecipazione diretta alle ostilità e beni duali v.: M. Nelser, *Interpretive Guidance on the Notion of Direct Partecipation in Hostilities under International Humanitarian Law*, Comitato Internazionale della Croce Rossa*,* 2009; G. D. Solis, *The Law of Armed Conflicts- International Humanitarian Law in War,* Seconda edizione, Cambridge, 2016, 521-522

[60] I. Bode - I. Bhila, *The problem of algorithmic bias in AI-based military decision support systems*, in *blogs.icrc.org*, 3 settembre 2024; A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, cit., 32; Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach*, cit., 476; A. Roberts - A. Venables, *The Role of Artificial Intelligence in Kinetic Targeting from the Perspective of International Humanitarian Law*, cit., 52

[61] Comitato Internazionale della Croce Rossa, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts Building a culture of compliance for IHL to protect humanity in today's and future conflicts*, in *icrc.org*, 2024, 56

presenza di dati viziati, di un margine di errore non mitigato da particolari accorgimenti e, soprattutto, di un'eccessiva fiducia nel sistema da parte degli operatori umani (c.d. *autonomation bias),* hanno portato ad ingenti ripercussioni sul rispetto del principio di distinzione e, conseguentemente, sui civili[62].

Il principio di proporzionalità

Numerose difficoltà, per alcuni insormontabili, emergono anche in relazione al rispetto del principio di proporzionalità[63]. Tale principio, disciplinato agli articoli 51(5)(b) e 57(2)(b) del Primo protocollo addizionale, pone, per le parti in conflitto, l'obbligo di non effettuare attacchi in cui, pur verso obiettivi legittimi, il danno collaterale atteso sia eccessivo rispetto al vantaggio militare diretto e concreto previsto. Ne consegue che, nel condurre tale valutazione, le parti in conflitto sono chiamate a bilanciare due fattori di natura differente (c.d. calcolo di proporzionalità): il danno collaterale e il vantaggio militare. Data l'evidente difficoltà di comparare elementi così diversi tra loro, Yoram Dinstein ha rimarcato che tale bilanciamento corrisponde a una comparazione tra «*apples and oranges*»[64]. Ciò implica, inoltre, valutare e decidere basandosi su elementi che, al momento, non sono tramutabili in termini unicamente matematici, imponendo anche delle valutazioni di tipo "soggettivo"[65]. Concretamente, vi sono tre fasi che compongono il suddetto calcolo[66]: 1) stima del danno collaterale che si prevede derivare da un attacco specifico; 2) valutazione del vantaggio militare che deriverà dall'attacco; 3) bilanciamento tra il danno collaterale atteso e il vantaggio militare diretto e concreto, di modo che il primo non risulti "eccessivo"[67]. Se l'impiego dell'IA nella prima fase è molto diffuso,

---

[62] V.: A. Civitella, *Intelligenza artificiale e diritto internazionale umanitario: l'uso di Lavender nel conflitto Israelo-palestinese*, in *sidiblog.org*, 3 giungo 2024; D. Amoroso, *Sistemi di supporto alle decisioni basati sull'IA e crimini di guerra: alcune riflessioni alla luce di una recente inchiesta giornalistica,* cit.; *D. Mauri, Numeri, persone, umanità. Sistemi di Supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, cit.; M. Sisson, *Multistakeholder Perspectives on the Potential Benefits, Risks, and Governance Options for Military Applications of Artificial Intelligence*, in *Report the Militarization of Artificial Intelligence*, 2019, 4; E. M. Forrest - B. Boudreaux - A. J. Lohn - M. Ashby - C. Curriden - K. Klima - D. Grossman, *Military Applications of Artificial Intelligence. Ethical Concerns in an Uncertain World,* cit., 10

[63] A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, cit., 46-48

[64] Y. Dinstein, *Distinction and Loss of Civil Protection in International Armed Conflicts*, in *International Law Studies*, 84, 2008, 186

[65] Per una disamina sul principio di proporzionalità v. Y. Dinstein, *The principle of proportionality,* in K. Mujezinovic Larsen - C. Guldahl Cooper - G. Nystuen (eds.), *Searching for a Principle of Humanity in International Humanitarian Law*, Cambridge, 2012, 72-85; N. Melzer, *Diritto Internazionale Umanitario un'ampia introduzione,* Comitato Internazionale della Croce Rossa, 2023, 116-117; Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflicts*, Cambridge, 2022, 172-188

[66] D. Amoroso, *Autonomous Weapons Systems and International Law,* cit., 77-86; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit.,150

[67] Il Commentario al Primo protocollo addizionale del 1987 fa riferimento all'esistenza di una "sproporzione" tra il vantaggio militare e il danno collaterale previsto. V., C. Pilloud- J. De Preux- Y. Sandoz et al., *Commentary on the Additional Protocols to the Geneva*

specialmente tramite l'impiego di appositi DSS, e non suscita particolari preoccupazioni[68], lo stesso non può dirsi per il suo impiego nella seconda e, ancora di più, nella terza fase. Sono due gli elementi che risultano critici in tal senso: la definizione di vantaggio militare ed il concetto di eccessività. Nel caso del primo, infatti, diverse interpretazioni sono state date di che cosa costituisca un vantaggio militare "concreto e diretto" e, nel caso di specie, è dubbio se un algoritmo di IA possa effettuare un tale tipo di interpretazione altamente contestuale[69]. Ancor più critico risulta essere il concetto di "eccessività"[70]. Ci si chiede, infatti, come sia (e se sarà mai) possibile per un'IA effettuare un bilanciamento tra due fattori intrinsecamente diversi, cosicché uno non risulti eccessivo rispetto all'altro[71]. Non si esige, infatti, di valutare il danno collaterale in ordine di superiorità numerica, ma in modo tale che non sia sproporzionato. Si configura, dunque, una valutazione che include anche elementi di natura non squisitamente oggettiva ed altamente contestuali che non possono, al momento, essere effettuati da un calcolo algoritmico[72]. Non a caso, infatti, lo standard di riferimento che viene posto è quello del *reasonable commander*, il comandante responsabile, ossia un individuo che possiede l'addestramento, l'esperienza e la comprensione necessari per prendere tale tipo di decisioni[73]. Dubbi permangono, segnatamente, in merito all'effettivo rispetto del principio di proporzionalità nella sua interezza nell'impiego di IA, qualora utilizzata senza l'intervento e le valutazioni di un essere umano.

Il principio di precauzione

Considerazioni di natura simile possono essere fatte in merito al rispetto del principio di precauzione. Questo principio, disciplinato all'art. 57 del

Conventions of 8 June 1977 to the Geneva Conventions of 12 August 1949, cit., para 1979, 626

[68] A. Michel Holland, *Decisions, Decisions, Decisions: Computation and Artificial Intelligence in Military Decision Making*, cit., 33; P. Margulies, *The Other Side of Autonomous Weapons: Using Artificial Intelligence to Enhance IHL Compliance*, in R. T. P. Alcala - E. Talbot Jensen (eds.) *The Impact of Emerging Technologies on the Law of Armed Conflict*, New York, 2018, 147-174

[69] Per un approfondimento su tale concetto v. K. Watkin, *Assessing Proportionality: Moral Complexity and Legal Rules*, in *The Conduct of Hostilities in International Humanitarian Law Volume I*, Londra, 2012, 96 ss.

[70] Per un approfondimento v. International Law Commission, *Final report: The Conduct of Hostilities and International humanitarian law*, Presented at the 77th ILA conference in Johannesburg, South Africa, 2017, 34-35

[71] Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflicts,* cit., 179-181

[72] D. Amoroso, *Autonomous Weapons Systems and International Law,* cit., 91; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit.,151-152

[73] Lo standard del *reasonable commander* non è presente nel testo degli articoli 51(5)(b), 57 (2)(a)(iii) o 57(2)(b), ma è stato utilizzato come riferimento per la per la prima volta nel *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia* del 2000 (Ufficio del procuratore, Tribunale penale internazionale per l'ex Jugoslavia), per poi essere ripreso in *Prosecutor v. Galić*, Judgment and Opinion, 2003, para 58; nella giurisprudenza di alcune corti interne; nonché, successivamente, da autorevoli fonti. Sul punto, v. I. Henderson - K. Reece, *Proportionality under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects*, in *Vanderbilt Journal of Transnational Law*, 51-3, 2018, 835-855

Primo protocollo addizionale, pone in capo alle parti in conflitto una serie di obblighi puntuali da effettuarsi al fine di verificare che il principio di distinzione e di proporzionalità siano effettivamente rispettati[74]. In altri termini, il principio di precauzione abbia il merito di trasformare gli obblighi negativi, espressi nei principi di distinzione e proporzionalità, in obblighi positivi di *due diligence*[75]. Ne consegue che sono applicabili al principio di precauzione le considerazioni espresse sopra in merito ai principi di distinzione e proporzionalità. Per quanto il mantenimento del controllo umano nell'impiego delle armi autonome sia sovente ritenuto un elemento necessario al fine di rispettare il suddetto principio[76], si sostiene in questa sede che la presenza dell'operatore umano nell'uso di armi autonome o DSS non equivale necessariamente ad una garanzia del rispetto degli obblighi previsti dal principio di precauzione. L'insorgenza di *bias* cognitivi, invero, ossia di tendenze di comportamento da parte degli operatori umani derivanti dall'interazione con i sistemi autonomi, può compromettere il mantenimento di un controllo umano efficiente[77]. La prassi nell'uso di DSS è prova di tale evenienza[78]. La restrizione del tempo di reazione derivante dall'impiego dell'IA assume, anche in questo caso, particolare rilevanza. Come è stato osservato[79], l'utilizzo di questi sistemi e la conse-

---

[74] Oltre all'obbligo di verificare che gli obiettivi identificati siano legittimi e che nella pianificazione ed esecuzione degli attacchi si usino mezzi e metodi di guerra che minimizzino i danni collaterali che, in ogni caso, non devono essere eccessivi rispetto al vantaggio militare anticipato, le parti in conflitto sono chiamate a sospendere un attacco qualora non rispetti i suddetti obblighi e, se possibile, ad avvisare la popolazione civile di attacchi che potrebbero metterla in pericolo (Art. 57(2)(a)(b)(c) Primo protocollo addizionale)

[75] D. Amoroso, *Autonomous Weapons Systems and International Law,* cit., 99; M. Longobardo, *Due Diligence in International Humanitarian Law*, in H. Krieger - A. Peters - L. Kreuzer (eds.), *Due Diligence in the International Legal Order*, Oxford, 2020, 187 ss.

[76] Ivi, 109 ss. Ciò si manifesterebbe, ad esempio, in merito all'obbligo espresso all'art. 57(2)(b), vale a dire l'obbligo precauzionale di sospendere un attacco qualora si preveda essere in contrasto con le norme sopra descritte: v. M. Sassóli*, Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified*, cit., 337. Vi sono, però, opinioni contrarie, in quanto anche nel caso nell'impiego di armi o munizioni non autonome non sempre è possibile per un militare abortire l'attacco; in tali casi, tuttavia, nessuna obiezione è stata sollevata in relazione agli obblighi *ex* art. 57(2)(b). V., T. McFarland, *Autonomous Weapon Systems and the Law of Armed Conflict. Compatibility with International Humanitarian Law*, cit., 118

[77] Per un approfondimento, v.: A. Nadibaidze- I. Bode - Q. Zang, *AI in Military Decision Support Systems: a Review of Developments and Debates*, cit., 30 ss. Si omette qui volontariamente il termine "meaningful" riferito al controllo umano al fine di evitare fraintendimenti relativi a questo concetto. Per un approfondimento v., M. C. Horowitz - P. Scharre, *Meaningful Human Control in Weapon Systems: A Primer*, Centre for New American Security, Working Paper, in cnas.org, marzo 2015

[78] Sul punto v. D. Mauri, *Numeri, persone, umanità. Sistemi di supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, cit.; T. Mimran - G. Dahan, *Artificial Intelligence in the Battlefield: A Perspective from Israel,* in *opiniojuris.org*, 20 aprile 2024; D. Amoroso, *Sistemi di supporto alle decisioni basati sull'IA e crimini di guerra: alcune riflessioni alla luce di una recente inchiesta giornalistica*, cit.

[79] D. Mauri, *Numeri, persone, umanità. Sistemi di supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, cit.; T. Mimran - G. Dahan, *Artificial Intelligence in the Battlefield: A Perspective from Israel,* cit.; M. Bo - J. Dorsey, *Symposium on Military AI and*

guente impossibilità per gli operatori umani di verificare adeguatamente le informazioni ricevute[80] impedisce l'esercizio nel momento di pianificazione e conduzione di un attacco della c.d. *constant care*, ossia l'obbligo di fare ciò che è possibile al fine di salvaguardare beni e persone civili e, in ultima istanza, di rispettare il suddetto principio[81].

Infine, vi sono due ulteriori elementi che possono inficiare il rispetto dei principi sopra descritti: la generale imprevedibilità[82] dell'IA, e la possibilità che questa "inganni" l'operatore umano (c.d. *Deceptive AI*). In merito al primo elemento, è generalmente impossibile prevedere in ogni circostanza quali comportamenti verranno adottati dall'IA, specialmente durante l'interazione del sistema con il contesto in cui essa viene impiegata. Ne consegue l'impossibilità di prevedere gli *output* prodotti e, dunque, di stabilire *ex ante* qualora le decisioni o le informazioni fornite dal sistema siano conformi al DIU[83]. Ciò si ricollega al fenomeno della c.d. *black box*[84], per cui ricostruire a ritroso i passaggi che sono stati effettuati dal sistema per arrivare ad un determinato *output* risulta pressoché impraticabile[85]. In merito al secondo aspetto, è stato osservato come i sistemi più innovativi dotati di IA abbiano imparato nelle fasi di addestramento ad "ingannare" l'essere umano che interagisce con esso. Essi, infatti, imparano ad usare tecniche quali manipolazioni, imbrogli e adulazione, al fine di raggiungere lo scopo

the Law of Armed Conflict: The 'Need' for Speed – The Cost of Unregulated AI Decision-Support Systems to Civilians, in *opiniojuris.org,* 4 aprile 2024

[80] Ad esempio v., Comitato Internazionale della Croce Rossa, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a culture of compliance for IHL to protect humanity in today's and future conflicts,* 30 settembre 2024, 55-57; W. Boothby, *AI Warfare and the Law*, cit., spec. 155 e 181

[81] L'art. 57 del Primo protocollo addizionale, nella sua versione in lingua inglese, enuncia: «*In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects*». In base al Commentario del 1987, questo paragrafo completa il principio di distinzione come espresso all'art. 48 del Protocollo, fornendo la base teorica su cui vengono poi costruiti gli obblighi sulle applicazioni pratiche del suddetto principio nei paragrafi successivi dell'art. 57. V., C. Pilloud- J. De Preux- Y. Sandoz et al., *Commentary on the Additional Protocols to the Geneva Conventions of 8 June 1977 to the Geneva Conventions of 12 August 1949*, cit., para. 1863, 598

[82] Per imprevedibilità (*unpredictability*) si intende l'incapacità di un sistema di eseguire un compito con la stessa prestazione ottenuta nella fase di addestramento, o, nel caso del *machine learning,* con il *dataset* su cui è stato addestrato. V., A. Michel Holland, *The Black Box, Unlocked*, UNIDIR, Ginevra, 2020, 5

[83] S. Gutan, *"Terminator Factor"- AI Targeting Decision-Making and the Law, International Conference Knowledge-based Organization*, cit., 5; A. Blanchard - M. Taddeo, *Predictability, Distinction & Due Care in the use of Autonomous Weapon Systems*, cit., 6-11

[84] Questo termine indica «*a system for which we know the inputs and outputs but can't see the process by which it turns the former into the latter*». V., A. Michel Holland, *The Black Box, Unlocked*, cit., III

[85] Comitato Internazionale della Croce Rossa, *Artificial intelligence and machine learning in armed conflicts: A human-centred approach*, cit., 476; N. Hitoshi, *Artificial Intelligence and the obligation to respect and ensure respect for IHL*, in E. Massingham - A. McConnachie (eds.) *Ensuring Respect for International Humanitarian Law*, New York, 2021, 134; A. Roberts - A. Venables, *The Role of Artificial Intelligence in Kinetic Targeting from the Perspective of International Humanitarian Law*, cit., 52-53

che gli era stato prefissato[86]. Ciò è risultato evidente in casi di IA addestrata per sfidare altri partecipanti in diverse tipologie di giochi, e quando addestrata tramite *reinforced learning* basato su riscontri forniti da operatori umani[87]. Sebbene ciò non venga fatto partendo da intenzioni malevole, come potrebbe fare un essere umano, ma semplicemente al fine di raggiungere lo scopo dato, l'impiego di sistemi in grado di operare in tale modo compromette quella che è l'affidabilità[88] del sistema e degli *output*, specialmente qualora impiegati in applicazioni militari.[89]

4. Tra etica e diritto: Clausola Martens e principio di umanità

Giunti al punto, è opportuno indagare come l'ampliamento delle capacità autonome nei sistemi d'arma e nei DSS conferito dall'impiego di IA si rapporta con un altro principio fondamentale, sebbene più evasivo nei contenuti, del DIU: il principio di umanità. Questo principio è considerato alla base del *corpus* del DIU, tanto che esso viene descritto come il frutto del delicato bilanciamento tra tale principio e quello di necessità militare.[90] È proprio in considerazione di questa veste che il principio di umanità è sovente invocato al fine di proibire lo sviluppo di sistemi con capacità autonome nelle decisioni inerenti all'impiego della forza armata[91]. Due sono le principali questioni che meritano di essere sollevate al riguardo: da un lato la privazione dell'essere umano del potere decisionale sull'uso della forza letale verso un altro essere umano; dall'altro la de-umanizzazione derivante dalla considerazione degli individui come meri numeri e dati forniti ad algoritmi. Nel dibattito sulle armi autonome, più risalente nel tempo[92], ciò è risultato particolarmente evidente. Sin dai suoi albori, tale dibattito ha visto nell'autonomia di queste armi un contrasto coi principi di umanità e di dignità umana degli individui in ragione della

[86] W. Boothby, *AI Warfare and the Law*, cit., 46

[87] P.S. Park - S. Goldstein - A. O'Gara - M. Chen - D. Hendrycks, *AI Deception: A Survey of Examples, Risks, and Potential Solutions*, in *Patterns*, 5-5, 2024, 2 ss.

[88] Per affidabilità (*reliability*) del sistema si intende il grado in base al quale il sistema fallisce nel compito affidatogli. V., A. Michel Holland, *The Black Box, Unlocked*, cit., 5

[89] W. Boothby, *AI Warfare and the Law*, cit., 46

[90] Da notare che gli argomenti inerenti al principio di umanità si sovrappongono a quelli riguardanti il principio di dignità umana inerente al diritto internazionale dei diritti umani. V., D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit., 107 ss. Tale qualifica del DIU è riscontrabile nel Preambolo della Dichiarazione sulla rinuncia all'uso, in tempo di guerra, di proiettili esplosivi di peso inferiore di 400 grammi, San Pietroburgo, 29 novembre-11 dicembre 1868

[91] Inter alia, v. C. Heyns, *Autonomous Weapons in Armed Conflict and the Right to a Dignified Life: An African Perspective*, in *South African Journal on Human Rights,* 33-1, 2017, 46-71

[92] Nel 2003 venne pubblicato il Report del US Joint Force Command, *Unmanned Effects (UFX): Taking the Human Out of the Loop*, in cui per la prima volta si parlò della necessità dello sviluppo di sistemi autonomi; il vero e proprio dibattito internazionale, tuttavia, si originò a partire dal 2010, con la pubblicazione di alcuni documenti come, tra cui: Human Rights Watch, *Losing Humanity. The Case against Killer Robots,* in *hrw.org*, 2012 e la US Department of Defense, *DoD directive 3000.09 on autonomy in weapon systems*, 2012

"de-umanizzazione" dell'individuo oggetto di un attacco, sia esso civile o combattente[93]. Come espresso dal Comitato internazionale della Croce Rossa, infatti, l'uso di armi autonome «*raises fundamental ethical concerns for humanity, in effect substituting human decisions about life and death with sensor, software and machine processes*»[94]. Affidare l'uso della forza armata letale ad una macchina, si argomenta inoltre, renderebbe impossibile per la persona oggetto di attacco "appellarsi all'umanità" dell'altro e, ancora, priverebbe della speranza di invocare la compassione di un altro essere umano[95]. A differenza delle armi autonome, l'attenzione sulla conformità dei DSS al principio di umanità ha solo da poco suscitato l'interesse di alcuni autori[96]. Ciò, a parere di chi scrive, è dovuto a due motivazioni principali. In primo luogo, i DSS sono diventati solo recentemente oggetto dell'attenzione di accademici, Stati e società civile. In secondo luogo, come già descritto, i DSS non "decidono" l'impiego della forza, la quale rimane nelle mani del decisore umano. Questa caratteristica, tuttavia, sostiene Diego Mauri, non implica che dubbi non possano ugualmente sollevarsi in relazione al rispetto dei principi di dignità umana e di umanità nell'impiego di tali sistemi. Secondo l'autore, il principio di umanità potrebbe evolversi ad assumere significati nuovi, in risposta al rischio di considerare gli individui, e specialmente le persone protette, come meri numeri, e privandoli, quindi, di un "trattamento umano"[97]. È stato osservato altrove che, come nel caso delle armi autonome, anche i DSS potrebbero essere impiegati per lo svolgimento di compiti e per coadiuvare nel prendere decisioni che normalmente coinvolgono anche considerazioni di tipo etico, facendo emergere anche in questa eventualità possibili ripercussioni sul principio di dignità umana di combattenti e civili, ridotti a meri dati[98]. A parere di chi scrive, esiste un ulteriore aspetto che merita di essere evidenziato in merito alla relazione tra DSS e principio di umanità, ossia la restrizione del potere

---

93 N. Davinson, *A legal perspective: Autonomous weapon systems under international humanitarian law,* UNODA Occasional papers 30, 2018, 9; D. Amoroso, *Jus in bello and jus ad bellum arguments against autonomy in weapons systems: A re-appraisal*, in *Questions of International Law*, 43, 2017, 23 ; P. Asaro, *Jus Nascendi, Robotic Weapons and the Martens Clause,* in R. Calo - M. A. Froomkin - I. Kerr (eds.) *Robot Law* ,Cheltenham - Northampton, 2016, 367. Tra gli altri, v. D. Mauri, *Numeri, persone, umanità. Sistemi di supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, cit., 338; P. Asaro, *On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making,* in *International Review of the Red Cross*, 2012, 699-700

94 Comitato Internazionale della Croce Rossa, *ICRC Position on Autonomous Weapon Systems*, in *icrc.org*, 12 maggio 2021

95 Tra gli altri v. T. Chengeta, *Measuring Autonomous Weapon Systems against International Humanitarian Law Rules*, cit., 132 ss.

96 Eccezioni sono, ad esempio: D. Mauri, *Numeri, persone, umanità. Sistemi di supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, cit.; N. C. Renic - E. Schwarz, *Inhuman-in-the-loop: AI-targeting and the Erosion of Moral Restraint*, in *opiniojuris.org,* 19 dicembre 2023; M., Klaus, *Transcending weapon systems: the ethical challenges of AI in military decision support systems*, in *blogs.icrc.org*, 24 settembre 2024

97 D. Mauri, *Numeri, persone, umanità. Sistemi di supporto alle decisioni umane in campo militare da parte dell'IDF e diritto internazionale umanitario*, cit., 340 ss.

98 M., Klaus, *Transcending weapon systems: the ethical challenges of AI in military decision support systems,* cit.

decisionale dell'essere umano nel loro impiego. Prendendo a riferimento tali considerazioni e le riflessioni effettuate nelle pagine precedenti, si può ipotizzare infatti che, data la crescente velocità e complessità dei compiti svolti dai DSS, potrebbe crearsi un contrasto col principio di umanità qualora emergesse nella prassi una concreta limitazione del potere decisionale dell'operatore umano.

Per quanto l'importanza di questo principio sia innegabile, la sua natura ed il suo contenuto effettivo rimangono dubbi. La prima formulazione scritta del principio di umanità si ritrova all'interno di quella che è oggi conosciuta come Clausola Martens[99]. Tale Clausola, che prende il nome dal suo proponente[100], venne inserita per la prima volta nel preambolo della II Convenzione dell'Aja del 1899 e poi riproposta in modo quasi del tutto identico nel preambolo della IV Convenzione dell'Aja del 1907[101], nelle Convenzioni di Ginevra del 1949[102], nel Primo protocollo addizionale[103] e, da ultimo, nella Convenzione su certe armi convenzionali del 1980[104]. Essa stabilisce che:

«[…] nei casi non compresi nelle disposizioni regolamentari da esse adottate, le popolazioni e i belligeranti rimangono sotto la tutela e sotto l'impero dei principi del diritto delle genti, quali risultano dagli usi stabiliti dalle nazioni civili, dalle leggi dell'umanità e dalle esigenze della pubblica coscienza»[105]

A una prima lettura, è facile comprendere le motivazioni che hanno reso la Clausola celebre: pur in assenza di regolamentazione specifica, non vi è un *vacuum* normativo, in quanto le parti in conflitto dovranno comunque sottostare al rispetto del diritto consuetudinario, del principio di umanità e dei dettami della coscienza pubblica. In altri termini, non è necessariamente legittimo ciò che non è esplicitamente proibito[106]. Come visto, ciò

[99] D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit.,162

[100] Fyodor Fyodorovich Martens (1845-1909), giurista e diplomatico dell'Impero della Russia zarista, delegato presso la Conferenza Diplomatica dell'Aja, 1899

[101] IV Convenzione dell'Aja concernente le leggi e gli usi della guerra terrestre e regolamento annesso, adottata il 18 ottobre 1907 ed entrata in vigore il 26 gennaio 1910, 205 CTS 277

[102] I Convenzione di Ginevra del 12 Agosto 1949 per migliorare la sorte dei feriti e dei malati delle forze armate in campagna, UN Treaty Series 75-31, art. 63; II Convenzione di Ginevra del 12 Agosto 1949 per migliorare la sorte dei feriti, dei malati e dei naufraghi delle forze armate in mare, UN Treaty Series 75-85, art. 62; III Convenzione di Ginevra del 12 Agosto 1949 relativa al trattamento dei prigionieri di guerra, UN Treaty Series 75-135, art. 142; IV Convenzione di Ginevra del 12 Agosto 1949 relativa alla protezione delle persone civili in tempo di guerra, UN Treaty Series 75-287, art. 158

[103] Articolo 1 Primo protocollo addizionale

[104] Convenzione sul divieto o la limitazione dell'impiego di talune armi convenzionali che possono essere ritenute capaci di causare effetti traumatici eccessivi o di colpire in modo indiscriminato, 1980, UN Treaty Series 1342-137, preambolo, 5

[105] Preambolo alla IV Convenzione relativa alle leggi e agli usi della guerra terrestre, 1907

[106] T. Meron, *The Martens Clause, Principles of Humanity and Dictates of Public Conscience*, in *American Journal of International Law*, 94-1, 2000, 87. In tal senso, si sostiene che la Clausola

riguarda anche l'impiego di nuove tecnologie nei conflitti armati, le quali non sono ancora oggetto di disciplina specifica, come nel caso dell'IA[107]. Sebbene le sia riconosciuto il merito di aver, per la prima volta, approcciato il principio di umanità non solo quale principio morale ma anche giuridico, permangono dubbi in merito al valore giuridico della Clausola Martens e, conseguentemente, del principio di umanità[108]. Più nel dettaglio, Antonio Cassese identifica tre possibili interpretazioni[109]. Secondo la prima, essa opererebbe solo a livello interpretativo delle norme del DIU[110]. La seconda interpretazione, invece, conferisce un ruolo più decisivo alla Clausola Martens in relazione alle fonti del DIU, dando origine al principio di umanità quale fonte autonoma di tale regime[111]. Infine, secondo la terza interpretazione, pur non assurgendo a fonte autonoma, la Clausola avrebbe il merito di esprimere nozioni che sono all'origine del DIU[112]. Semplificando, dunque, ad un estremo il principio di umanità viene ritenuto un principio generale del diritto internazionale, e, perciò, fonte autonome del diritto capace di regolare situazioni che non sono direttamente disciplinate da norme pattizie o consuetudinarie[113]. All'altro estremo, esso si configura

si opponga al noto principio espresso dalla Corte Permanente di Giustizia Internazionale nel caso S.S. Lotus (1927), in base al quale ciò che non è vietato dal diritto internazionale allora è permesso: sul punto v. D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit., 164

[107] Il valore della Clausola Martens nel far fronte alle nuove tecnologie è stato sottolineato anche dalla Corte Internazionale di Giustizia nel Parere della Corte internazionale di Giustizia sulla liceità della minaccia o dell'uso delle armi nucleari, 8 luglio, 1996, 78

[108] A. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 188; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit.,166. Diverse interpretazioni si ritrovano, infatti, anche nella giurisprudenza interna ed internazionale che si è occupata, anche se in maniera marginale, del principio di umanità, incluse nelle opinioni dissenzienti di giudici. Per una disamina v., A. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 202-208; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit.,167-170; P. Kilibarda - R. Kolb, *The International Court of Justice, international humanitarian law and human rights law*, in R. Kolb - G. Gaggioli - P. Killbarda (eds.), *Research Handbook on Human Rights and Humanitarian Law*, Cheltenham-Northampton, 2022, 170 ss.; T. Meron, *The Martens Clause, Principles of Humanity and Dictates of Public Conscience*, cit., 82-83

[109] V. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 189 ss. V., inoltre: T. D. Evans, *At War with Robots: Autonomous Weapons Systems and the Martens Clause*, in *Hofstra Law Review*, 41-3, 2013, 716 ss.; T. Meron, *The Martens Clause, Principles of Humanity and Dictates of Public Conscience*, cit., 87 ss.

[110] V. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 189-190

[111] All'interno di questa seconda interpretazione ritroviamo la posizione di coloro che considerano il principio di umanità come fonte autonoma del diritto così come "creato" dalla Clausola Martens e di coloro che, invece, considerano che la Clausola Martens abbia un ruolo indiretto nella creazione di fonti del diritto internazionale, facendo assurgere di volta in volta determinati standard a principio di umanità. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 191 e 193

[112] V. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 192

[113] D. Amoroso, *Autonomous Weapon systems and international law. A study on human-machine interactions in ethically and legally sensitive domains*, cit., 178-179; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person. An International Law Analysis*, cit., 167. A support di tale interpretazione, il giudice Shahabbuddeen, nella sua opinion dissenziente, riconosce il valore del principio di umanità quale principio del diritto internazionale

quale principio ispiratore per la formazione delle norme del DIU e per la loro interpretazione[114].

Ciò detto, la domanda da porsi è la seguente: è possibile considerare il principio di umanità come fonte autonoma del DIU avente una propria forza normativa e, segnatamente, in grado di proibire l'impiego di armi autonome e DSS basate su IA?

Richiamando dottrina autorevole[115], è opinione di chi scrive che il principio di umanità non possa essere invocato come fonte autonoma del DIU capace di proibire l'impiego di nuovi mezzi o metodi di guerra. Sebbene sia indiscutibile che il principio di umanità abbia ispirato e sia sotteso ai principi ed alle norme che proibiscono diversi tipi di armamenti, è altrettanto vero che nessun'arma, fino ad oggi, è stata proibita per contrasto al principio in questione[116]. Inoltre, è d'uopo evidenziare come nonostante il fascino delle argomentazioni portate a sostegno della possibile proibizione di sistemi autonomi in base al principio di umanità, nella maggioranza dei casi, tali argomentazioni ricadono più nell'ambito morale che giuridico. In altri termini, il richiamo era al principio di umanità in senso lato, e non alla sua portata giuridica[117].

Se, dunque, l'impiego dell'IA nelle armi autonome e nei DSS non può essere proibito invocando come unica fonte il principio di umanità, il valore di questo principio deve essere riconosciuto, piuttosto, nella sua natura trascendentale che gli permette di influenzare l'interpretazione del diritto esistente e di essere il motore ispiratore di nuove norme. Non a caso, William Boothby sostiene che:

«*the principles of humanity and the 'dictates of the public conscience' appear to have been common and enduring sources of inspiration for the negotiators of the past and will continue to inspire future initiatives*»[118]

Pertanto, riprendendo la concezione del principio di umanità quale strumento per assicurare un "trattamento umano" a coloro coinvolti in un

indipendente dai «*customs*». V., *Dissenting Opinion* del giudice Shahabuddeen in merito al Parere della CIG sulla liceità della minaccia o dell'uso delle armi nucleari. Disponibile a: Dissenting Opinion Judge Shahabuddeen, in *icj-cig.org*, spec. 406 ss.

114 Y. Dinstein, *The Principle of Proportionality*, cit. Sul punto si veda anche: Tribunale penale per l'ex Jugoslavia, *The Prosecutor v. Zoran Kupreškić, Mirjan Kupreškić, Vlatko Kupreškić et al.*, Trial Chamber, Judgement, 2000, para 525

115 V. Cassese, *The Martens Clause: Half of a Loaf or Simply Pie in the Sky?*, cit., 211; D. Amoroso, *Jus in bello and jus ad bellum arguments against autonomy in weapons systems: A reappraisal*, cit., 27; T. Meron, *The Martens Clause, Principles of Humanity and Dictates of Public Conscience*, cit., 88; Y. Dinstein, *The principle of Proportionality*, cit., 73

116 Sull'impossibilità del principio di umanità di proibire lo sviluppo ed impiego di mezzi e metodi di guerra v. M. Hickleton, *Shaky Foundations: Killer Robots and the Martens Clause*, in *Perth International Law Journal,* 4, 2019; T. Meron, *The Martens Clause, Principles of Humanity and Dictates of Public Conscience*, cit. 88

W. Boothby, *The Weapons Law*, Oxford, 2009, 373

117 Ad esempio, v. CICR, Report: Ethics and autonomous weapon systems: An ethical basis for human control?, 3 aprile 2018, in *icrc.org*; N. Davinson, *A legal perspective: Autonomous weapon systems under international humanitarian law*, in *UNODA Occasional Papers*, 30, 2018. Sul punto: D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person- An International Law Analysis,* cit., 171

118 W. Boothby, *The Weapons Law*, Oxford, 2009, 373.

conflitto, siano essi civili o combattenti[119], si vuole insistere sull'enorme portata dei valori racchiusi in questo principio al fine di assicurare un impiego dell'IA che sia il più rispettoso possibile della persona umana.

5. Conclusioni

La trattazione effettuata ha voluto fornire un'introduzione generale su quelle che sono le applicazioni dell'IA nei conflitti armati, delle loro comunanze e differenze, incentrandosi sui rischi che l'impiego di tale tecnologia nelle armi autonome e nei DSS può comportare per il rispetto dei principi di distinzione, precauzione, proporzionalità ed umanità. In guisa di conclusione, si vuole evidenziare che, per quanto armi autonome e DSS siano sovente considerati separatamente, l'impiego in essi dell'IA comporta alcuni elementi comuni ad entrambe le applicazioni. Tra questi, ve ne sono due che emergono in modo particolarmente rilevante dall'analisi effettuata. In primo luogo, l'elemento controverso, seppur centrale, dell'erosione di un controllo (o supervisione) umano effettivo nell'impiego di armi autonome e DSS. In secondo luogo, i limiti intrinseci che caratterizzano l'IA come tecnologia.

La mancanza di controllo da parte dell'essere umano nella selezione degli obiettivi, e, più in generale, nelle fasi critiche del processo del *targeting*, è alla base delle difficoltà inerenti al rispetto dei principi di distinzione, precauzione e proporzionalità. Nel caso delle armi autonome ciò si esplica in modo più diretto, tantoché, come visto, a parere di parte degli Stati e della dottrina, il mantenimento di un controllo umano che sia configurabile almeno come *on-the-loop* diventa necessario per il rispetto dei suddetti principi [120]. Tale necessità si riflette anche nei dibattiti internazionali inerenti alla possibile conclusione di un trattato volto alla regolamentazione di queste armi, nei quali la proibizione le armi autonome che non prevedono, nel loro impiego, una supervisione da parte di un essere umano rimane un elemento centrale[121]. Simili – seppur non identiche – considerazioni possono

---

[119] D. Fleck*, The Handbook of International Humanitarian Law (4th Edition),* Oxford, 2021, 89 ss.; J. Corn, *Humanity, Principle of*, Max Planck Encyclopedias of International Law, 2013

[120] Definizione fornita per la prima volta nel rapporto *Losing Humanity: the case against killer robots* redatto dall'organizzazione non governativa Human Rights Watch, dove viene effettuata una distinzione tra armi autonome dove l'essere umano è *in-the-loop*, *on-the-loop* e *out-of-the-loop*. Con il primo termine, ci si riferisce a quei sistemi autonomi in cui l'essere umano supervisiona ogni singola azione dell'arma, prendendo tutte le decisioni rilevanti in tal senso. Ne consegue che, in tali casi, l'arma autonoma non funzionerà propriamente in maniera autonoma. Con il secondo termine, invece, ci si riferisce a quei casi in cui l'essere umano, per quanto presente, si limita ad un ruolo di generale supervisione sull'operato dell'arma, intervenendo solo laddove necessario al fine di evitare errori da parte di quest'ultima. Infine, con il terzo termine ci si riferisce a quelle armi in cui l'essere umano svolge una funzione puramente inziale attivando l'arma, senza che poi gli sia concessa la possibilità di intervenire. Solo nel secondo e nel terzo caso descritti, dunque, il sistema d'arma potrà dirsi come propriamente autonomo. Si veda: HRW, *Losing Humanity. The Case against Killer Robots*, cit.

[121] Si veda a tal proposito: GGE, *Chair's summary – First 2025 session of the GGE on LAWS,* 7 aprile 2025, CCW/GGE.1/2025/WP.1

essere fatte in merito all'impiego dei DSS. Per quanto la decisione ultima in merito all'impiego della forza armata rimanga nelle mani di un essere umano, l'impiego di Lavender e The Gospel nel conflitto israelo-palestinese ha reso del tutto evidente come ciò sia condizione necessaria, ma non sufficiente al rispetto del DIU. A tale riguardo, la tematica del controllo umano si unisce a quella delle caratteristiche tipiche dell'IA che possono comportare ad una restrizione della supervisione umana (ad esempio, tramite l'*autonomation bias*) o ad errori e risultati imprevedibili. Ne consegue, dunque, che nell'impiego dei DSS la presenza di un controllo umano non implichi necessariamente che esso sia tale garantire il rispetto dei principi del DIU[122]. Inevitabilmente, dunque, l'impiego di tale tecnologia dovrà essere affiancata da particolari accorgimenti al fine di evitare che i suddetti elementi compromettano la possibilità per gli operatori umani di rispettare le norme applicabili[123].

Infine, qualche considerazione conclusiva deve essere fatta in merito al ruolo del principio di umanità di fronte all'applicazione dell'intelligenza artificiale nei conflitti armati. Infatti, l'impiego di tecnologie in grado di restringere il ruolo del decisore umano fino ad arrivare a 'sostituirsi' ad esso nelle decisioni inerenti all'impiego diretto della forza armata necessariamente suscita delle riflessioni sulle potenzialità del suddetto principio nel limitare – o addirittura proibire – l'impiego dei sistemi descritti. Se i principi di distinzione, precauzione e proporzionalità guardano alle modalità in cui viene usata la forza armata, indipendentemente da chi la usa, il discorso sull'impiego dell'IA impone un ulteriore cambio di prospettiva, andando a considerare anche "chi" o "che cosa" impiega la forza[124]. Per quanto tale principio, non essendo una norma autonoma del DIU, non potrà portare alla proibizione dell'impiego e dello sviluppo di armi autonome e sistemi di supporto alle decisioni basati su algoritmi di IA, esso potrà in ogni caso influenzare, come è già accaduto, i dibattiti internazionali in merito a questi sistemi. A tal fine, si guarda favorevolmente alla recente tendenza dimostrata dalle Nazioni Unite di attenzionare la militarizzazione dell'intelligenza artificiale, non rilegandola alla sola applicazione nelle armi autonome o in altre applicazioni specifiche[125]. Per quanto in tali strumenti

---

[122] A. Nadibaidze, *Do AI Decision Support Systems 'Support' Humans in Military Decision-Making on the Use of Force?,* in *opiniojuris.org* , 29 novembre 2024; A. Roberts - A. Venables, *The Role of Artificial intelligence in Kinetic Targeting from the Perspective of International Humanitarian law*, cit., 49-51; D. Amoroso, *Sistemi di supporto alle decisioni e crimini di guerra: alcune riflessioni alla luce di una recente inchiesta giornalistica,* cit., 367

[123] Sul punto, si veda l'ipotesi di inserire *self-reflection mechanisms* proposta da C.M. Jonker - L. Cavalcante Siebert - P.K. Murukkanaiah, *Reflective Hybrid Intelligence for meaningful human control in decision-support systems*, in G. Mecacci - D. Amoroso - L. Cavalcante Siebert - D. Abbink - J. van den Hoven - F. Santioni de Sio (eds.), *Research Handbook on Meaningful Human Control of Artificial Intelligence Systems*, Cheltenham-Northampton, 2024, 188 ss.

[124] Ivi,162

[125] Nazioni Unite, *Security Council Debates Use of Artificial Intelligence in Conflicts, Hears Calls for UN Framework to Avoid Fragmented Governance,* SC/15946, 19 dicembre 2024; Risoluzione dell'Assemblea generale delle Nazioni Unite*, Artificial intelligence in the military domain and its implications for international peace and security,* cit. Sul punto v. A. Civitella, *La militarizzazione dell'intelligenza artificiale nel contesto internazionale: alcune riflessioni sulla Risoluzione 79/239 dell'Assemblea generale delle Nazioni Unite*, in *Osservatorio sulla attività delle*

non si chiarisca il ruolo che il principio di umanità assume nell'impiego militare dell'IA, l'analisi qui effettuata ha voluto dimostrare come esso non solo potrà portare ad un'interpretazione delle esistenti norme tali per cui, nel particolare caso dell'IA, le considerazioni di umanità assumano un ruolo centrale, ma potrà anche influenzare la creazione di una disciplina specifica in merito all'impiego dell'IA all'interno dei mezzi e metodi di guerra che sia il più possibile garantista della persona umana in quanto tale.

organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana, Working Paper 1-25, maggio 2025

Abstract

L'impiego dell'intelligenza artificiale all'interno di applicazioni militari è una realtà dei conflitti armati contemporanei. Sebbene siano innegabili i vantaggi che l'impiego di tale tecnologia può comportare in contesti di conflitto armato, allo stesso tempo emergono diversi dubbi di natura etica e giuridica in relazione al suo utilizzo. A fronte di ciò, il presente contributo intende investigare le comuni sfide che tale tecnologia pone per il diritto internazionale umanitario quando impiegata in due applicazioni particolari: sistemi d'arma autonomi e i sistemi di supporto alle decisioni. Più nel dettaglio, si analizzeranno le peculiari difficoltà poste dall'intelligenza artificiale nei suddetti sistemi per il rispetto dei principi di distinzione, proporzionalità e precauzione, per dedicarsi, infine, al ruolo più controverso del principio di umanità nella loro regolamentazione.

The use of artificial intelligence for military applications has become a reality of nowadays armed conflicts. The advantages of the use of artificial intelligence algorithms in these applications are well-known; nevertheless, it raises several ethical, moral and legal questions. Therefore, this work aims at investigating the common challenges posed by the employment of artificial intelligence to the respect of International Humanitarian Law in two specific applications: Autonomous Weapon Systems and Decision Support Systems. More in particular, this investigation will focus on the respect of the principles of distinction, proportionality and precaution in their use and, finally, it will turn to the more controversial role of the principle of humanity in their regulation.

Keywords

intelligenza artificiale – diritto internazionale umanitario – principio di umanità – armi autonome – sistemi di supporto alle decisioni

Altri saggi

La regolazione dei videogiochi: tra opere audiovisive e digitali, cultura e mercato*

Marina Caporale

Sommario

1. Premessa. – 2. Alla ricerca di una definizione giuridica di videogioco. Elementi distintivi di un'opera complessa. – 3. Unione Europea, principi di regolazione del comparto audiovisivo e digitale e videogiochi. Tra prodotto e servizio. – 3.1. Videogiochi, opere audiovisive, prodotti e servizi digitali. Prospettive di regolazione. – 4. Videogiochi e approccio normativo e regolatorio in Italia. - 5. I videogiochi come opera culturale complessa e le geometrie variabili della regolazione.

1. Premessa

Nel quadro di una regolazione sempre più attenta al mercato di servizi e di prodotti audiovisivi e digitali, apparentemente in incognito, si aggira un elefante, un enorme fenomeno di incerta qualificazione giuridica, che tuttavia costituisce, ormai da diversi anni, un mercato sempre a saldo positivo e con numeri crescenti: i videogiochi. Questo particolare tipo di prodotto patisce da tempo una sottovalutazione, in termini di percezione della sua vera dimensione e di regolazione, dovuta in parte alla loro natura incerta, cui non corrisponde una definizione giuridica univoca. Questo ultimo aspetto, tuttavia, non ha costituito un limite ma è forse uno dei presupposti del successo e della loro potente espansione, non solo in termini di significatività economica, ma anche in termini di impatto e di incidenza, come fattore culturale, nella società.

La sottovalutazione ha riguardato anche la natura culturale dei videogiochi stessi, che pure, come tipologia di consumo, rappresentano un elemento che è ormai parte integrante della dieta mediatica, digitale e in senso lato culturale degli italiani e degli europei ma anche a livello globale, in modo trasversale, anche se con lo stesso tipo di discredito, sembra, che ha caratterizzato l'affermazione del cinema prima e del fumetto o dei cartoni animati poi[1].

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

[1] Per un primo inquadramento del fenomeno sia consentito rinviare a M. Caporale, *I videogiochi: evoluzione e possibile regolazione*, in *Rivista il Mulino*, 4, luglio-agosto 2018, 637 ss. Sui videogiochi esistono ormai molti studi e statistiche. Per quanto riguarda in particolare l'Italia

Le caratteristiche dei videogiochi, a fronte dell'evoluzione della società e delle possibilità tecnologiche, di modelli di fruizione, di dinamiche di gioco, ne fanno un prodotto che costituisce sempre di più un elemento determinante nella costruzione culturale degli individui e della società, ormai innegabile, e non è più, da molto tempo, un prodotto destinato solo a bambini e adolescenti[2].

Queste resistenze, unite a una mancata comprensione complessiva del fenomeno, hanno fatto sì che, nella prospettiva del decisore politico e del legislatore, i videogiochi non siano stati a tutt'oggi inclusi in un compiuto assetto regolatorio, tanto più che l'impressionante evoluzione tecnologica cambia con grandissima velocità caratteristiche e possibilità offerte dal mondo videoludico.

Per quanto riguarda il mercato europeo ed italiano occorre inoltre considerare che, sul fronte della domanda, si registrano valori affatto disprezzabili, mentre sul fronte della produzione videoludica la situazione è molto diversa: i soggetti presenti sul mercato europeo hanno numeri in aumento ma contenuti, e, al pari di altri prodotti "culturali", necessiterebbero di misure di sostegno.

---

v. i dati pubblicati annualmente da Italian Interactive Digital Entertainment Association, IIDEA, in iideassociation.com. Per uno sguardo aggiornato e una prospettiva generale IRIS*, Legal challenges and market dynamics in the video games sector,* European Audiovisual Observatory, Strasbourg, 2024; European Commission, Directorate-General for Communications Networks, Content and Technology, *Understanding the value of a European video games society – Final report*, Publications Office of the European Union, 2023. Solo per dare una sintesi dai dati del 2023 emerge che il 75% dei giocatori di videogiochi in Europa sono adulti e l'età media è di 31,4 anni; che il 53% degli europei gioca ai videogiochi; che fa forza lavoro complessiva in Europa è aumentata e sono circa 115.000 i lavoratori in questo comparto, di cui le donne costituiscono più del 24%; che il fatturato è di circa 25 miliardi di euro nei mercati chiave. Il 2024 sembra avere registrato i primi dati, ancora non definitivi, che evidenziano qualche segno di crisi, ritenuta in parte fisiologica dopo l'esplosione del mercato a seguito della pandemia. Il mercato complessivo è sempre in crescita ma con ritmi ridotti e si sono registrati anche molti licenziamenti nell'industria videoludica a livello globale. Per un primo commento L. Saettone, *L'industria dei videogiochi vacilla: licenziamenti di massa e futuro incerto,* in *agendadigitale.eu,* 11 luglio 2024.

[2] La sensibilità degli utenti è talmente matura e accorta, e anche qualificata dalla presenza di portatori di interesse sempre più rilevanti - ben lungi da quella che potrebbe essere espressione di una platea di soli minorenni - da avere portato alla registrazione di una iniziativa dei cittadini europei dal titolo "*Stop Destroying Videogames*", presentata alla Commissione europea , richiesta registrata nell'ambito del diritto di rivolgersi direttamente alla Commissione sottoponendole una richiesta in cui la si invita a presentare una proposta di un atto legislativo dell'Unione (regolamento (UE) 2019/788 del Parlamento europeo e del Consiglio del 17 aprile 2019, riguardante l'iniziativa dei cittadini europei, ex art. 24 TFUE). Scopo dell'iniziativa è di "imporre agli editori di lasciare in uno stato funzionale (giocabile) i videogiochi che vendono o concedono in licenza (o le collegate funzionalità e risorse che vendono per i videogiochi che trattano) ai consumatori dell'Unione europea. Nello specifico l'iniziativa mira a impedire che gli editori possano disattivare da remoto i videogiochi prima che siano forniti mezzi ragionevoli per mantenerli in funzione" senza coinvolgere gli stessi editori. Per l'avanzamento dell'iniziativa e lo stato di avanzamento della raccolta delle firme necessarie (in cui spicca il contributo dei sottoscrittori italiani) Decisione di esecuzione (UE) 2024/1824 della Commissione, del 19 giugno 2024, relativa alla richiesta di registrazione dell'iniziativa dei cittadini europei dal titolo Stop Destroying Videogames (Mettiamo fine alla distruzione dei videogiochi) a norma del regolamento (UE) 2019/788 del Parlamento europeo e del Consiglio [notificata con il numero C(2024) 3860].

Accedere a una idea di videogiochi come prodotto culturale sembra peraltro la scelta di fondo portata avanti anche dal legislatore nazionale, nel momento in cui ha previsto le prime misure economiche a sostegno del comparto in attuazione della legge sul cinema e sull'audiovisivo (l. 220/2016)[3]. È peraltro una prospettiva che sembra si stia affermando anche nell'Unione europea, che negli ultimi anni ha contribuito a disciplinare alcuni aspetti delle produzioni videoludiche.

I videogiochi, come anticipato, sono stati considerati per decenni prevalentemente come un tipo di intrattenimento minore, destinato a un pubblico di bambini e adolescenti, per cui la principale preoccupazione è stata quella di prevenire e tutelare questi soggetti da eventuali effetti nocivi di giochi violenti o comunque che avessero contenuti per loro non idonei, nonché da una certa dipendenza intesa come eccessiva, di dedizione prevalentemente esclusiva a questa forma di intrattenimento. La tutela dei minori ha costituito e costituisce, ancora oggi, uno dei tratti caratterizzanti dell'approccio normativo e regolatorio ai videogiochi ma l'ambito delle tutele si amplia se si pensa ai contenuti discriminatori o anche di possibile incitamento all'odio che alcuni videogiochi possono esprimere e che hanno rilievo non solo in una prospettiva di tutela dei minori[4].

Riguarda principalmente i minori anche il timore dell'eventuale aspetto "patologico", collegato al loro uso, che ha avuto anche un riconoscimento dall'Organizzazione Mondiale della Sanità[5], riguarda un numero comunque ristretto di persone rispetto a una platea di videogiocatori sempre più ampia e sempre più aperta a fasce di popolazione che, fino a pochi anni fa, non erano considerate come possibili utenti: donne e adulti, ad esempio. I videogiochi sono disponibili per tutti i supporti (dallo smartphone alle console da tavolo), online e offline, possono essere giocati da soli e in compagnia (sia trovandosi fisicamente insieme che collegandosi online con i propri compagni di gioco), prevedono scambi e interazione onli-

[3] La Commissione europea ha disciplinato il regime dei sostegni economici pubblici a infrastrutture e attività culturali nell'ambito del regolamento di esenzione n. 651/2014, *Regolamento (UE) n. 651/2014 della Commissione, del 17 giugno 2014, che dichiara alcune categorie di aiuti compatibili con il mercato interno in applicazione degli articoli 107 e 108 del Trattato*, stabilendo le condizioni di compatibilità degli aiuti di Stato in questo settore. Secondo quanto previsto nel Considerando 72, testo originario del regolamento, l'elenco di obiettivi e di attività culturali ammissibili non comprende le attività commerciali quali anche i videogiochi. Il punto è evidentemente nodale per l'applicazione di misure di sostegno pubblico, su cu v. C.E. Baldi, *Finanziamento della cultura e regole di concorrenza. Nuove prospettive dal ripensamento della Commissione europea*, in *Aedon*, 3, 2016.

[4] Una iniziativa del Consiglio d'Europa, molto attivo anche oggi sul tema, è, in tempi non sospetti riferita all'adozione delle *Human rights guidelines for online games providers Developed by the Council of Europe in co-operation with the Interactive Software Federation of Europe*, Consiglio d'Europa, 2008.

[5] La proposta dell'OMS che ha inserito nell'ICD (*International Classification of Diseases*), il manuale internazionale di classificazione delle patologie, la dipendenza da videogiochi o *gaming disorder* è in vigore dal 1° gennaio 2022. Più di un osservatore ha espresso riserve sulle forti influenze esercitate da alcuni paesi, che possono avere indotto l'OMS a fare questo passo. Da tale definizione sono esclusi i giochi d'azzardo, la cui dipendenza costituisce un altro tipo di patologia; anche per il legislatore, il sistema del "*gambling*", *online* o *offline*, è sempre stato regolato secondo diversi criteri. Gli effetti patologici dell'uso smodato dei videogiochi sono peraltro solo in parte conseguenza delle strategie di *marketing* dei produttori, evidentemente volte a fidelizzare l'utente in modo anche estremo.

ne che implicano anche contatti con gli altri videogiocatori e conseguenti tutele in ordine alla moderazione dei contenuti scambiati e al trattamento dei dati personali, hanno dinamiche di gioco semplici o estremamente complesse e articolate, sono gratuiti (alcuni solo apparentemente) e facilmente scaricabili e/o condivisibili o piuttosto costosi e prevedono a volte eventuali integrazioni da pagare per l'upgrade e contenuti "speciali", con quelle che sono definite microtransazioni. Il prodotto videoludico è sempre più raffinato, non ha solo finalità puramente ludiche, come ad es. i cosiddetti "serious game" o anche i videogiochi puramente educativi, studiati e utilizzati anche per vari tipi di terapie riabilitative, senza considerare che spesso i modelli videoludici concorrono a metodi e strategie di apprendimento anche in senso più ampio (si pensi anche, in senso lato, alla "gamification", intesa come l'utilizzo di elementi mutuati dal gioco in generale e in particolare dai videogiochi delle tecniche di gaming in contesti diversi, ad es. di formazione aziendale ma anche per reinventare forme d partecipazione alle politiche pubbliche e, più in generale, nella pubblica amministrazione)[6].

I videogiochi quindi posso assumere molte forme, si sono evoluti e, per quanto riguarda le sfide di una regolazione efficace del prodotto in sé, in termini di mercato e tutele degli utenti, occorre considerare un significativo cambiamento che ha portato al passaggio dal "prodotto" al "servizio", attraverso il tendenziale passaggio dal modello "arcade" e "boxed", basato su un prodotto acquistato su supporto materiale e percepito e giocato come proprio, sul proprio dispositivo domestico, a un modello commerciale, ad oggi ampiamente utilizzato, basato sui giochi come servizio, pay-to-win o freemium. Il servizio in questo caso è messo a disposizione attraverso una piattaforma dedicata oppure insieme ad altri servizi (si pensi alle piattaforme che offrono principalmente contenuti audiovisivi ma si sono aperte anche a una offerta di videogiochi online, ai social media, ai principali fornitori di servizi internet) con una serie di considerazioni ulteriori sulla competitività dell'offerta videoludica e gli eventuali filtri all'accesso posti da produttori o dalle piattaforme di distribuzione, nella forma dell'accessibilità gratuita o a pagamento del prodotto videoludico.

Sempre più spesso questo prodotto, inoltre, interagisce con altri, non solo per una strategia di marketing dei produttori ma per una assonanza di mondi, di racconto: si pensi ai videogiochi che traggono ispirazione da film o da opere letterarie ma anche, al contrario, a opere cinematografiche o serie televisive, e iniziative editoriali (libri, fumetti) che nascono da prodotti videoludici.

Assistiamo a un fenomeno che esiste fin dalla fine degli anni '40 del secolo scorso e che si è sempre evoluto, particolarmente negli ultimi decenni, per mezzi e modalità di espressione. Le attuali generazioni hanno usufruito dei videogiochi molto più a lungo delle precedenti, facendoli entrare nel tessuto culturale della società più di quanto si sia disposti ad ammettere e spesso molto più di qualunque gioco reale, opera letteraria, film, fumetto, cartone animato o serie televisiva lo siano stati per le generazioni precedenti. Lo

[6] V. in particolare G. Sgueo, *Ludocrazia. Quando il gioco accorcia le distanze tra governo e cittadini*, Milano, 2018, e dello stesso A. "*Gamification*", in P. Harris - A. Bitonti - C.S. Fleisher (eds.), *The Palgrave Encyclopedia of Interest Groups, Lobbying and Public Affairs,* Berlino, 2020.

stesso videogioco continua ad essere fruito dal proprio utente per lungo tempo, anche per anni. Le tecniche di coinvolgimento usate nei confronti dei videogiocatori sono sempre più raffinate, e sarebbe da approfondire quanto possano essere legittimamente pervasive, soprattutto in termini di tutela dei dati personali, e/o di condizionamento del comportamento dei videogiocatori, nel breve, nel medio e nel lungo periodo. È chiaro a tutti che qualunque attività ludica, coltivata in modo ossessivo, reca una serie di danni eppure, d'altra parte, può accentuare alcune capacità e così è anche per le attività videoludiche. Viceversa occorre considerare che i videogiocatori possono diventare dei professionisti del videogioco e l'attività videoludica è, in alcuni paesi ma non ancora in Italia, considerata un'attività sportiva in senso proprio, secondo la definizione dei cosiddetti e-sports[7].
Questo complesso di elementi ha permesso al regolatore di svolgere riflessioni differenti rispetto al passato e di accostare progressivamente la regolazione dei videogiochi alla regolazione di prodotti e servizi audiovisivi e digitali, accentuando la valorizzazione dell'elemento creativo e culturale.
L'obiettivo di questo contributo è quindi di verificare l'utilità e l'orizzonte di una possibile definizione giuridica univoca o quanto più completa dei videogiochi, considerandone la natura di prodotto culturale ed espressione di creatività.

2. Alla ricerca di una definizione giuridica di videogioco. Elementi distintivi di un'opera complessa

L'inquadramento normativo dei videogiochi, come anticipato, patisce ancora oggi, nel diritto dell'Unione europea e in Italia, ma anche in altri paesi europei, un problema di definizione e di qualificazione giuridica, da cui derivano implicazioni e conseguenze sulla regolazione di un prodotto e/o di un servizio che cambia costantemente[8].
Storicamente, fino ad oggi, ha prevalso una prospettiva giuridicamente incentrata sulla tutela del videogioco nella complessità e unitarietà del-

[7] Si fa riferimento al fenomeno degli *e-sports*, su cui non ci soffermeremo in questa sede, che si presta ad essere un ulteriore tassello da collocare nella ricostruzione complessiva di un fenomeno ad oggi privo si una regolazione positiva autonoma. S Ceretta - D. Filosa - L. Mazzei - N. Serao - L. Viola (a cura di) *Esport: profili normativi e contrattuali*, Milano, 2022; L. Zambelli, A. Strinati, *Analisi sistemica del fenomeno eSport. I videogames come sport e la necessità di una governance*, in *federalismi.it*, 14, 2021; P. Raimondo, *Sport vs esports. Una difficile convivenza*, in *federalismi.it*, 1, 2022.

[8] L'analisi comparata restituisce un quadro ancora frammentario per i Paesi europei, che hanno seguito lo stesso percorso, grosso modo, che si cercherà di evidenziare con riferimento alla normativa italiana. Le caratteristiche essenziali della normativa, in chiave comparata, sono evidenziate nel rapporto A. Ramos - L. López - Mr. Anxo Rodríguez - T. Meng - S. Abrams, *The Legal Status of Video Games: Comparative Analysis in National Approaches*, World Intellectual Property Organization, WIPO, 2013. Esistono anche studi successive, che raccolgono le disposizioni vigenti in vari paesi, a cura di associazioni di categoria o di studi legali specializzati che restituiscono questa frammentarietà ancora oggi, tra tutela dei diritti d'autore, tutela dei minori e legittimazione di forme di sostegno economico.

le sue componenti, quali opere dell'ingegno in sé, ma anche sulla tutela dell'apporto fornito dagli autori delle sue singole componenti. In particolare, la Corte di Giustizia dell'UE è stata chiamata ad esprimersi su aspetti di tutela del diritto d'autore connessi all'elaborazione del software e del supporto fisico, che nei primi decenni della affermazione dei videogiochi, era necessariamente fisso (il computer, la console di gioco), in linea con la tecnologia del tempo. Nel quadro normativo dell'UE i videogiochi sono dunque protetti, in prima istanza, dalla direttiva 2009/24/CE relativa alla tutela giuridica dei programmi per elaboratore e dalla direttiva 2001/29/CE relativa all'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.

In una sentenza che costituisce un approdo fondamentale e una sintesi del percorso svolto dalla giurisprudenza europea, parallelamente alla evoluzione dei prodotti videoludici, la Corte di Giustizia dell'Unione europea afferma che «i videogiochi […] costituiscono un materiale complesso, che comprende non solo un programma per elaboratore, ma anche elementi grafici e sonori che, sebbene codificati nel linguaggio informatico, possiedono un valore creativo proprio che non può essere ridotto alla suddetta codificazione»[9].

Pur ampliando la prospettiva e integrando elementi diversi, l'elemento essenziale e distintivo dei videogiochi è la presenza del software e sul software si è concentrata la normativa e anche la giurisprudenza italiana, che, in una prima fase, era tesa a individuare la possibilità di richiamare, per similitudini e differenze, il regime applicabile alle opere cinematografiche[10]. È stato ritenuto infatti che le opere cinematografiche condividono con i videogiochi la presenza di immagini in movimento e suoni, in una prospettiva utile per accordare le tutele proprie del diritto d'autore all'opera videoludica qualora presenti un livello minimo ma sufficiente di creatività, secondo quanto disposto, a quel tempo, dalla Legge sul diritto d'autore, l. 633/1941 (L.D.A.). Questo tipo di riflessioni della giurisprudenza del tempo si accompagnano a valutazioni del tutto critiche del prodotto videoludico («aggeggi creati per sollevare dalla noia gente sfaccendata») e valorizzano la dimensione "audiovisiva" del videogioco (immagini in movimento, animazioni, suoni…) anche in ragione della mancata inclusione, a quel tempo, del software come oggetto di tutela nella normativa allora vigente sul diritto d'autore[11].

L'assimilabilità alle opere audiovisive è un elemento che, come vedremo, ritorna nel diritto nazionale e anche dell'UE, e che si affianca alla tutela del software che, nel trascorrere del tempo e nelle successive interpretazioni della giurisprudenza, è diventato prima un elemento necessario e, poi, non più sufficiente a dare un compiuto riconoscimento giuridico ai videogiochi, come evidenziato già dalla giurisprudenza europea citata.

---

[9] CGUE, C-355/12, *Nintendo e a. c. PC Box srl e a.* (2014).

[10] Trib. Torino, sez. I civ., 17 ottobre 1983, *ATARI inc. e soc. Fratelli Bartolino e soci c. SIDAM*, in *Giurisprudenza Piemontese*; Trib. Milano, 20 giugno 1988, *Soc. Gruppo ed. Jackson c. Soc. Sipe*, in *Il Diritto dell'informazione e dell'informatica*, 1988, 878 ss.; Cass. pen., sez. III, 6 maggio 1999, n. 1716, in *Rivista penale*, 1999, 653. In senso conforme Cass. pen., sez. III, 26 marzo 1999, n. 1204, in *Diritto d'autore*., 1999, 489.

[11] A. Cataldi, *L'inquadramento giuridico del videogioco*, in *Il Diritto d'Autore*, 2016, 322 ss.

A seguito dell'adozione della direttiva 91/250/CE (codificata in seguito nella direttiva 2009/24/CE), in Italia è stato introdotto solo nei primi anni '90[12] il secondo comma dell'art. 1 della L.D.A., che stabilisce la protezione dei programmi per elaboratore (ossia del software) «come opere letterarie ai sensi della Convenzione di Berna sulla tutela delle opere letterarie e artistiche». Il software entra così nel perimetro della legge sul diritto d'autore e costituisce anche l'aspetto su cui si concentra certa successiva giurisprudenza interna, volta a verificare la portata dell'applicazione delle cosiddette misure tecnologiche di protezione che, ex art. 102-quater L.D.A., i titolari di diritti d'autore e di diritti connessi possono apporre sulle opere e sui materiali protetti[13].

Attraverso la giurisprudenza sulle misure di protezione, emerge una definizione dei videogiochi come «qualcosa di diverso e di più articolato rispetto ai programmi per elaboratore comunemente in commercio, così come non sono riconducibili per intero al concetto di supporto contenente "sequenze d'immagini in movimento". Essi, infatti, si "appoggiano" ad un programma per elaboratore, che parzialmente comprendono, ma ciò avviene al solo fine di dare corso alla componente principale e dotata di propria autonoma concettuale, che è rappresentata da sequenze di immagini e suoni che, pur in presenza di molteplici opzioni a disposizione dell'utente (secondo una interattività, peraltro, mai del tutto libere perché "guidata" e predefinita dagli autori), compongono una storia ed un percorso ideati e incanalati dagli autori del gioco. Ma anche qualora lo sviluppo di una storia possa assumere direzioni guidate dall'utente, è indubitabile che tale sviluppo si avvalga della base narrativa e tecnologica voluta da coloro che hanno ideato e sviluppato il gioco, così come nessuno dubita che costituiscano opera d'ingegno riconducibili ai loro autori i racconti a soluzione plurima o "aperti" che caratterizzano alcuni libri. In altri termini, i videogiochi impiegano un software e non possono essere confusi con esso».[14]

Nella giurisprudenza interna si è perso, in questa fase, l'intento di creare di un parallelismo con le opere cinematografiche, e quindi torna recessivo l'elemento della narrazione per immagini - anche se non sono frutto di riprese audiovisive - rispetto a quello di elaborazione di un software, di cui sono comunque parte integrante scelte narrative, di regia e di strategia, di musiche ed effetti sonori ed altri elementi analoghi a quelli usati per le opere audiovisive. Questo approdo della giurisprudenza italiana appare già non più sufficiente ad esaurire le plurime dimensioni del videogioco, in potente espansione espressiva resa possibile dalla tecnologia, dal software ma che, appunto, non si esauriscono in questo[15].

---

[12] Tramite il decreto di attuazione d. lgs. n. 528 del 29 dicembre 1992.

[13] Le misure tecnologiche di protezione hanno lo scopo di impedire o limitare atti non autorizzati. Su cui in particolare Cass. pen., sez. III, 1° agosto 2017, n. 38204.

[14] Cass. pen., sez. III, 25 maggio 2007, n. 33768, ripresa anche da giurisprudenza successiva.

[15] Analogamente in Francia, in cui il videogioco è stato definito dalla giurisprudenza come un'opera composta da due elementi costitutivi: il software e gli "aspetti audiovisivi, grafici e sonori". Court d'Apelle, Parigi, sez. XII, 26 settembre 2011, *Sarl Aakro Pure Tronic e a. c. Nintendo. Mission parlementaire sur le regime juridique du jeu video en droit d'auteur,*

Questo possibile accostamento ma anche disallineamento tra videogiochi e tutela del software ma anche tra videogiochi ed opere audiovisive si riflette in particolare nel diritto dell'UE e nazionale, in un momento caratterizzato anche da numerosi interventi normativi su contenuti, servizi e mercati digitali e implementati dai possibili sconfinati scenari che l'uso dell'intelligenza artificiale prospetta anche in questi ambiti, e di cui, peraltro, proprio i videogiochi costituiscono un degli ambiti principali di sperimentazione e sviluppo e quindi sono un ambito che favorisce l'affermazione dell'IA, anche in chiave economica. [16]
Nel diritto italiano più recente emerge l'accostamento dei videogiochi alle opere audiovisive per cui sarà utile cogliere i tratti essenziali che potrebbero supportare questa scelta, che consente anche di riflettere sul riconoscimento del valore culturale dei videogiochi.

3. Unione europea, principi di regolazione del comparto audiovisivo e digitale e videogiochi. Tra prodotto e servizio

L'intervento dell'Unione europea nel settore audiovisivo, in particolare dei prodotti audiovisivi, si misura, storicamente, con la loro dimensione culturale, la loro capacità di fare circolare idee e valori e di valorizzare le identità dei popoli dei paesi europei e dell'Europa nel suo insieme, per favorire l'integrazione europea[17].
Come noto l'intervento dell'UE nel comparto dei "media" può essere dedotta da vari articoli del Trattato sul Funzionamento dell'UE, anche alla luce della natura complessa dei beni e dei servizi relativi al comparto, che non sono esclusivamente beni culturali e nemmeno esclusivamente beni economici. La base giuridica è quindi ricondotta a vari articoli del TFUE in materia di libera circolazione delle merci, delle persone, dei servizi e dei capitali, di politica in materia di concorrenza, di armonizzazione tecnologica e ravvicinamento, ma anche, e ai nostri fini, soprattutto, cultura, industria e politica commerciale comune.
Più che ad altri principi e competenze contenuti nei Trattati (libera circolazione dei servizi, concorrenza, armonizzazione tecnologica e, diversamente il pluralismo da intendersi in questa sede sia come pluralismo informativo e in particolare dei media, ma anche, e forse prevalentemente, come pluralismo culturale), qui viene in considerazione l'art. 167 TFUE[18] per individuare il fondamento e il ruolo dell'Unione in questo ambito e la

*Rapport de M. Patrice Martin-Lalande,*30 mai - 30 novembre 2011.

[16] J. Togelius, *Artificial Intelligence and Games*, Berlino, 2018; sull'impatto del Regolamento (UE) 2024/1689, *infra*, §. 3.1.

[17] Per sintesi, in questa sede, rispetto alla vastità del tema, si rinvia all'interessante ricostruzione di S. Cicerchia, *Europa: dalla cultura alla creatività e ritorno. Proposte e dilemmi politici*, in *Economia della Cultura*, 3, 2013, 297 ss.

[18] Art. 167 TFUE (*ex* art. 151 del TCE), par. 1: «L'Unione contribuisce al pieno sviluppo delle culture degli Stati membri nel rispetto delle loro diversità nazionali e regionali, evidenziando nel contempo il retaggio culturale comune».

sua eventuale estensione anche all'ambito videoludico[19].
In questa prospettiva si comprende che l'approccio al settore audiovisivo della Comunità Europea prima e dell'Unione poi, rispetto alle opere audiovisive, sia di tipo protezionistico e di promozione dell'industria audiovisiva europea[20], per tutelare e promuovere il valore culturale e identitario di cui è portatrice e per sostenere un comparto da sempre schiacciato dallo straripante predominio, storicamente, dell'industria audiovisiva statunitense. Nell'impostazione dell'Unione si afferma per prima la dimensione e il rilievo culturale, ma nel corso degli anni la dimensione industriale ed economica incrementano costantemente la loro rilevanza, anche in relazione all'esigenza di realizzare un Mercato unico digitale in cui il settore audiovisivo gioca un ruolo essenziale[21].
La prima versione della Direttiva "Televisione senza frontiere"[22] considerava, oltre ai servizi, anche trasmissioni, programmi, e, genericamente, le opere europee. Per queste c'era stato un tentativo di introdurre forme obbligatorie di tutela della produzione audiovisiva europea e l'obbligo per le emittenti europee di riservare una parte della loro programmazione ad opere prodotte in Europa, ma tali vincoli non furono poi inseriti, in modo esplicito e con soglie pre-fissate e trasversali, da applicare a tutte le emittenti, nel testo definitivo della direttiva[23]. Nel sistema dei media di quel

[19] In questa prospettiva e competenze possono essere espresse con azioni di incentivazioni e raccomandazioni, come specificato dallo stesso art. 167, trattandosi di competenze cosiddette di sostegno, che cioè completano e integrano le competenze esistenti a livello nazionale e sub-nazionale. A. Contaldo - B. Marchesano, *Le politiche europee nel settore audiovisivo e cinematografico*, in *MC*, *Diritto ed economia dei mezzi di comunicazione*, 1, 2015-2016, 25 ss.

[20] G. Rossi, *Produzione audiovisiva e indipendente*, in F. Bassan - E. Tosi (a cura di), *Il diritto degli audiovisivi*, Milano, 2012, 273 ss.

[21] Comunicazione della Commissione «Strategia per il mercato unico digitale in Europa» del 6 maggio 2015, COM(2015) 192 final.

[22] Direttiva 89/552/CEE del Consiglio, del 3 ottobre 1989, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati Membri concernenti l'esercizio delle attività televisive.

[23] R. Mastroianni, *La Direttiva sui servizi di media audiovisivi e la sua attuazione nell'ordinamento italiano*, Torino, 2012, 62-63. Al riguardo si consideri il testo degli artt. 4 e 5 della direttiva 89/552/CEE poi ripreso negli artt. 16 e 17 della direttiva 2010/13/UE che fa riferimento a obblighi differenziati: A) tutte le emittenti devono riservare ad opere europee, in generale, la *maggior parte del loro tempo di trasmissione*, per tale intendendosi almeno il 50%, escluso il tempo assegnato a notiziari, manifestazioni sportive, giochi, pubblicità, servizi di teletext e televendite", secondo "criteri appropriati" che tutte le emittenti devono autonomamente individuare per raggiungere gradualmente questa proporzione; qualora non possa essere raggiunta la proporzione citata, la proporzione effettiva non deve comunque essere inferiore a quella constatata in media nel 1988 nello Stato membro di interesse. B) Con riferimento alle emittenti e ai produttori di opere europee *indipendenti dalle emittenti stesse* le direttive proseguono affermando, con il medesimo testo, che gli Stati membri, ogni qualvolta sia possibile e ricorrendo ai mezzi appropriati, provvedono a che le emittenti riservino alle opere di tali produttori il 10 % almeno del loro tempo di trasmissione — escluso il tempo assegnato a notiziari, manifestazioni sportive, giochi, pubblicità, servizi di teletext e televendite — oppure, a scelta dello Stato membro, il 10 % almeno del loro bilancio destinato alla programmazione. assegnando una quota adeguata ad opere recenti, vale a dire quelle diffuse entro un termine di cinque anni dalla loro produzione (art. 17, direttiva 2010/13/UE). Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate

periodo radiotelevisione e cinema viaggiavano su binari che si cercava di tenere separati, in modo che la prima non erodesse pubblico ed entrate del secondo ma, piuttosto costituisse un'ulteriore possibilità di sfruttamento delle opere cinematografiche, concepite per essere destinate e fruite, in prima battuta, nelle sale cinematografiche.

Un cambio di passo si registra con il "Libro verde sulla convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione e sulle sue implicazioni normative e dalla successiva Comunicazione della Commissione CEE sulla politica audiovisiva nell'era digitale"[24]. In questa Comunicazione la Commissione europea parla ancora di "materiale audiovisivo"[25] e di "servizi audiovisivi". Il cinema è posto in una posizione apparentemente distinta, ancora agganciato, nella prospettiva comunitaria, alla collocazione in cui le tradizionali tecniche di produzione e diffusione lo avevano sempre posto. D'altra parte sono i primi anni in cui si comincia a delineare l'impatto della digitalizzazione dei contenuti e delle nuove possibilità per la loro fruizione. In questo documento la CE rileva anzi che lo sviluppo dei nuovi servizi - come pay-TV, pay-per-view, Near-Video-on-Demand (NVOD) - non incide in modo negativo sui mezzi già esistenti, come il cinema e il mercato dei video (allora su cassetta o in formato DVD) e ipotizza un possibile rapporto di complementarietà tra diversi servizi.

Successivamente un'altra Comunicazione della Commissione europea[26] si riferisce alle opere cinematografiche e alle "altre opere audiovisive", configurando queste ultime come un'unica categoria, non definita in sé, di cui si sottolinea la duplice natura: «Sono beni economici che offrono notevoli opportunità per creare ricchezza e occupazione […] Sono anche beni culturali che, al tempo stesso, rispecchiano e modellano la nostra società»[27].

L'Unione interviene più incisivamente sui servizi televisivi, soffermandosi sulla promozione delle opere europee attraverso le modifiche alla Direttiva "TV senza frontiere" avvenute nel 1997 e nel 2007[28]. La direttiva 2007/65/

disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (Direttiva sui servizi di media audiovisivi), in *GUUE* L 95 del 15 aprile 2010.

[24] Comunicazione della Commissione al Consiglio, al Parlamento Europeo, al Comitato Economico e Sociale e al Comitato delle Regioni. Principi e Orientamenti per la Politica Audiovisiva della Comunità nell'Era Digitale, COM(1999) 657 definitivo.

[25] Traduzione ufficiale in italiano, piuttosto infelice, di "*audiovisual content*", nel testo in inglese della Comunicazione.

[26] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni su taluni aspetti giuridici riguardanti le opere cinematografiche e le altre opere audiovisive, COM/2001/534 def., in GUCE C 43 del 16 febbraio 2002.

[27] Così testualmente la Comunicazione citata. La Convenzione è vincolante per gli stati firmatari e prevede l'obbligo legale del deposito di qualsiasi materiale di "immagini in movimento" prodotto o co-prodotto e reso disponibile al pubblico in ogni Stato firmatario.

[28] Direttiva 97/36/CE del Parlamento Europeo e del Consiglio del 30 giugno 1997 che modifica la direttiva 89/552/CEE del Consiglio relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti l'esercizio delle attività televisive, in GUCE L 202 del 30 luglio 1997; Direttiva 2007/65/

CE, che modificava l'impianto della Direttiva TV senza frontiere in modo sostanziale, come noto è stata approvata e poi abrogata e sostituita dalla direttiva 2010/13/UE ("Direttiva SMAV"). In questa sede sono definiti i programmi quali «una serie di immagini animate, sonore o non, che costituiscono un singolo elemento nell'ambito di un palinsesto o di un catalogo stabilito da un fornitore di servizi di media la cui forma e il cui contenuto sono comparabili alla forma e al contenuto della radiodiffusione televisiva. Sono programmi, ad esempio, i lungometraggi, le manifestazioni sportive, le commedie di situazione (*sitcom*), i documentari, i programmi per bambini e le *fiction* originali» (art. 1, c. 1, lett. *b*). In questa definizione compaiono sicuramente quelle che possono essere comprese tra le opere audiovisive che però in sé, come categoria, non sono esplicitamente definite dalla direttiva.

La Direttiva SMAV riconosce, in particolare, un sostegno alle produzioni europee attraverso un sistema di quote di programmazione a queste destinate, vincolanti per le emittenti europee. Non sono esplicitate soglie o percentuali, ma la loro fissazione è sostanzialmente rinviata agli Stati membri (art. 16, c. 1) [29].

Da questa previsione si desume che il tipo di prodotti citati è escluso dal novero delle opere europee tutelate, ma quali siano le "opere" da sostenere attraverso le quote non viene esplicitamente stabilito. Le definizioni contenute nella direttiva si soffermano esclusivamente sulla loro natura "europea", idonea ad includerle nel sistema delle quote, o meno (art. 1, c. 1, lett. *n*) nonché c. 2, 3 e 4). Nel considerando 32 viene richiamata la necessità di definire le opere europee ma, anche in questo caso, viene fatto un sostanziale rinvio alla normativa degli Stati membri[30]. Nel precedente considerando 22 si menzionano, viceversa, gli ambiti esclusi dalla definizione di servizi di media audiovisivi, tra cui figurano anche i giochi "in linea", facendo riferimento alle forme allora possibili del *gaming* online, che prevedevano comunque una "trasmissione" e fruizione online dei videogiochi ma non i videogiochi in sé, nella loro complessità e varietà di forme, in quanto "opere". Questo riferimento scompare, peraltro, nella nuova edizione della Direttiva e davvero sembrava sovrabbondante visto che la differenza tra videogiochi online e servizi audiovisivi, per come definiti nella successione delle direttive UE, pare sostanziale ed evidente.

La più recente revisione della Direttiva SMA[31] reca alcune importanti novi-

CE del Parlamento europeo e del Consiglio, dell' 11 dicembre 2007, che modifica la direttiva 89/552/CEE del Consiglio relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti l'esercizio delle attività televisive (Testo rilevante ai fini del SEE), in GUCE L 332/27 del 18 dicembre 2007.

[29] Salvo quanto precisato in nota 23, con riferimento agli art. 16 e 17 della Direttiva SMAV.

[30] Considerando 32, direttiva 2010/13/UE: «Per i fini della presente direttiva occorre definire le "opere europee", fatta salva la possibilità per gli Stati membri di precisare questa definizione per quanto riguarda i fornitori di servizi di media audiovisivi soggetti alla loro competenza nel rispetto del diritto dell'Unione e tenendo conto degli obiettivi della presente direttiva».

[31] Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di

tà ma neanche in questa occasione ricorrono elementi che possano anche solo sollevare la possibilità di una assimilazione alle opere audiovisive dei prodotti videoludici. D'altra parte applicare ai videogiochi il complesso di norme maturate in sessanta anni per il sistema audiovisivo, ieri analogico, oggi digitale, pone una serie di problemi applicativi notevoli per cui sembra ragionevole l'estrapolazione di una serie di principi e relative ricadute in termini di regolazione, da applicare solo agli aspetti che più compiutamente coincidono, tra i due tipi di prodotti/servizi.

3.1. Videogiochi, opere audiovisive, prodotti e servizi digitali. Prospettive di regolazione.

Da questo quadro, in base alla normativa vigente e a quella che si prefigura, si coglie l'evoluzione dei media e il tentativo sempre più determinato dell'UE di tutelare e promuovere la propria produzione audiovisiva in una prospettiva culturale ma sempre più decisamente anche industriale ed economica. Questa prospettiva emerge con maggiore chiarezza anche nei documenti e nelle iniziative che l'UE sta conducendo per la realizzazione del Mercato unico digitale e in particolare per il Decennio digitale europeo[32]. Il Libro verde sulla distribuzione *online* di opere audiovisive nell'Unione europea del 2011 e il successivo Libro verde sulla convergenza del 2013[33] evidenziano gli aspetti critici e le sfide che i cambiamenti del sistema dei media vanno ponendo alla produzione e diffusione audiovisiva europea in un contesto digitale e preparano il terreno alle priorità che saranno definite nella strategia per un Mercato unico digitale europeo, tra cui rientra, non a caso, anche la revisione della direttiva SMA. In questo contesto l'evoluzione dei videogiochi registra, come anticipato, la dematerializzazione dei prodotti e l'affermarsi del *gaming* online e di nuove forme di produzione, diffusione e fruizione di "servizi" videoludici.
A fronte di questo quadro possiamo osservare che, in assenza di una definizione di cosa siano le opere (audiovisive) europee e quali possano essere sicuramente qualificate come tali, in nessuno dei numerosi passaggi normativi citati queste sono accostate ai videogiochi.
Si intravede però qualche possibile cambiamento di approccio per una definizione dei videogiochi se si considera anche che, anche sotto l'espansione del mercato videoludico *online* e l'affermarsi parallelo del fenomeno degli *e-sports*, l'UE ha incluso i videogiochi tra i numerosi interventi nelle politiche per la realizzazione di un mercato unico digitale che, a diverso ti-

determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato, in *GUUE* L 303 del 28 novembre 2018. La direttiva è stata attuata in Italia con il d.lgs. 208/2021, che costituisce il nuovo Testo unico dei servizi di media audiovisivi. Sulla direttiva e sul suo impatto v. G. B. Abbamonte - E. Apa - O. Pollicino (a cura di), *La riforma del mercato audiovisivo europeo*, Torino, 2019.

[32] Decennio digitale europeo: obiettivi digitali per il 2030, in *commission.europa.eu.*

[33] *Libro verde sulla distribuzione online di opere audiovisive nell'Unione europea - Verso un mercato unico del digitale: opportunità e sfide*, COM(2011) 427 definitivo; *Libro Verde, Prepararsi a un mondo audiovisivo della piena convergenza: crescita, creazione e valori,* COM(2013) 231 final.

tolo, l'Unione persegue, in particolare sottolineandone la valenza culturale e l'importanza di rafforzare anche questo comparto produttivo.
L'UE sembra quindi, in particolare negli ultimi anni, tentata dall'attrarre la disciplina dei videogiochi nell'orbita delle opere audiovisive e tuttavia in modo incerto, come fosse un approdo comunque insoddisfacente[34]. Sembra dunque sia, ad oggi, privilegiata ancora una pluralità di approcci, maggiormente sensibile alla valorizzazione dei videogiochi come prodotto in senso lato culturale ma anche in relazione alla loro dimensione digitale[35]. Una risoluzione del Parlamento europeo[36] invita infatti la Commissione e il Consiglio a riconoscere i videogiochi quali "potente strumento intersettoriale", che incrocia varie tecniche artistiche con tecnologie innovative, ed esprime l'auspicio di una valorizzazione dell'"ecosistema" dei videogiochi quale importante industria culturale e creativa, auspicando lo sviluppo di una strategia europea coerente e a lungo termine in materia.
Più incisive ancora le conclusioni del Consiglio dell'UE del 2023[37] che ripropongono la definizione dei videogiochi quali opere creative complesse, esaltandone il valore creativo proprio, rifacendosi alla giurisprudenza della Corte di giustizia, in particolare alla causa C-355/12, citata *supra*. Inoltre il Consiglio conferma il settore dei videogiochi quale parte integrante dell'ecosistema delle industrie culturali e creative, evidenziando come interagisca con altri settori. Se ne sottolinea anche il grande potenziale nel creare e trasmettere contenuti e valori culturali ed evidenziare la ricchezza e la diversità della creazione, del patrimonio e della storia europei, oltre ad avere un impatto significativo in termini di creazione di posti di lavoro e a contribuire considerevolmente al Prodotto Interno Lordo. Soprattutto il Consiglio rafforza la caratteristica dei videogiochi come vero e proprio bene culturale (parr. 11 e 13) e sembra implicitamente valorizzare la prospettiva normativa italiana, su cui ci soffermeremo nel paragrafo successivo, laddove auspica che gli Stati membri si adoperino per introdurre meccanismi di finanziamento, anche, se del caso, ispirandosi a quelli esistenti per altri settori culturali e creativi quale l'industria audiovisiva (par. 12).
Al momento, dunque, l'UE sembra orientata a considerare la dimensione culturale dei videogiochi, pur mantenendoli distinti dalle opere audiovisive, alla cui regolazione tuttavia si ispira sempre di più per mutuare principi

[34] Si veda ad es. la Risoluzione del Parlamento europeo del 18 gennaio 2023 Protezione dei consumatori nei videogiochi online: un approccio a livello del mercato unico europeo (2022/2014(INI)), in *GUUE* C del 16 giugno 2023, considerando D: «considerando che, nonostante il suo ruolo centrale nell'ecosistema culturale e creativo europeo, il settore dei videogiochi è ancora trascurato dai legislatori rispetto ad altri settori dei media, in particolare i film e altri prodotti audiovisivi, che ricevono generalmente maggiori finanziamenti e sono utilizzati come modello per dare forma alla regolamentazione e alle politiche in materia di videogiochi, un approccio che non tiene conto delle differenze tra di loro».

[35] Alle definizioni già richiamate si aggiunge ad es. quella di «intrattenimento popolare» ma anche «opera d'arte con un valore culturale», contenute nella Risoluzione del Parlamento europeo appena citata.

[36] Risoluzione del Parlamento europeo del 10 novembre 2022 su sport elettronici e videogiochi (2022/2027(INI)), in GUUE C del 5 maggio 2023.

[37] Conclusioni del Consiglio sul rafforzamento della dimensione culturale e creativa del settore europeo dei videogiochi (C/2023/1345), in GUUE C del 30 novembre 2023.

e modelli di tutela e valorizzazione culturale.
Se da un lato questo intervento è da salutare con favore, come segno di interesse dell'Unione per questo settore e come auspicio per una regolazione sistemica di fonte UE, dall'altro se ne deve registrare il significativo ritardo, su cui incidono, trasversalmente, anche gli altri interventi normativi su mercato e servizi digitali. Dobbiamo necessariamente fare riferimento, quindi, agli elementi che influiscono sulla regolazione dei videogiochi e che sono rintracciabili nelle principali fonti che stanno plasmando il sistema digitale europeo, quali, tra le altre, il *Digital Service Act* (DSA)[38], il *Digital Market Act* (DMA)[39] ma anche la direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale, attuata in Italia con il d.lgs. 177/2021, che modifica la nostra L.D.A.[40], nonché la direttiva (UE) 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, attuata con d.lgs. 173/2021[41].
Concentrandoci principalmente, in termini di regolazione, sul DSA[42] questo costituisce un riferimento normativo anche per i videogiochi solo se il videogioco si configuri come servizio *online* e ricada nelle ipotesi previste dal DSA. Come noto, i destinatari del DSA sono i prestatori di servizi intermediari, e in particolare quelli consistenti in servizi noti come semplice trasporto (*mere conduit*), memorizzazione temporanea (*caching*) e memorizzazione di informazioni (*hosting*)[43]. Questi servizi di intermediazione sono effettivamente propri anche dei videogiochi *online* se si pensa ad es. ai servizi di messaggistica multigiocatore attivi in quasi tutti i giochi *online*, o ai videogiochi con contenuti generati dall'utente, che quindi possono

[38] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in GUUE L del 27 ottobre 2022.

[39] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE)2020/1828 (regolamento sui mercati digitali), in GUUE L 265 del 12 ottobre 2022.

[40] E sulla base della quale l'Agcom viene investita di nuove e significative competenze. Su uno specifico aspetto di questa direttiva è da segnalare, per quanto qui rileva, una affermazione contenuta nelle Conclusioni dell'Avvocato generale H. Saugmandsgaarde, presentate il 15 luglio 2021, nella causa CGUE, C-401/19, *Repubblica di Polonia c. Parlamento europeo e Consiglio dell'Unione europea*. Nelle sue Conclusioni, l'avvocato generale infatti afferma che l'art. 17 della direttiva (UE) 2019/790 si applica, in assenza di qualsivoglia limitazione al riguardo nei termini di tale articolo o nella definizione del «prestatore di servizi di condivisione di contenuti online» figurante all'art. 2, p. 6, di tale direttiva, a tutti i tipi di materiali protetti (visivi, musicali, cinematografici, testuali, ma anche le linee di codici, i videogiochi, ecc.).

[41] D.lgs. 173/2021, recante "Attuazione della direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali".

[42] Anche il DMA impatta sulla regolazione del mercato videoludico, ad es. per aspetti connessi alla disponibilità dei videogiochi attraverso le piattaforme, aspetto su cui qui non ci soffermiamo.

[43] Tali prestatori di servizi rientrano nella più ampia categoria dei prestatori di determinati servizi della società dell'informazione definiti nella direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ossia qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario.

essere inclusi nella categoria degli *hosting*. Quindi valgono anche in ambito videoludico i principi di maggiore responsabilizzazione degli intermediari *online*, specie quelli di più grandi dimensioni e così anche in ambito videoludico si dovrà applicare il meccanismo di *notice and action*, che contempla non solo la rimozione dei contenuti (*notice and take down*), ma prevede che gli intermediari predispongano meccanismi idonei a garantire che la rimozione o, meglio, la moderazione degli stessi. Le società che offrono servizi di videogioco *online* devono quindi, ove ne ricorrano le condizioni e con le specifiche previsioni per le piattaforme online molto grandi, corrispondere alle nuove regole così come qualsiasi altro prestatore di servizi intermediari *online*.

Un altro aspetto da considerare ai fini di un inquadramento giuridico europeo dei videogiochi, da richiamare in questa sede, è legato all'impatto dell'*AI Act*, regolamento (UE) 2024/1689[44]. A titolo di premessa, e in via indicativa, occorre segnalare che l'IA, in particolare con un sistema LLM, può intervenire in un videogioco sia nella fase di produzione che nella fase di fruizione, anche se in alcuni momenti le due fasi sono collegate tra loro. L'IA può intervenire attivamente, come se fosse un altro giocatore, un *player*, o, in senso più ampio, accompagnando l'esperienza di gioco del giocatore umano come un assistente che dà consigli, commenta, incoraggia, oppure può intervenire anche solo per controllare l'efficace funzionamento del gioco, anche ai fini di un suo miglioramento in fase di produzione. Oppure l'IA può contribuire, in modo più o meno intenso, nella progettazione di un gioco in sostituzione o a supporto dei programmatori e altri soggetti che operano nella catena di produzione videoludica; si pensi anche solo al processo di analisi dei dati di gioco, per migliorare il prodotto che implica peraltro, di fatto, un monitoraggio puntuale delle abitudini e delle dinamiche di gioco adottate dal giocatore[45]. In questa duplice prospettiva i produttori di videogiochi, rispetto al regolamento (UE) 2024/1689 possono rientrare tra le categorie di fornitori o di *deployer*, quindi quali fornitori di sistemi di IA, se realizzino autonomamente sistemi propri da utilizzare nella filiera produttiva del videogioco, o come di utilizzatori di sistemi di IA, laddove invece utilizzino prodotti e sistemi di IA generati da altri soggetti. Secondo questi due diversi ruoli che possono assumere saranno assoggettati alle disposizioni dell'*AI Act*, e, secondo la classificazione delle diverse categorie di rischio, ai divieti e agli obblighi da queste conseguenti. Si pensi ad esempio all'applicazione, in ambito videoludico, del divieto di tecniche subliminali o di tecniche volutamente manipolative o ingannevoli o al divieto di sfruttare le vulnerabilità di una persona fisica o di uno specifico gruppo di persone (art. 5, *AI Act*), o dai sistemi, considerati "ad alto rischio" che configurino una profilazione di persone fisiche, profilazione che, più o meno in profondità, avviene attraverso l'analisi delle abitudini

[44] 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), in GUUE L del 12 luglio 2024.

[45] R. Gallotta et al., *Large Language Models and Games: A Survey and Roadmap*, in *IEEE Transactions on Games, Institute of Electrical and Electronics Engineers (IEEE)*, 2024.

di gioco, soprattutto per determinati giochi. A seconda dei ruoli quindi i produttori dovranno adottare i sistemi di gestione del rischio e di *governance* dei dati previsti dal Regolamento, nonché, per i fornitori di sistemi di IA, il rispetto degli obblighi di trasparenza e informazione nei confronti dei *deployer*. Inoltre occorre ricordare che gli obblighi di alfabetizzazione sull'IA, che competono tanto ai fornitori che ai *deployer* (art. 4, *AI Act*), definita come le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai *deployer* e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto dell'*AI Act*, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare (art. 3, par. 1, n. 56).

4. Definizione giuridica dei videogiochi e approccio normativo e regolatorio in Italia: tra sostegno economico e tutela dei minori

A fronte di questo quadro europeo, e prima che maturassero i vari provvedimenti europei sul mercato e i servizi digitali, il legislatore italiano aveva iniziato a percorrere una propria via per una definizione giuridica dei videogiochi. Le novità più rilevanti arrivano infatti dagli interventi in materia di "opere audiovisive" e riguardano il riconoscimento di alcune misure di sostegno economico e la classificazione dei videogiochi al fine di tutelare i minori. Si riprende in qualche modo il risalente richiamo alle opere cinematografiche, facendo prevalere l'elemento audiovisuale, il carattere narrativo e culturale rispetto a quello, esplorato negli ultimi tre decenni del secolo scorso, della presenza del *software*.

La legge che riforma il cinema e l'audiovisivo (l. 220/2016, Disciplina del cinema e dell'audiovisivo), interviene principalmente a ridisegnare le forme di sostegno a questo settore oltre ad introdurre e modificare alcuni altri aspetti relativi alle "opere audiovisive", sia in una prospettiva tipicamente culturale che in quella produttiva e industriale.

La legge 220/2016 ruota intorno a un nuovo apparato definitorio che si fonda proprio sulle "opere audiovisive", definite quali «la registrazione di immagini in movimento, anche non accompagnate da suoni, realizzata su qualsiasi supporto e mediante qualsiasi tecnica, anche di animazione, con contenuto narrativo, documentaristico o videoludico, purché opera dell'ingegno e tutelata dalla normativa vigente in materia di diritto d'autore e destinata al pubblico dal titolare dei diritti di utilizzazione» (art. 2, c. 1, lett. *a*). Il contenuto videoludico è quindi uno dei possibili contenuti delle opere audiovisive e, dal dato testuale, i videogiochi si intendono collocati tra le opere audiovisive in un rapporto di *species* e *genus*.

Inoltre con la l. 220/2016 viene riformata la mai amata "censura cinematografica", la revisione preventiva dei film e anche questo aspetto riverbera nella disciplina dei videogiochi. In realtà la legge, all'art. 33, si limita a delegare il Governo ad adottare uno o più decreti legislativi per la riforma delle disposizioni legislative di disciplina degli strumenti e delle procedure previsti in materia di tutela dei minori nella visione di opere cinemato-

grafiche e audiovisive[46]. Il d.lgs 203/2017, di attuazione della delega con riferimento alle opere cinematografiche[47] a sua volta delega l'Autorità per le Garanzie nelle Comunicazioni, Agcom, ad adottare un regolamento per disciplinare la classificazione delle "opere audiovisive destinate al web" e dei videogiochi, introdotti già con la l. 220/2016 tra le opere audiovisive (art. 10, d.lgs. 203/2017).

Importante sottolineare che il d.lgs. 203/2017 tra i vari principi di attuazione della delega, deve rispettare quello volto a garantire la uniformità di classificazione con gli altri prodotti audiovisivi, inclusi i videogiochi (art. 33, c. 2, lett. *a)* l. 220/2016), che garantisca la tutela dei minori e la protezione dell'infanzia e la libertà di manifestazione del pensiero e dell'espressione artistica.

Tra tutte le definizioni della l. 220/2016 non troviamo però quella dei videogiochi che ricompaiono nel d.lgs. 203/2017, art. 10, già citato, solo per sub-delegare l'Agcom ad adottare un regolamento per la classificazione delle "opere audiovisive destinate al web" e per i videogiochi [48].

---

[46] In realtà il testo dell'art. 33 è già in apparente contraddizione con l'art. 1 della stessa legge, che avrebbe limitato gli interventi da realizzare tramite delega al Governo per la tutela dei minori al solo ambito cinematografico («anche attraverso apposite deleghe legislative al Governo, della normativa in materia di tutela dei minori nel settore cinematografico»). Più in particolare, l'art. 33, l. 220/2016 individua i principi cui il Governo nell'esercizio della delega dovrà attenersi: a) il principio della responsabilizzazione degli operatori cinematografici in materia di classificazione del film prodotto, destinato alle sale cinematografiche e agli altri mezzi di fruizione; b) il principio della uniformità di classificazione con gli altri prodotti audiovisivi, inclusi i videogiochi. Entrambi i principi dovranno garantire la tutela dei minori e la protezione dell'infanzia e la libertà di manifestazione del pensiero e dell'espressione artistica. Vale la pena sottolineare che la classificazione dei prodotti, da quelli cinematografici in poi, assolve alla necessaria e meritoria tutela dei minori ma si porta dietro conseguenze rilevanti anche ai fini dei mercati in cui tali prodotti vanno a collocarsi, e quindi, in senso lato, di appetibilità commerciale dei prodotti ai fini di una fruizione da parte di un pubblico più o meno ampio. Il d.lgs. 203/2017, in ossequio al principio di responsabilizzazione, vede effettuare la proposta di classificazione direttamente dagli operatori, salvo successiva verifica della neo-istituita Commissione per la classificazione delle opere cinematografiche. Per una analisi di questi aspetti si rinvia a M. Ramajoli, *Cinema e libertà: dalla censura preventiva al* movie rating system, in Aedon, 1, 2018.

[47] D. lgs. 203/2017, recante "Riforma delle diposizioni legislative in materia di tutela dei minori nel settore cinematografico e audiovisivo, a norma dell'articolo 33 della legge 14 novembre 2016, n. 220".

[48] Art. 10, d. lgs. 203/2017, recante "Classificazione delle opere audiovisive destinate al web e dei videogiochi": «1. Con regolamento dell'Autorità per le garanzie nelle comunicazioni, adottato entro centoventi giorni dalla data di pubblicazione del presente decreto, sentito il Ministro dei beni e delle attività culturali e del turismo, è disciplinata la classificazione delle opere audiovisive destinate al web e dei videogiochi. 2. La classificazione di cui al presente articolo è finalizzata ad assicurare il giusto e equilibrato bilanciamento tra la tutela dei minori e la libertà di manifestazione del pensiero e dell'espressione artistica. In particolare, il regolamento di cui al presente articolo è adottato nel rispetto: a) dei principi di cui all'articolo 2, comma 1, del presente decreto; b) delle disposizioni, in quanto compatibili, degli articoli 34 e 35 del decreto legislativo 31 luglio 2005, n. 177, e successive modificazioni, anche con specifico riguardo alla definizione di accorgimenti tecnici idonei ad escludere che i minori vedano normalmente opere vietate, e delle relative sanzioni ivi previste; c) degli standard e delle migliori pratiche internazionali del settore, con particolare riferimento ai sistemi di classificazione maggiormente diffusi, tra i quali il PEGI, Pan European Game Information - Informazioni paneuropee sui giochi».

Si tralasciano, in questa sede, alcune riflessioni sui criteri di attuazione della delega,[49] e in particolare in relazione alla scelta con cui il d.lgs. 203/2017 prima e l'Agcom poi hanno individuato e definito e regolato i videogiochi per gli aspetti delegati, su cui la stessa l. 220/2016 non aveva dato una propria definizione e quindi un perimetro giuridico[50].

È quindi al regolamento Agcom che interviene in materia di classificazione dei videogiochi nel 2019[51] che occorre guardare per individuare una prima definizione normativa di videogioco, per tale intendendosi: «l'opera multimediale interattiva a carattere videoludico fruibile mediante ogni mezzo di comunicazione che ne consenta l'operatività» (art. 1, c. 1, lett. *f)*, delibera n. 74/19/CONS).

La definizione individuata dall'Agcom fa riferimento al carattere multimediale dei videogiochi che, da un lato, ne costituisce un tratto distintivo potremo dire connaturato - se si accede alla qualificazione "multimediale" come opera caratterizzata dalla compresenza di plurimi mezzi di espressione quali immagini, suoni, etc. utilizzando tecnologie digitali e un sistema di *software* - dall'altro lato porta con sé un annoso dibattito sulla natura giuridica di questa definizione e sulla sua estensione in termini, ancora una volta, di applicazione della normativa in materia di diritto d'autore[52].

A riprova di questa stratificazione, tra fonti di diverso livello, e conseguenti implicazioni definitorie, esiste peraltro una ulteriore competenza

---

[49] Si segnala inoltre che, la delega contenuta nella l. 220/2016 è anche esplicitamente volta a «prevedere le abrogazioni e modificazioni della normativa vigente». Le abrogazioni ma anche le modificazioni della normativa vigente non possono quindi che intervenire con norma di rango primario, quale appunto un decreto legislativo, e non con un regolamento Agcom (art. 33, c. 2, lett. *e*) che interviene su aspetti tecnici, ma comunque rilevanti per i settori considerati.

[50] Il d.lgs. 203/2017 effettua una subdelega a soggetto diverso dal Governo, l'Agcom, appunto, che la attuerebbe attraverso, evidentemente, fonti normative non di rango primario. La subdelega non è ignota al nostro sistema costituzionale ma è da limitare ad alcuni casi. In particolare, secondo la giurisprudenza della Corte, l'esercizio del potere di delega a soggetti diversi dal Governo, che attuerebbero tale subdelega attraverso atti che non sono fonti di rango primario, è da ancorare alla natura soggettiva agli organi destinatari della subdelega. Dovrebbe infatti trattarsi di organi espressione del potere politico del Governo, in sostanza i Ministeri, e questo essenzialmente perché non si realizzi, attraverso la subdelega, la mancanza di una assunzione diretta di responsabilità politica da parte del Governo, facendo così venire meno uno degli elementi essenziali su cui si fonda l'art. 76 Cost.

[51] Agcom, delibera n. 74/19/CONS del 6 marzo 2019, regolamento sulla classificazione delle opere audiovisive destinate al web e dei videogiochi di cui all'art. 10, commi 1 e 2, del decreto legislativo 7 dicembre 2017, n. 203 recante «riforma delle disposizioni legislative in materia di tutela dei minori nel settore cinematografico e audiovisivo, a norma dell'art. 33 della legge 14 novembre 2016, N. 220». V. anche delibera n. 359/19/CONS del 18 luglio 2019 *Linee guida relative alla classificazione delle opere audiovisive destinate al web e dei videogiochi di cui al Regolamento approvato con delibera n. 74/19/CONS e istituzione dell'Osservatorio permanente per la co-regolamentazione della classificazione delle opere audiovisive destinate al web e dei videogiochi.* Sulla elaborazione del Regolamento da parte dell'Agcom sia consentito rinviare a M. Caporale, *L'Agcom e la legge sul settore cinematografico e audiovisivo. Le opere audiovisive destinate al web*, in questa *Rivista*, 3, 2018.

[52] Il termine "multimediale" ricorre peraltro anche nella giurisprudenza italiana riferita ai videogiochi, tra cui v. Cass. pen, sez. III, 1° agosto 2017, n. 38204; C. Di Cocco, *Multimedialità e diritto d'autore*, in *Diritto di Internet*, 3, 2007, 297 ss.; S. Magelli, *Le opere multimediali nell'esperienza giurisprudenziale italiana*, in *Diritto industriale*, 2, 2021, 190 ss.

dell'Agcom riferita ai prodotti videoludici ma che, in questo caso, risultano collocati nell'alveo delle "opere digitali". Nell'ambito delle proprie competenze per la tutela del diritto d'autore online[53], infatti, l'Agcom promuove lo sviluppo dell'offerta legale di opere digitali e l'educazione alla corretta fruizione delle stesse, anche attraverso la definizione di procedure volte all'accertamento e alla cessazione delle violazioni del diritto d'autore e dei diritti connessi, comunque realizzate, poste in essere sulle reti di comunicazione elettronica.

Il regolamento dell'Agcom sul diritto d'autore qualifica l'"opera digitale" quale «un'opera, o parti di essa, di carattere sonoro, audiovisivo, fotografico, videoludico, editoriale e letterario, inclusi i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla Legge sul diritto d'autore e diffusa su reti di comunicazione elettronica».

Una ulteriore variazione sul tema, quindi, un diverso sguardo con cui lo stesso soggetto, l'Agcom, esercita le proprie, diverse competenze sui videogiochi, quali "opere audiovisive" da un lato, ma anche "opere digitali" dall'altro, su binari diversi, in ragione delle diverse caratteristiche dei videogiochi e quindi per l'esercizio di diverse competenze dell'Agcom.

Da questo *excursus* emerge chiaramente comunque che il legislatore italiano sembra finalmente consapevole della valenza dei videogiochi ed il suo intervento è teso da un lato alla promozione e sostegno alla produzione, a dare maggiore riconoscimento alla natura creativa dell'opera videoludica attraverso le categorie e gli strumenti approntati per le opere e l'industria audiovisiva, non ultimo attraverso misure di promozione e supporto e qualche prima forma di sostegno economico ad una categoria che ne è rimasta sempre priva; dall'altro alla tutela del diritto d'autore, in ragione delle specificità della tutela a contrasto della prateria digitale, appunto includendo i videogiochi tra le "opere digitali".

I videogiochi non sono espressamente evidenziati come oggetto delle misure previste dalla legge 220/2016 ma, essendo parte delle opere audiovisive e poiché sono queste le destinatarie, come categoria generale, dei benefici della legge, godono anch'essi delle misure di sostegno ivi contemplate, in particolare una forma di *tax credit*, il cui modello ispiratore sembra essere quello del credito di imposta francese[54], che può essere riconosciuto a videogiochi che siano qualificati come prodotti italiani, con una percentuale di "italianità" individuata nel 25% della produzione considerata, secondo diversi indicatori. Il riconoscimento di questi benefici,

[53] Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70, della delibera n. 680/13/CONS e s.m.i., testo coordinato con le modifiche di cui alla delibera n. 233/21/CONS, nonché, da ultimo, dalla delibera n. 189/23/CONS. Non è questa la sede per ripercorrere il dibattito nato intorno a questo provvedimento. Per una ricostruzione delle competenze Agcom in questo ambito v. Servizio Studi della Camera dei Deputati, *Prevenzione e repressione della diffusione illecita di contenuti tutelati dalla normativa sul diritto d'autore mediante le reti di comunicazione elettronica*, Schede di lettura, 26 maggio 2021.

[54] *Décret n° 2022-1392 du 19 octobre 2022 modifiant les dispositions du code du cinéma et de l'image animée relatives aux crédits d'impôt en faveur des créateurs de jeux vidéo.* La Francia è il Paese europeo che ha una regolazione più avanzata sul settore videoludico, anche grazie all'esperienza maturata nel sostegno al cinema e all'audiovisivo, che hanno costituito un tratto distintivo della legislazione francese in ambito culturale.

posto sotto l'egida del Ministero della Cultura, promuove e quindi orienta la produzione videoludica italiana verso un'accezione in senso lato culturale dei videogiochi e per le quali è possibile invocare il regime di "eccezione culturale"[55] e le tutele previste per le opere europee, secondo un sistema mutuato appunto dai sistemi di regolazione delle opere audiovisive.

Il decreto con cui è stata data attuazione, per la prima volta, a tali misure di sostegno[56] , precisa che ai fini del medesimo decreto, si applicano le definizioni contenute nella legge n. 220 del 2016 e le ulteriori specificazioni contenute nei decreti di attuazione della medesima legge. Tuttavia, come abbiamo segnalato, né la legge 220/2016 né i successivi decreti legislativi recano una definizione di videogioco, che è stata fornita dall'Agcom in attuazione della "sub-delega" in materia di classificazione dei videogiochi. Lo stesso decreto citato definisce quindi il videogioco quale: «l'opera audiovisiva che simula situazioni ambientate in mondi virtuali o reali di diversa natura ed è costruita intorno a un percorso di base che si sviluppa in funzione dell'interazione ludica con uno o più giocatori; può essere fruita mediante appositi dispositivi elettronici, computer o altri apparecchi, anche portatili; può prevedere una fruizione online» (art. 1, c. 2, lett. *e*) d.i. MC-MEF 12 maggio 2021). Viene quindi fatto cenno alla possibilità che l'opera si trasformi in un servizio, secondo le categorie del DSA e della fruizione di servizi online, ma non si entra evidentemente nel merito di questa opzione.

Come anticipato, definendo i videogiochi come una sotto-specie delle opere audiovisive e riconoscendogli natura culturale, li si sottopone al regime di "eccezione culturale" e quindi anche alla conseguente ammissibilità di forme di sostegno economico compatibili con il generale divieto di aiuti di stato di matrice europea. Nella prima versione del regolamento (UE) n. 651/2014 che dichiara alcune categorie di aiuti compatibili con il mercato interno i videogiochi erano stati espressamente esclusi dall'ammissibilità di aiuti di stato mentre nel testo oggi vigente del Regolamento, a seguito delle numerose modifiche intervenute, l'esclusione dei videogiochi è scomparsa. Sono sempre ammessi gli aiuti di stato, invece, a determinate condizioni, per le "opere audiovisive" per le quali sono definiti i tipi di sostegno e i tipi di costo che può essere sostenuto, ma non sono definite le opere audiovisive in sé, salvo alcune specifiche caratteristiche. In questa sede tale mancanza di definizione permette quindi che le "opere audiovisive", a parere di chi scrive, possano comprendere anche i videogiochi[57].

---

[55] L'eccezione culturale consente agli Stati membri dell'UE ma anche nell'ambito di altre organizzazioni internazionali di assoggettare determinati prodotti e servizi a speciali tutele a aiuti economici, in regime di deroga rispetto alle norme a favore della concorrenza, a tutela della cultura propria di ogni stato e a sostegno della diversità culturale. V. S. Foà - W. Santagata, *Eccezione culturale e diversità culturale. Il potere culturale delle organizzazioni centralizzate e decentralizzate*, in *Aedon*, 2, 2004; G. Mazzone, *Dall'eccezione alla diversità culturale: ministoria di una sfida per l'Europa*, in *Economia della Cultura*, 3, 2008, 327 ss.

[56] D.I. MiC e MEF 12 maggio 2021 REP 187, Disposizioni applicative in materia di credito di imposta per le imprese di produzione di videogiochi di cui all'articolo 15 della legge 14 novembre 2016, n. 220.

[57] Regolamento (UE) n. 651/2014 della Commissione del 17 giugno 2014 che dichiara alcune categorie di aiuti compatibili con il mercato interno in applicazione degli articoli 107 e 108 del Trattato, v. considerando 72 del testo originario, secondo cui «l'elenco di

5. I videogiochi come opera culturale complessa e le geometrie variabili della regolazione

Nella diversa prospettiva in cui sono adottati i due provvedimenti del MiC e dell'Agcom le definizioni di videogioco che, rispettivamente, vi sono riportate assolvono a finalità diverse e scontano l'assenza di una previa definizione per via normativa, con fonte di rango primario, dell'oggetto "videogioco". La definizione dell'Agcom, che ha per oggetto la classificazione dei videogiochi ai fini della tutela dei minori, sottolinea l'elemento multimediale e quindi la molteplicità di canali di fruizione attraverso cui i minori possono entrare in contatto con prodotti videoludici potenzialmente lesivi dei loro diritti. La definizione del decreto interministeriale evidenza più l'elemento creativo e narrativo, più coerente con la contestualizzazione dei videogiochi tra i prodotti culturali destinatari di sostegni economici, lasciando l'elemento del *software* più in secondo piano e facendo solo un cenno veloce alla possibile fruizione *online* dei videogiochi e quindi alla possibile natura cangiante degli stessi, da prodotto a servizio. Queste definizioni sono compatibili con la normativa al momento adottata dall'UE ma soprattutto con le sue carenze. Costituiscono, anzi uno spunto di riflessione utile anche per i prossimi passi che l'UE *in primis* dovrebbe intraprendere per disciplinare il comparto. Nonostante queste asimmetrie lo sforzo per dare dignità e riconoscimento normativo al comparto videoludico ha un grandissimo significato che peraltro ha anticipato alcuni degli spunti normativi che stanno emergendo anche a livello europeo.

Tuttavia, sembra che una definizione giuridica unica, utilizzabile nei contesti normativi richiamati – principalmente sostegno alle opere videoludiche (anche come *species* del *genus* delle opere audiovisive) e classificazione dei videogiochi ai fini della tutela dei minori ma anche diritto d'autore, tutela dei dati personali, etc. –, sia pure nelle diverse finalità perseguite, gioverebbe a una più limpida definizione del perimetro normativo dei videogiochi e a una più sistematica riconoscibilità dei diritti e delle tutele applicabili.

Colpisce che, nella frammentarietà degli interventi normativi commentati, si perda quasi del tutto la dimensione fondamentale dei videogiochi e cioè l'elemento ludico, di gioco in sé, che potrebbe aiutare a discriminare e precisare meglio i confini dei videogiochi e delle loro caratteristiche, anche culturali.

Sembra quindi auspicabile una definizione giuridica unica ma che individui le varie componenti possibili dei videogiochi, che valorizzi i differenti elementi dell'opera complessa e rinvii alla normativa applicabile a seconda delle caratteristiche del videogioco, rafforzandone la natura culturale per favorire questa specifica espressione e diffusione della cultura europea e dei singoli Stati membri, con le necessarie tutele che le vecchie, ma soprattutto le nuove potenzialità dei videogiochi richiedono.

---

obiettivi e di attività culturali ammissibili non comprende attività commerciali, quali la moda, il design o i videogiochi». Il testo coordinato del Regolamento, a seguito delle numerose modifiche, è consultabile dalle pagine Eur-Lex anche se si tratta di una ricostruzione priva di valore legale. V. C. E. Baldi, *Finanziamento della cultura e regole di concorrenza. Nuove prospettive dal ripensamento della Commissione europea*, in *Aedon*, 3, 2016; F. Togo, *Aiuti di Stato nel settore culturale*, in *Aedon*, 2, 2009.

Abstract

L'articolo propone una riflessione sulla natura dei videogiochi e sull'opportunità di una loro definizione giuridica, in un momento in cui tecniche e modalità espressive favoriscono il riconoscimento delle loro caratteristiche di opere creative e culturali, ponendo alcune nuove sfide al regolatore. Nell'attuale, frammentario e carente quadro normativo prevale infatti la natura complessa dei videogiochi, che rende solo in parte mutuabile la normativa in materia di opere audiovisive e delle disposizioni adottate per i servizi digitali, a fronte di un comparto che rappresenta valori di mercato che superano di gran lunga quelli delle opere audiovisive e cinematografiche e che necessiterebbe di una più adatta cornice normativa.

The article proposes a reflection about the legal nature of video games and the opportunity of its juridical definition, when techniques and expressive methods favor the recognition of their characteristics as creative and cultural works, posing some new challenges to the regulator. In fact, in the ongoing fragmented and lacking legislative framework, the nature of complex work of the video games prevails, making the legislation on audiovisual works and the provisions adopted for digital services only partially interchangeable, and referred to a sector that represents market values that far exceed those of audiovisual and cinematographic works and that seems to need a more adequate normative framework.

Keywords

videogiochi – opere audiovisive – industria creativa – prodotto culturale – eccezione culturale.

The EU Legal Framework on Personal Data Flows to Third Countries and its Interplay with EU International Commitments in the Field of Trade Law*

Gabriele Rugani

Table of Contents

1. Introduction. – 2. The current EU internal legal framework on transborder flows of personal data. – 2.1. The approach of the current EU internal legal framework. – 2.2. The purposes of the current EU internal legal framework. – 3. The interplay between the EU legal framework and EU international commitments in the field of trade law. – 3.1. EU international commitments concerning the liberalisation of trade in services in general. – 3.2. Data flows commitments included in some EU international trade agreements. – 3.3. The impact of the EU international commitments on the EU legal framework. – 3.4. The "horizontal provisions": a possible solution? – 4. Conclusions and suggestions.

1. Introduction

This paper will focus on how the European Union deals with transfers of personal data to non-EU States, the regulation of which aims at balancing two conflicting interests: on the one hand, the need to favour cross-border data flows, in order to foster the expansion of international trade; on the other, the need to protect personal data and privacy by limiting those same transfers.

First of all, it will be highlighted that the current EU internal legal framework concerning personal data flows to third countries – as designed in Regulation (EU) 2016/679 (GDPR), as interpreted by the Court of Justice of the European Union (CJEU) and as implemented by the EU Commission – gives clear priority to the fundamental rights to privacy and to the protection of personal data.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Given the above, the contribution deals with a specific research question: whether certain international commitments made by the EU in the field of trade law – some concerning in general the liberalisation of trade in services, some others devoted more specifically to data flows – are consistent or not with the balance designed by the abovementioned EU internal legal framework.

It can be anticipated that the answer to the question above will be negative. It will be highlighted that the rules binding the EU in the field of international trade law give clear priority to the need to transfer data: in order to favour the latter, the Union made several data flows commitments, counterbalanced by data protection provisions whose scope and effectiveness are at least questionable. This might create issues of consistency with the approach of the EU internal legal framework.

Therefore, it will be necessary to analyse the consequences of the divergence between the two approaches, and whether one can affect the other. In particular, it will be demonstrated that the approach of EU trade commitments seriously risks undermining the one of the EU internal legal framework. Indeed, since at international level trade agreements have strong enforcement mechanisms, this creates a significant risk of a de facto supremacy of trade law over human rights law: fearing the consequences of such mechanisms, several institutional players could be induced not to limit personal data flows, at the expense of data protection.

At this point, the investigation will proceed step by step, beginning with the underlying premises. In particular, it must be preliminary remembered that, as part of the ongoing digital transformation of the world economy, the use of data is becoming increasingly valuable to all kinds of businesses: not only to «data-enabled» ones[1], such as big tech firms[2], but also to traditional industries[3], defined as «data-enhanced businesses»[4]. We are witnessing a true «data economy», that it is growing every year and worldwide[5].

A key reality of a similar global economy is that a significant share of

---

[1] OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows. A Business Perspective, OECD Digital Economy Papers No. 297*, Paris, 2020, 9-11.

[2] See for instance: J.C.M. De Bustos-J. Izquierdo-Castillo, *Who will control the media? The impact of GAFAM on the media industries in the digital economy*, in *Revista Latina de Comunicación Social*, 74, 2019, 803 ss., at 812.

[3] See for instance: R.D. Atkinson, *International Data Flows: Promoting Digital Trade in the 21st Century, Testimony Before the U.S. House Judiciary Committee – Subcommittee on Courts, Intellectual Property and the Internet*, 2015, 5.

[4] See for instance: G. Magalhaes-C. Roseira, *Open government data and the private sector: An empirical view on business models and value creation*, in *Government Information Quarterly*, 37(3), 2020, 1 ss.

[5] See for instance: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building a European Data Economy, 10 January 2017, COM (2017) 9 final. See also: European Commission, *The European Data Market Monitoring Tool – Key Facts & Figures, First Policy Conclusions, Data Landscape and Quantified Stories – D2.9 Final Study Report*, 2020; European Commission, *Data Market Study 2021-2023 – D2.4 Second Report on Facts and Figures*, 2023; European Commission, *The European Data Market Study 2024-2026 - D1 Inception Report*, 2024.

such data needs to move freely, not only within States, but also across borders. Transborder flows of data, indeed, bring incredible benefits to enterprises[6], since they are of remarkable importance both in terms of volume[7] and, above all, of economic value[8]. Data flows, moreover, will grow exponentially year after year, mainly due to the incessant development and diffusion of new technologies[9].

Flows can involve different typologies of data. However, only personal data, i.e. information relating to identified or identifiable natural persons ("data subjects"), will be considered. Such choice is not random: on the one hand, personal data are extremely valuable for business activities (e.g. they allow companies to predict the behaviour of individuals)[10]; on the other, since natural persons are concerned, processing and transferring such data risk affecting the rights to privacy and protection of personal data.

The right to privacy, originally conceived in the US at the end of the XIX century[11], offers a "static", "negative" kind of protection: it only prevents others from interfering with one's private life[12]. The more recent right to personal data protection, instead, offers a "dynamic", "positive" kind of protection, since it confers to the individual control and intervention powers which follow data in all their movements[13]. Both rights are enshrined in the Charter of Fundamental Rights of the EU (CFREU), respectively in art. 7 and in art. 8[14]; it is worth clarifying that the qualification of a right as "fundamental" implies particularly stringent conditions on its limitations, which must in any case respect its essence[15].

Anyway, both rights can be jeopardised by transborder flows of personal data. This happens if the recipient country provides to those rights a lower

---

[6] See for instance: V. Espinel, *Executive Survey Shows the Benefits of Data Innovation Across the Whole Economy*, in *BSA Tech Post*, 2014; D. Castro-A. McQuinn, *Cross-Border Data Flows Enable Growth in All Industries – Information Technology & Innovation Foundation*, 2015.

[7] See for instance: McKinsey Global Institute, *Globalization in Transition: The Future of Trade and Value Chains – McKinsey&Company*, 2019, 72.

[8] See for instance: McKinsey Global Institute, *Digital Globalization: The New Era of Global Flows – McKinsey&Company*, 2016, 1.

[9] See for instance: M.C. Meneghetti, *I trasferimenti di dati personali all'estero*, in G. Finocchiaro (ed), *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 594 ss., at 599-600.

[10] G. D'Acquisto-F. Pizzetti, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi Giuridica dell'Economia*, 1, 2019, 89 ss., at 102.

[11] S.D. Warren-L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 4(5), 1890, 193 ss.

[12] S. Rodotà, *Data Protection as a Fundamental Right*, in S. Gutwirth-Y. Poullet-P. De Hert-C. De Terwangne-S. Nouwt (eds), *Reinventing Data Protection?*, New York, 2009, 77 ss., at 79.

[13] Ivi, at 79-80. See also: G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, 2014.

[14] On the point see, for instance: G. Braibant, *La Charte des Droits fondamentaux de l'Union européenne*, Paris, 2001, 47; N. Bernsdorff, *Kapitel II, Freiheiten: Artikel 6 Bis 19*, in J. Meyer (ed), *Kommentar zur Charta der Grundrechte der Europäischen Union*, Baden-Baden, 2003, 135 ss., at 160; B. Docquir, *Le droit à la vie privée*, Bruxelles, 2008, 41.

[15] On the point see, for instance: K. Lenaerts, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *German Law Journal*, 20(6), 2019, 779 ss.

protection than the one of the State from which the flow originated. Such eventuality raises concerns about the fate of the transferred information, that may result in the adoption of certain limitations and conditions to similar transfers.
Consequently, several legal instruments were developed worldwide with the purpose of balancing the two conflicting interests: on one side, the need to favour cross-border flows of personal data; on the other, the need to protect the rights of individuals[16]. Such instruments can end up favouring the first or the second of the two abovementioned interests[17]. As anticipated, this contribution will only focus on the balance designed by the EU, the details of which will be set out below.

2. The current EU internal legal framework on transborder flows of personal data

First of all, the paper will focus on the current EU internal legal framework concerning personal data flows to third countries, showing that it gives clear priority to the fundamental rights to privacy and to the protection of personal data, and explaining the purposes of such approach.

2.1. The approach of the current EU internal legal framework

The EU legal framework on cross-border personal data transfers has its origin in two important international law instruments. On the one hand, the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (reviewed in 2013), not binding but extremely influential globally: they were also imitated by other international instruments, such as the APEC (Asia-Pacific Economic Cooperation) 2005 Privacy Framework (reviewed in 2015)[18]. On the other hand, the 1981 Convention of the Council of Europe (CoE) for the Protection of Individuals with regard to Automatic Processing of Personal Data, better known as "Convention 108", the only international legally binding instrument in the

[16] On the tension between the needs of international trade, on the one hand, and the rights to privacy and personal data protection, on the other, as well as on the possible instruments to balance these opposing interests, see for instance: M. Burri, *Interfacing Privacy and Trade*, in *Case Western Reserve Journal of International Law*, 53(1), 2021, 35 ss.; A. Chander-P.M. Schwartz, *Privacy and/or Trade*, in *The University of Chicago Law Review*, 90(1), 2023, 49 ss.

[17] See for instance: C. Kuner, *Transborder Data Flows and Data Privacy Law*, Oxford University Press, Oxford, 2013; S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, in World Trade Review, 17(3), 2018, 477 ss., at 483.

[18] See for instance: L.A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford, 2014, 75 ss.

field[19], modernised in 2018 ("Convention 108+"[20]). The Guidelines and the Convention represent two different approaches to the regulation of personal data flows: while the former mainly aims at promoting transfers for economic reasons, the latter is more attentive to the protection of personal data[21].

Despite the differences, both instruments deeply influenced the subsequent EU legal framework on the matter. Indeed, the first legislative act adopted by the European Union in the field – Directive 95/46/CE – had two «twin objectives»[22]: the protection of individuals with regard to the processing of personal data and the free movement of such data. The latter, however, was clearly prioritised: the legal framework at stake was seen as instrumental to the needs of intra-Community trade.

In the years that followed the adoption of the Directive, things changed: data protection, born as a "market-building device", received growing attention in its dimension of fundamental right[23]: art. 8 of the CFREU enshrined the protection of personal data as a fundamental right deserving protection per se, and art. 16 TFEU provided an ad hoc legal basis for the adoption of rules concerning personal data.

In this new scenario, Directive 95/46/CE seemed outdated. In 2012, thus, a proposal for a General Data Protection Regulation (GDPR) was submitted by the European Commission, namely by Directorate-General Justice and Consumers (DG JUST). Such DG, that became in charge of the subject after the Lisbon Treaty, is much more consumer-oriented rather than market-oriented and is very sensitive to the protection of personal data as a fundamental right[24]. At the end of a long and complex iter legis, Regulation (EU) 2016/679 was finally adopted.

The whole GDPR clearly strengthens, through various provisions, the positions of individuals whose data are processed[25]. This is true also with

---

[19] UNCTAD, *Data protection regulations and international data flows: Implications for trade and development – United Nations Publication*, 2016, 83.

[20] Convention 108+ is not yet in force.

[21] See for instance: F.W. Hondius, *A Decade of International Data Protection*, in *Netherlands International Law Review*, 30, 1983, 103 ss., at 106; A. Newman, *Protecting Privacy in Europe: Policy Feedback and Regional Politics*, in S. Meunier-K.R. McNamara (eds), *The state of the European Union. Vol. 8. Making history: European integration and institutional change at fifty*, Oxford, 2007, 123 ss.; S. Nouwt, *Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union*, in S. Gutwirth-Y. Poullet-P. De Hert-C. De Terwangne-S. Nouwt (eds), *Reinventing Data Protection?*, cit., 275 ss., at 280.

[22] Y. Suda, *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy*, New York, 2018, 31.

[23] M.P. Granger-K. Irion, *The right to protection of personal data: the new posterchild of European Union citizenship?*, in S. De Vries-H. De Waele-M.P. Granger (eds), *Civil Rights and EU Citizenship. Challenges at the Crossroads of the European, National and Private Spheres*, Cheltenham, 2018, 279 ss., at 281.

[24] J. Hildén, *The Politics of Datafication: The Influence of Lobbyists on the EU's Data Protection Reform and its Consequences for the Legitimacy of the General Data Protection Regulation*, Helsinki, 2019, 71 and 94; M. Laurer-T. Seidl, *Regulating the European Data Driven Economy: A Case Study on the General Data Protection Regulation*, in *Policy & Internet*, 2020, 257 ss., at 265.

[25] On the GDPR, see for instance: C. Kuner-L.A. Bygrave-C. Docksey (eds), *The EU*

reference to the rules on transfers of personal data to non-EU States, included in Chapter V: in principle, transferring personal data outside the EU is prohibited; nevertheless, flows are allowed in presence of a numerus clausus of conditions: the "adequacy decision" (art. 45) adopted by the Commission towards a third country that «ensures an adequate level of protection»; the "appropriate safeguards" (art. 46), contractual arrangements between the exporter and the importer of the data, such as standard contractual clauses (SCCs), ad hoc contractual clauses and binding corporate rules (BCRs); and to "derogations for specific situations" (art. 49), such as the explicit consent of the data subject or the necessity of the transfer for specific purposes. At first glance, such legal framework is similar to the one of Directive 95/46/CE. However, the provisions of the GDPR are much more detailed, complete and robust: therefore, it becomes increasingly difficult to transfer personal data to third countries where EU protection standards are not met.

Furthermore, the rules at stake acquired an even clearer connotation thanks to the activity of Article 29 Working Party – replaced, under the GDPR, by the European Data Protection Board (EDPB) – and, above all, thanks to the case law of the CJEU.

Firstly, with reference to the adequacy decision, the Court elevates the standard of "adequacy" by requiring the third country to ensure a level of protection that is "essentially equivalent" to that guaranteed within the EU by the relevant legal framework read in the light of the CFREU[26]. Such reading, in the context of the "Schrems saga", implied the invalidation of two adequacy decisions concerning the US, known as "Safe Harbor" (2000)[27] and "Privacy Shield" (2016)[28], respectively by Schrems I ruling (6 October 2015)[29] and Schrems II ruling (20 July 2020)[30].

Secondly, the CJEU has also intervened on appropriate safeguards (to be used in absence of an adequacy decision). From the text of the GDPR, it already appears that these are intrinsically limited and can be only used in circumscribed situations[31]. Moreover, the Court – once again in Schrems II ruling – specifies that even such guarantees must ensure that transfer-

General Data Protection Regulation (GDPR): A Commentary, Oxford, 2020; G. Comandé-G. Malgieri (eds), *Manuale per il trattamento dei dati personali. Le opportunità e le sfide del nuovo regolamento europeo sulla privacy*, Milan, 2018.

[26] On the point, see for instance: O. Pollicino-M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in G. Resta-V. Zeno-Zencovich (eds), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Rome, 2016, 73 ss.

[27] Commission Decision 2000/520/EC.

[28] Commission Implementing Decision (EU) 2016/1250.

[29] CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (2015).

[30] CJEU, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems* (2020).

[31] On the limits of appropriate safeguards, see for instance: G.M. Riccio, *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in G. Resta-V. Zeno-Zencovich (eds), *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield"*, Rome, 2016, 215 ss.; A. Mattoo-J.P. Meltzer, *International Data Flows and Privacy: The Conflict and Its Resolution*, in *Journal of International Economic Law*, 21(4), 2018, 769 ss.

red data benefit from a protection "essentially equivalent" to that of the EU; this might require the adoption of "supplementary measures" by the data controller. If the necessary protection still cannot be guaranteed, the controller or – failing that – the competent supervisory authority, must suspend or end the transfer. In other words, the CJEU aims at avoiding safeguards being used as mere legal fictions and transforms them into «mini adequacy decisions»[32].

Thirdly, the Court has dealt even with derogations for specific situations, true "safety valves" for circumstances where the protection is not adequate, but the risks are small, or there is an overriding societal interest[33]. According to the CJEU, like all derogations and limitations to fundamental rights, they apply only in so far as it is strictly necessary[34].

Given the extremely high level of protection required by the GDPR and by the case law of the Court, the Commission also has generally been cautious on the matter. In particular, with regard to adequacy decisions, DG JUST (the DG in charge) has recognised only 15 non-EU States as "adequate"[35].

In summary, as anticipated, it can be stated that the current EU internal legal framework concerning flows of personal data to third countries – as designed by the EU legislators in the GDPR, as interpreted by the CJEU in its rulings and as implemented by the Commission through the adoption of some of its acts – gives top priority to the fundamental right to the protection of personal data. This often happens at the expense of the need to favour international transfers for commercial reasons.

2.2. The purposes of the current EU internal legal framework

The human rights-oriented approach described above has several aims. First of all, EU institutions want to prevent data flows from undermining the level of protection guaranteed in Europe by the GDPR: strengthening the position of data subjects in the Union would be useless if it was possible to easily avoid EU rules by transferring personal data to third countries.

However, there are even other objectives. The EU has also the explicitly

[32] C. Kuner, *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, in *European Law Blog*, 2020.

[33] C. Kuner, *Article 49. Derogations for specific situations*, in C. Kuner-L.A. Bygrave-C. Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*, cit., 841 ss., at 843.

[34] CJEU, Joint Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung and others* (2014), § 52; CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (2015), § 92.

[35] The European Commission has so far recognised Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, the United States and Uruguay as providing adequate protection.

stated aim to export its high data protection standards towards the largest possible number of third countries. If the latter wish to allow entities within their territories, in particular companies, to receive personal data from the EU and to have access to the EU market, such States will have to adopt and implement EU-conformant data protection laws[36].

This is a clear example of the Brussels effect, i.e. the ability of the EU to unilaterally influence third countries' regulations through its central position in the global economy. Such influence is possible because in the EU, with reference to this field, specific conditions occur: a large internal market; a substantial regulatory capacity; the preference for strict rules; the predisposition to regulate "inelastic targets", such as data subjects ("inelastic" means that they cannot be "moved" to another jurisdiction to circumvent the rules); and the "nondivisibility" of standards (which means that it is not possible to comply with such standards only in the relations with the EU; on the contrary, once adopted, they must be applied worldwide)[37].

The intention to export EU data protection standards was one of the reasons that led to the adoption of the new legal framework. After some years since the entry into force of the GDPR, it is now possible to state that the results achieved are relevant: according not only to the Commission, but also to important authors, the Regulation emerged as a key reference point at international level and inspired a great number of third countries[38].

The exportation of EU data protection standards is also pursued in other ways. This contribution focuses on Chapter V GDPR, but even art. 3 of the GDPR itself, concerning the territorial scope of the Regulation, has a significant role: such provision requires the single foreign entities that target the EU market to respect the GDPR in its entirety[39]. The final aim, therefore, is the same: the extension of EU safeguards beyond the borders of the EU itself. Such extension, moreover, can be not only unilateral (through the GDPR), but also multilateral: in this perspective, the EU is promoting as much as possible the accession to CoE Convention 108+, the provisions of which are often very similar to the ones of Regulation (EU) 2016/679.

---

[36] W. Höglund, *Exporting data protection law. The extraterritorial reach of the GDPR*, Umeå, 2018, 26. On the point see also: S.A. Aaronson-P. Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law*, 21(2), 2018, 245 ss.; K. Irion-M. Burri-A. Kolk-S. Milan, *Governing "European values" inside data flows: Interdisciplinary perspectives*, in *Internet Policy Review*, 10(3), 2021.

[37] A. Bradford, *The Brussels Effect*, in *Northwestern University Law Review*, 107(1), 2012, 1 ss.; A. Bradford, *The Brussels effect: How the European Union rules the world*, Oxford, 2020.

[38] Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, 24 June 2020, COM (2020) 264 final; G. Greenleaf, *Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance*, in *Privacy Laws & Business International Report*, 2021; G. Greenleaf, *Now 157 Countries: Twelve Data Privacy Laws in 2021/22*, in *Privacy Laws & Business International Report*, 2022; G. Greenleaf, *Global data privacy laws 2023: 162 national laws and 20 Bills*, in *Privacy Laws & Business International Report*, 2023.

[39] On the point see, for instance: O.J. Gstrein-A.J. Zwitter, *Extraterritorial application of the GDPR: promoting European values or power?*, in *Internet Policy Review*, 10(3), 2021, 1 ss.

The abovementioned exportation of EU principles towards third countries has, in turn, multiple objectives.
Firstly, there is the pure and simple will to promote fundamental rights globally. This is perfectly consistent with the aims of the EU external action: the latter, according to art. 21 TEU, seeks to advance in the wider world the principles which have inspired the creation, development and enlargement of the Union.
Secondly, there is also a strategic aim, i.e. trying to confer a competitive advantage to EU enterprises over non-EU competitors. While the former can maintain their approach with regard to data protection, the latter will be forced to conform to the most demanding EU standards: they will have to change their business practices, incurring related costs. The alternative would be not being able to receive and process EU data, the value of which would benefit only European firms: even in this case, therefore, such companies would obtain a competitive advantage[40].
It is clear that what until now has been constantly defined as a conflict between the protection of fundamental rights, on the one hand, and commercial needs, on the other, is in truth much more complex. Even behind personal data protection and the subsequent limitation of data flows, indeed, lie economic reasons, consisting precisely in the will to give a benefit to EU enterprises, protecting them from the fierce competition of companies based in third countries, in particular in the US, but not only.
Before concluding this part of the contribution, however, we must highlight that it is also possible to notice certain elements which could undermine the above-described EU approach. Indeed, while it is true that the Commission has generally been very cautious in adopting adequacy decisions, and that most of the 15 measures do not raise relevant problems, it is also true that some decisions, in particular those concerning important trading partners of the EU, raise critical questions: they seem more motivated by economic interests than by a real "adequacy" of the protection in the countries at stake; for this reason, in order to adopt them, the Commission had to figure out creative solutions, such as "sector-specific" decisions (i.e. decisions only concerning certain sectors of the economy of a non-EU State)[41]. We refer to cases such as those of Canada, Israel, Japan, South Korea, the United Kingdom and also the United States: despite the invalidation of the "Safe Harbor" and of the "Privacy Shield", the European Commission adopted a third measure, better known as "EU-US Data Privacy Framework", in 2023[42]. We will come back to the adequacy decisions concerning these countries, and to the impact they can have on the previously described approach.

[40] On the economic advantages enjoyed by countries that are concerned by adequacy decisions compared to those that are not, see for instance: M.F. Ferracane.-B. Hoekman-E. Van Der Marel-F. Santi, *Digital Trade, Data Protection and EU Adequacy Decisions – RSC Working Paper 2023/37*, Florence, 2023.

[41] Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, 10 January 2017, COM (2017) 7 final.

[42] Commission Implementing Decision (EU) 2023/1795.

3. The interplay between the EU legal framework and EU international commitments in the field of trade law

Given the above, as anticipated, the paper will now explain that certain international commitments made by the EU in the field of trade law – some concerning in general the liberalisation of trade in services, some others devoted more specifically to data flows – are not consistent with the described approach and with its purposes. In particular, it will be highlighted that the rules binding the EU in the field of international trade law give clear priority to the need to transfer data, creating issues of consistency with the approach of the EU internal legal framework.

3.1. EU international commitments concerning the liberalisation of trade in services in general

Starting from WTO Law, particular attention should be given to the General Agreement on Trade in Services (GATS), aimed at the liberalisation of trade in services, which sometimes are supplied across borders and often consist in data flows[43]. The GATS requires the removal, as much as it is feasible, of prohibitions or limitations to data transfers, circumstance that could lead to frictions between the Agreement and the EU legal framework on personal data flows. For this reason, it is important to verify if the latter is consistent with the former through a two-step analysis. Firstly, we should verify if EU rules might be in conflict with existing GATS obligations and commitments. Secondly, if prima facie violations are possible, we should try to understand whether they can be justified under one of the exceptions provided by the GATS itself[44]. To date, there has never been a WTO procedure challenging the EU legal framework at stake; however, some reports of WTO bodies can be extremely useful in the investigation[45].

The analysis should start from the most relevant among the "General Obligations" of the GATS, i.e. the "Most-Favoured-Nation" (MFN) Tre-

[43] On the point, see for instance: P. Picone-A. Ligustro, *Diritto dell'organizzazione mondiale del commercio*, Padova, 2002, 367-368.

[44] On the point, see for instance: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements*, Amsterdam, 2016, 26.

[45] In particular, we refer to: WTO, European Communities – Regime for the Importation, Sale and Distribution of Bananas. Report of the Appellate Body, 9 September 1997, WT/DS27/AB/R; WTO, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body, 7 April 2005, WT/DS285/AB/R; WTO, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products. Report of the Appellate Body, 21 December 2009, WT/DS363/AB/R; WTO, Argentina – Measures Relating to Trade in Goods and Services. Report of the Appellate Body, 14 April 2016, WT/DS453/AB/R.

atment of art. II. The EU legal framework accords to services and service suppliers of some WTO Members (the ones which are not concerned by an adequacy decision) a treatment less favourable than the one it accords to like services and service suppliers of other countries (which, instead, benefit from the abovementioned measure): a violation of the MFN clause, at least prima facie, is therefore conceivable[46].

With regard to other General Obligations, it is also possible to assume infringements of the rules on "Domestic Regulation". According to art. VI.1, all measures of general application affecting trade in services must be administered in a reasonable, objective and impartial manner. If it is true that the EU legislation as such cannot be in conflict with the obligation in question, it is also true that there could be violations at the application level[47]. In particular, the practice of the Commission in the adoption of adequacy decisions is not always reasonable, objective and impartial (non-EU States with similar data protection standards are sometimes treated differently, maybe due to political reasons)[48], circumstance that could trigger the application of art. VI.1.

In the GATS there are also "Specific Commitments", that bind only WTO Members which manifested the will to further liberalise certain categories of services; the EU has actually made similar commitments also in sectors that involve the processing – and the transferring – of personal data[49]. In such sectors, it is possible to conceive a violation of the rules on "National Treatment" (art. XVII): indeed, it could be stated that the EU legal framework accords to services and service suppliers of some WTO Members (the ones which are not concerned by an adequacy decision) a treatment less favourable than the one it accords to domestic like services and service suppliers[50]. Moreover, in the case of a total suspension of personal data flows to a third country, there would be a "zero quota", i.e. a form of quantitative restriction which is prohibited by the rules on "Market Access" (art. XVI)[51]: a violation of the latter, albeit unlikely, is abstractly possible.

---

[46] C.L. Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, in *Melbourne Journal of International Law*, 12(1), 2011, 1 ss., at 16; K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., 30; F. Velli, *The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements*, in *European Papers*, 4(3), 2019, 881 ss., at 884-885.

[47] See for instance: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., 31.

[48] C. Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, in S. Gutwirth-Y. Poullet-P. De Hert-C. De Terwangne-S. Nouwt (eds), *Reinventing Data Protection?*, cit., 263 ss., at 271.

[49] WTO, European Union Schedule of Specific Commitments, 7 May 2019, GATS/SC/157; WTO, European Union Schedule of Specific Commitments. Supplement 1, 27 February 2024, GATS/SC/157/Suppl.1.

[50] See for instance: S. Yakovleva-K. Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, in *European Data Protection Law Review*, 2(2), 2016, 191 ss., at 204; K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., 32-33; F. Velli, *The Issue of Data Protection in EU Trade Commitments*, cit., 886.

[51] See for instance: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., 32.

Since EU rules on personal data flows (or their application) can be in conflict, at least prima facie, with several obligations and commitments enshrined in the GATS, the question is whether such violations can be justified under one of the exceptions of the GATS itself.

The first exception to consider is "Economic Integration": art. V GATS allows its Members to be a party of or to enter into an agreement liberalising trade in services between or among the parties to such an agreement. Such provision would likely be the first line of defence for the EU if an EU measure were found to treat less favourably a WTO Member State as compared to an EU Member State[52]. However, it would not help in the case of the less favourable treatment accorded to services and service suppliers from those members of the WTO (but not of the EU) that did not obtain an adequacy decision, compared to the treatment accorded to like services and service suppliers from members of the WTO (but not of the EU) that, instead, have benefited from such measure.

As a second line of defence, one could invoke the "General Exceptions" (art. XIV). Art. XIV.c.ii provides for an exception concerning measures which are necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of the GATS, including those relating to «the protection of the privacy of individuals in relation to the processing and dissemination of personal data». At a first reading, this article seems able to protect the EU from any possible claim. However, a more nuanced analysis of the article, and of the case law of WTO bodies regarding General Exceptions, paints a less positive picture.

Preliminarily, it would be difficult for the EU to demonstrate that the adopted measures are "necessary" to secure compliance with the abovementioned laws or regulations. As stated by WTO bodies, the less restrictive the measure and the greater the contribution to the enforcement of public interest the more likely it is that the measure in question will meet the "necessity test"[53]. In this respect, the EU legal framework on personal data flows shows some weaknesses that might make the outcome of a possible procedure uncertain. In particular, the fact that two adequacy decisions were criticised for their lack of effectiveness, and then invalidated by the CJEU, could seriously question the real contribution of similar measures to the achievement of the aim pursued[54]. Moreover, the complaining party could try to demonstrate that a less trade-restrictive alternative was reasonably available. As well known, there are other international legal frameworks that have a less negative impact on trade in services, being more sensitive to commercial needs: e.g., the OECD Guidelines and the APEC Privacy Framework. If WTO bodies were convinced that such less restrictive alternatives could achieve the same objectives, the EU legal framework would certainly fail the necessity test[55].

---

[52] K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., 33.

[53] WTO, Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef. Report of the Appellate Body, 11 December 2000, WT/DS161/AB/R, WT/DS169/AB/R, paras 162-163.

[54] See for instance: K. Irion-S. Yakovleva-M. Bartl, *Trade and Privacy: Complicated Bedfellows?*, cit., 35-37.

[55] See for instance: S. Yakovleva-K. Irion, *Pitching trade against privacy: reconciling EU*

But even if the abovementioned test was met, there would still be a further test, i.e. to assess whether the conditions set out in the introductory "chapeau" of art. XIV are met. Such "chapeau" requires that the exceptionally permitted measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services: such a standard is interpreted by WTO bodies as «consistency of enforcement» of the challenged measure[56].
The EU's ability to demonstrate that the conditions of the "chapeau" are met must not be taken for granted. A well-founded criticism could relate to the already mentioned adoption of "sector-specific" adequacy decisions. With regard to non-EU States whose legal systems do not fully guarantee an adequate level of protection, sometimes creative solutions have been sought to partially cover such systems (Canada, Israel, Japan, South Korea, UK, US); at other times, no adequacy decision was adopted, a circumstance that affects services and service suppliers of the countries at stake (e.g. Australia). Thus, WTO bodies could consider the practice used by the Commission in adopting adequacy decisions as "inconsistent": in that case, the conditions of the chapeau could not be satisfied, and it would be impossible to justify any violation of the GATS committed by the EU. Therefore, the approach of WTO Law, which gives great relevance to the expansion of international trade, diverges considerably from the restrictive approach which characterises the EU legal framework on personal data transfers to third countries. The latter could consequently be in conflict with several provisions of the GATS, and it would be extremely difficult to justify such violations in the case of a proceeding before WTO bodies. This means that the EU could incur a negative ruling and all the related consequences, which would imply a predominance of free flows over data protection.

3.2. Data flows commitments included in some EU international trade agreements

It is now necessary to focus on the interplay between the EU rules on personal data transfers and certain provisions that the EU has included in some of its international trade agreements and that represent commitments to allow the flow of information ("data flows commitments"); such commitments, which are aimed at promoting data transfers because of their importance for global commerce, are counterbalanced by provisions designed to safeguard the rights to privacy and to the protection of personal data ("data protection provisions").
The first instruments in which articles of this kind have been inserted are the Understanding on Commitments in Financial Services and the Annex

governance of personal data flows with external trade, in *International Data Privacy Law*, 10(3), 2020, 201 ss., at 212.

[56] WTO, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services. Report of the Appellate Body, cit., para 351.

on Telecommunications: they contain data flows commitments accompanied by data protection provisions, which are formulated as exceptions. The Understanding and the Annex, despite being multilateral in nature and part of WTO Law, introduced a solution that was later adopted in other contexts.

Indeed, it is possible to find similar articles also in some of the bilateral agreements subsequently concluded by the EU outside of the legal framework of the WTO. We refer to the Free Trade Agreements (FTAs), and more in general to the bilateral treaties having (at least partially) commercial nature concluded between the Union and third countries[57]. Since the turn of the millennium, in fact, the EU started to make a massive use of such instruments, also given the difficulties in multilateral negotiations within the WTO[58].

The abovementioned agreements include rules concerning trade in services that reproduce GATS obligations, such as the National Treatment, Most-Favoured-Nation Treatment and Market Access, but also data flows commitments accompanied by data protection provisions, as in the Understanding and in the Annex.

Those articles as well concern financial and telecommunication services. It is not surprising: the financial services sector is one of the most pertinent sectors for digital economy[59], but it also raises significant issues and the public is particularly concerned about the processing of personal financial data[60]. Similar considerations also apply to the telecommunication services sector: its importance for the digital economy is unquestionable, but its intensive use of data increases the demand of an appropriate protection[61].

The provisions described above can be found in the Comprehensive Economic and Trade Agreement (CETA) with Canada, but also in other EU trade agreements, such as the ones with South Korea, Colombia-Peru-Ecuador, Central America, Ukraine, Japan (Economic Partnership Agreement or EPA), Singapore and Viet Nam.

However, the data flows commitments and the data protection provisions included in the cited instruments raise critical issues. Some concern the mere presence of similar articles in the agreements concluded by the EU. DG TRADE (the DG of the Commission in charge) negotiates trade agreements in compliance with the mandates of the Council (arts. 207

---

[57] On EU trade agreements, see for instance: L. Pasquali, *The EU-MERCOSUR Agreement as Source of Development of Specific Global Norms and Standards*, in C. García Segura-J. Ibáñez-P. Pareja (eds), *Actores Regionales y Normas Globales: la Unión Europea y los BRICS como Actores Normativos*, Valencia, 2021, 131 ss.

[58] See for instance: S. Woolcock, *European Union policy towards Free Trade Agreements, ECIPE Working Paper No. 3 – European Centre for International Political Economy*, 2007; I. Bosse-Platière-C. Rapoport, *Negotiating and implementing EU free trade agreements in an uncertain environment*, in I. Bosse-Platière-C. Rapoport (eds), *The Conclusion and Implementation of EU Free Trade Agreements. Constitutional Challenges*, Cheltenham, 2019, 1 ss.

[59] M. Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, in *University of California Davis Law Review*, 51, 2017, 65 ss., at 83.

[60] A. Sousa De Jesus, *Data Protection in EU Financial Services – ECRI Research Report No. 6*, 2004, 4.

[61] See for instance: E. Van Der Marel, *Disentangling the Flows of Data: Inside or Outside the Multinational Company? – ECIPE OCCASIONAL PAPER No. 7*, 2015, 2.

and 218 TFEU). However, the mandates concerning the abovementioned agreements did not mention privacy or data protection. On this point, the former European Data Protection Supervisor (EDPS) Giovanni Buttarelli stated that it is «not fully clear as to what extent the Commission has the mandate to negotiate provisions that may have an effect on data protection»[62].

In truth, the absence of such references is not a coincidence. It is the result of the will to make those aspects non-negotiable[63]: dialogues with third countries on data protection and trade negotiations should consequently follow separate tracks[64]. Nevertheless, in the abovementioned agreements, there are provisions that undoubtedly affect privacy and data protection: a circumstance which represents a real problem.

Other issues concern the concrete formulation of the articles in question. In truth, there were some improvements over time, not so much in data flows commitments, which basically remain unchanged, but rather in data protection provisions. In the Understanding and in the Annex, these are formulated as exceptions that can be triggered on an optional basis and that require strict conditions to be met in order to be activated. On the contrary, in the bilateral agreements recently concluded by the EU such provisions are usually formulated as positive obligations to adopt or maintain "adequate safeguards" to protect the rights at stake: a clear step forward[65]. However, some problems remain: in particular, such safeguards must still comply with several limits and conditions, since the respect of trade obligations remains the priority[66].

Another consideration concerns the fact that the safeguards must be "adequate". Such term, as interpreted by the CJEU, ensures a protection which is extremely high ("essentially equivalent" to that of the EU): this is because the Court interprets it in the light of the CFREU, as explained.

However, the settlement of the disputes concerning the interpretation of trade agreements does not fall within the jurisdiction of the CJEU, but of supranational bodies established by such agreements: the latter, in case of a dispute, are not obliged at all to interpret the "adequate safeguards" in the light of the CFREU[67]. The same terminology does not imply the same

---

[62] European Data Protection Supervisor, *Trade agreements and data flows – Joint hearing of the INTA and LIBE committees – European Parliament*, 2015, 2.

[63] Jean-Claude Juncker, *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change – Political Guidelines for the next European Commission*, Strasbourg, 2014, para 6.

[64] Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, cit., para 3.1.

[65] A. Wessel, *Broken data protection in EU trade agreements*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 2016, para 4; S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., 493-495; A. Bendiek-M. Römer, *Externalizing Europe: the global effects of European data protection*, in *Digital Policy, Regulation and Governance*, 2018.

[66] With particular reference to art. 8.54 of the EU-Singapore FTA, see for instance: A. Wessel, *EU-Singapore Trade Agreement not compatible with EU data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 2018.

[67] On the point, with particular reference to art. 13.15 of the EU-Canada CETA, see: A. Wessel, *CETA will harm our privacy*, in *Foundation for a Free Information Infrastructure (FFII)*

meaning: the "adequacy" in EU bilateral trade agreements has «no precise obligational content»[68], and is likely to provide a lower protection than the "adequacy" stated by the CJEU in the context of the Schrems saga[69].
Moreover, the adjudicators established by trade agreements will unlikely give the due weight to the protection of fundamental rights. As authoritatively stated, specialist courts and tribunals tend to become over-enthusiastic about defending the purpose for which they were set up[70], which in this case is progressive trade liberalisation, that prevails over competing interests given the object and purpose of the agreement[71].
In brief, the rules contained in the trade agreements of the EU give clear priority to the needs of international trade: in order to favour the latter, the Union made several data flows commitments, counterbalanced by data protection provisions whose scope and effectiveness are at least questionable. This might create problems of coordination with the approach of the EU internal legal framework on data transfers, which is much more attentive to the protection of individuals.

3.3. The impact of the EU international commitments on the EU legal framework

This paper has so far shown that certain international commitments of the Union in the field of trade law are not consistent with the EU internal legal framework. This section of the article will also analyse the consequences of the divergence between the two approaches, and whether one can affect the other. In particular, it will be demonstrated that the approach of EU trade commitments seriously risks undermining the one of the EU internal legal framework.
Preliminarily, it is important to emphasise that, in the light of the text of international trade agreements and of the case law of the CJEU, it is unlikely that trade agreements themselves and the decisions of international trade adjudicating bodies will have direct effect in the EU[72]. Thus,

Blog, 2016.

[68] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., 495.

[69] A. Wessel, *CETA will harm our privacy*, cit.. See also: A. Wessel, *CETA: ISDS and data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 2016.

[70] A. Wessel, *Broken data protection in EU trade agreements*, cit.

[71] S. Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, cit., 495.

[72] See for instance: A. Semertzi, *The Preclusion of Direct Effect in the Recently Concluded EU Free Trade Agreements*, in *Common Market Law Review*, 51(4), 2014, 1125 ss., spec. 1132-1135; S. Yakovleva-K. Irion, *The Best of Both Worlds?*, cit., 200-202; S. Yakovleva, *Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'*, in *The Journal of World Investment & Trade*, 21(6), 2020, 881 ss., at 889. In many cases, the direct effect is excluded by the provisions of the agreements themselves (e.g. art. 23.5 of the EU-Japan EPA, art. 16.16 of the EU-Singapore FTA, art. 17.20 of the EU-Viet Nam FTA). In other cases, it is excluded by the case law of the Court of Justice; e.g., with reference to WTO rulings, see: CJEU, C-120/06, *P FIAMM and Others v. Council and Commission* (2008), §§ 129-131. On the direct effect of EU international agreements, see also: F. Martines, *Direct Effect of*

they cannot be invoked before national courts by individuals; moreover, if they are violated by an EU legislative act, the latter cannot be invalidated on such reason.

However, there might be other relevant aftermaths. The absence of direct effect does not make the EU's obligations under international trade law less binding from an international law perspective. Under international law, the EU must perform its obligations in good faith. Otherwise, the EU may face liability and legal consequences, even if the compliance with trade commitments is not possible due to constraints contained in EU law[73].

More specifically, before supranational dispute settlement bodies, one could argue that, by limiting data flows, the Union has violated its obligations: we refer not only to "explicit" data flows commitments, but also to "implicit" ones, i.e. the already mentioned general rules on trade in services (National Treatment, Most-Favoured-Nation Treatment, Market Access)[74]. And, if supranational bodies were convinced by the claim, the EU would face legal consequences, such as countermeasures and financial penalties.

The fear of such consequences could determine a heavy pressure on several institutional players, and theoretically could undermine their independence in protecting personal data. Firstly, national supervisory authorities could be induced not to exercise their power, enshrined in art. 58 GDPR, to suspend or end data flows towards third countries even when the latter do not guarantee the level of protection requested by EU law. Moreover, even if this has not happened yet, in the future the CJEU could eventually be discouraged from invalidating other adequacy decisions.

However, the main concerns regard the Commission's approach: indeed, fearing the consequences of breaching trade commitments, it could be induced to adopt an adequacy decision even in the absence of a level of protection "essentially equivalent" to that of the EU. And, in truth, there are reasons to believe that this has already happened.

We have already mentioned that the Commission has adopted some decisions, concerning in particular important EU trading partners, that seem motivated more by economic interests than by a real "adequacy" of the protection. Given the impossibility to recognise as "adequate" the legal systems of those States, at least in their entirety, the Commission had to figure out creative solutions, such as "sector-specific" decisions.

An example is the decision concerning Canada, that covers only data transfers to recipients subject to the Personal Information Protection and Electronic Documents Act (PIPEDA), i.e. private sector organisations that collect, use or disclose personal information in the course of commercial activities[75]; but also the one concerning Israel, that does not apply to international transfers of personal data from the EU to such coun-

International Agreements of the European Union, in *The European Journal of International Law*, 25(1), 2014, 129 ss.

[73] S. Yakovleva, *Personal Data Transfers in International Trade and EU* Law, cit., 899.

[74] On the point, with particular reference to the EU-Japan EPA, see: A. Wessel, *EU-Japan trade agreement not compatible with EU data protection*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 2018.

[75] Commission Decision 2002/2/EC.

try when the transfer and the subsequent data processing are carried out exclusively through non-automated means[76].

The case of Japan is even more emblematic. Firstly, it was necessary to adopt a sector-specific decision[77] that only covers transfers to personal information handling business operators subject to the so-called "APPI" (Act on the Protection of Personal Information). Secondly, above all, Japan had to complete its legal system with "Supplementary Rules" which are only applicable to personal data transferred from the EU; on the contrary, they do not apply to personal data of individuals in Japan or coming from non-EU countries. An approach that did not convince the EDPB[78] and the European Parliament[79] that did not give a favourable opinion on the point. The same criticisms, i.e. the limited scope of the adequacy assessment and the presence of "Supplementary Rules", also concern the South Korea adequacy decision[80], although to a lesser extent[81].

It was necessary to find a creative solution also with regard to the UK. The Commission excluded from the ambit of the relevant decision[82] any personal data transfer from the EU to the UK falling within the too broad "immigration exemption" provided by the UK legal framework. This was done in response to some of the critical remarks formulated by the EDPB[83] and by the European Parliament[84].

Similar adequacy assessments raise questions about their operational implementation. In the case of Japan there is the concrete risk of circumvention of the Supplementary Rules, while there is the fear that personal data transferred from the EU to the UK can still be subject, in some cases, to the "immigration exemption", circumstance that would cause an excessive restriction of the rights of data subjects[85].

Finally, among the "creative" adequacy decisions there is also the EU-US Data Privacy Framework: the latter, just like the two previous measures concerning the US, allows data transfers from the EU to organisations in the US that voluntarily commit to a set of privacy principles. The Com-

---

[76] Commission Decision 2011/61/EU.

[77] Commission Implementing Decision (EU) 2019/419.

[78] European Data Protection Board, *Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan*, 2018.

[79] European Parliament, *Resolution on the adequacy of the protection of personal data afforded by Japan (2018/2979(RSP))*, 2018.

[80] Commission Implementing Decision (EU) 2022/254.

[81] See for instance: G. Greenleaf, *The Draft Korea Adequacy Decision: Submission to European Union Authorities*, in *University of New South Wales Law Research Series*, 52, 2021.

[82] Commission Implementing Decision (EU) 2021/1772.

[83] European Data Protection Board, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, 2021.

[84] European Parliament, *Resolution on the adequate protection of personal data by the United Kingdom (2021/2594(RSP))*, 2021.

[85] On the point, with reference to Japan, see: European Data Protection Board, Opinion 28/2018, cit., para 30; with reference to the United Kingdom, see: A. Choromidou, *EU data protection under the TCA: the UK adequacy decision and the twin GDPRS*, in *International Data Privacy Law*, 2021.

mission has already carried out a first review of the Data Privacy Framework, with a positive outcome[86]; nevertheless, the EDPB invited it to continue its monitoring activity[87].

As anticipated, the adoption of the adequacy decisions falling in the above-described category often took place under heavy pressure, caused by the fear of negative commercial consequences, and, in some cases, things were done rather rapidly.

This happened in the case of Japan. The Commission hastened to adopt the decision at stake on the 23rd January 2019, so that it could precede the entry into force of the EPA which occurred on the 1st February 2019 (a few days later). This avoided any possible violation of EU commitments caused by the limitation of data flows towards Japan. A similar adequacy assessment, however, is the result of a compromise, and someone stated that, in the occasion, the Commission did not act in an independent manner[88]. The latter, moreover, decided to confirm the decision in 2023[89], an action on which the EDPB did not refrain from making observations[90].

Something similar happened also with reference to the UK. According to the EU-UK Trade and Cooperation Agreement (TCA), concluded in 2020, after the 30th June 2021 transmissions of personal data from the Union to the UK were considered as full-fledged transfers to a third country (art. 782), with the consequent need – in the absence of an adequacy decision – to apply the alternative mechanisms of Chapter V GDPR. In order to avoid such scenario, which could have led to possible violations of the commitments made by the EU in the TCA (to which we will return later), the Commission accelerated in the adoption of the adequacy decision concerning the UK, that occurred on the 28th June 2021 (just two days before the deadline).

The necessity to quickly adopt similar decisions induced the Commission not only to rely on creative solutions (as described), without which it would have been impossible to approve any kind of measure, but also not to take into sufficient account some critical aspects highlighted by the EDPB and by the European Parliament. One is the issue of access to personal data by public authorities for surveillance reasons: a crucial problem of the Schrems saga, that continues to worry with regard to the US[91] and

---

[86] Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, 9 October 2024, COM (2024) 451 final.

[87] European Data Protection Board, *EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 2024.

[88] A. Wessel, *EU-Japan trade agreement not compatible with EU data protection*, cit..

[89] Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decision for Japan, 3 April 2023, COM (2023) 275 final.

[90] European Data Protection Board, *Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan*, 2023.

[91] European Data Protection Board, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 2023.

turns out to be critical also with reference to other countries, e.g. the UK.
A further consideration can be added. The Commission, due to the already mentioned fear of the consequences deriving from a violation of trade commitments, could be induced not to repeal, amend or suspend an already adopted adequacy decision, even if the country at stake no longer ensures a protection "essentially equivalent" to that of the EU.
Two examples of this risk are represented by the measures concerning Canada and New Zealand[92]. Such countries are two of the so-called "Five Eyes", together with the UK and the US themselves, and also with Australia, a group of countries committed to mass surveillance programs[93]. The structure of their legal systems gives priority to State security over privacy[94]. Therefore, in the decisions concerning Canada and New Zealand, one would expect a significant attention to the issue of access to personal data by public authorities.
On the contrary, the abovementioned instruments, adopted under Directive 95/46/EC, are not only outdated, but also extremely brief and bare, especially if compared to more recent adequacy decisions. Thus, it would be appropriate to reconsider them, perhaps adopting further precautions to ensure more convincingly that surveillance by public authorities does not cause disproportionate interferences with data subjects' rights. However, this has not yet occurred; on the contrary, in 2024 the Commission decided to confirm the 11 oldest decisions in force, including those two[95]; an operation that was met with some reservations by the EDPB[96]. The reasons are not difficult to understand: e.g., repealing the decision concerning Canada could determine easily foreseeable consequences, since the EU could end up violating some of the obligations included in the CETA.
Adopting or maintaining adequacy decisions concerning States that do not ensure a protection «essentially equivalent» to that of the EU, due to the pressure caused by trade commitments, ends up undermining the approach of the EU legal framework, meant to give priority to the protection of personal data. This also affects the aims of such approach, including the one to export EU standards towards third countries (the "Brussels effect"), and everything that comes with it.
In truth, if the Union ceased completely to adopt adequacy decisions, the purpose of exporting the EU model would be undermined all the same. Indeed, if it was de facto impossible to obtain a similar measure, non-EU countries would not even try to modify their legal frameworks to raise the protection, since that effort would be meaningless. The model at stake

---

92 Commission Implementing Decision 2013/65/EU.

93 See for instance: O. Tene, *The show must go on*, in *iapp.org*, 2020.

94 M. Nino, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 14(3), 2020, 733 ss., at 752-753. See also: A. Wessel, *CETA and mass surveillance*, in *Foundation for a Free Information Infrastructure (FFII) Blog*, 2016.

95 Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC, 15 January 2024, COM (2024) 7 final.

96 European Data Protection Board, *EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC*, 2024.

would not function properly, and other States would unlikely try to imitate it. The latter could even embrace different models, in particular the OECD and APEC ones, that adopt a less restrictive and more free-trade-centred approach: unsurprisingly, they are promoted by the US, that are trying to oppose the role of the GDPR as "international rule-setter" with instruments which are more suitable for their own needs[97]. If the Commission wants to avoid such risk, it must continue to make adequacy assessments, and it cannot adopt a too rigid approach that leads to immobility.

However, such argument cannot justify the adoption of decisions towards countries that surely do not ensure an "adequate" protection. In that case, the Commission would not only seriously endanger Europeans' personal data, but also give up exporting EU standards, allowing third countries to receive data flows even without (sufficiently) raising their protection[98].

The case of Japan is symbolic. The Supplementary Rules, without which it would have been impossible to adopt any kind of adequacy decision, are only applicable to personal data transferred from the EU. It has already been said that there are doubts concerning the operational implementation of a similar system. Even assuming it can work, in any case the EU has given up fully exporting its standards towards Japan: the higher protection only concerns "European" data, while the partner country can still maintain lower safeguards with regard to other personal data. The conditions of the "Brussels effect" would be lacking, since one of the requirements is the "nondivisibility" of standards, and this makes it unlikely that Japan will move significantly closer towards an EU-style data privacy framework[99].

On the contrary, in the case of the US, the uncompromising approach of the CJEU could bring some results. In 2015, the Freedom Act introduced some modifications (that turned up not to be decisive) which tried to reduce surveillance powers of public authorities. More recently, after the Schrems II ruling, there were several exhortations to further reform the US legal framework[100], and there were new dialogues with the EU that led to the adoption by President Biden, in 2022, of an Executive Order which limits intelligence activities[101]: at that point, the European Commission adopted the EU-US Data Privacy Framework. If the Union really succeeded in inducing the US to change significantly their surveillance rules, it would be an incredible achievement for the EU model and the "Brussels effect".

---

97 See for instance: M. Scott, *Digital Bridge: Transatlantic competition – Washington's privacy plan – Microsoft lobbying*, in *politico.eu*, 2021.

98 See for instance: C. Kuner, *Protecting EU Data Outside EU Borders Under the GDPR*, in *Common Market Law Review*, 60(1), 2023, 77 ss.

99 F.Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, in *Harvard Journal of Law & Technology*, 33(2), 2020, 66 ss., at 691.

100 See for instance: S. Bradford Franklin-L. Sarkesian, *Congress Has the Opportunity to Enact Meaningful Surveillance Reforms Now: Here's How*, in *newamerica.org*, 2020; S. Bradford Franklin, *Rethinking Surveillance on the 20th Anniversary of the Patriot Act*, in *justsecurity.org*, 2021.

101 See for instance: H. Ruschemeier, *Nothing new in the west? The executive order on US surveillance activities and the GDPR*, in *European Law Blog*, 2022.

However, putting aside the latter case (where both adequacy decisions were invalidated by the CJEU and not repealed by the Commission), it has been demonstrated not only that the approach of EU agreements diverges considerably from the one of the EU internal legal framework, but also that the former risks undermining the latter. Indeed, since at international level trade agreements have strong enforcement mechanisms, this creates a significant risk of a de facto supremacy of trade law over human rights law: fearing the consequences of such mechanisms, several institutional players – especially the Commission – could be induced not to limit personal data flows, at the expense of data protection.

3.4. The "horizontal provisions": a possible solution?

In truth, the described issue has not been completely neglected: in recent years, a solution has been explored. In 2018, following the exhortations of the European Parliament[102], the European Commission endorsed a new mechanism: the "Horizontal provisions for cross-border data flows and for personal data protection", to be inserted in subsequent EU trade agreements in place of "old-fashioned" provisions[103]. On the one hand, they contain data flows commitments, which cover all economic sectors (they are not limited to specific fields such as financial or telecommunication services). On the other hand, they also include provisions devoted to the fundamental rights to personal data protection and privacy: their formulation, which is very different from the past, is aimed at enabling the compliance with the EU legal framework on personal data, that would be excepted from EU trade commitments[104].

Additionally, in 2019 the Commission proposed the adoption of broadly similar provisions also in the framework of the WTO, in the context of the negotiations to regulate electronic commerce worldwide[105].

Thanks to such provisions, several criticisms would be overcome: the risk of negative consequences for the Union for limiting personal data flows to non-EU countries would be considerably reduced; consequently, also

[102] European Parliament, *Resolution containing the European Parliament's recommendations to the Commission on the negotiations for the Trade in Services Agreement (TiSA) (2015/2233(INI))*, 2016.

[103] European Commission, *Press release – European Commission endorses provisions for data flows and data protection in EU trade agreements*, 2018.

[104] On the Horizontal Provisions, see for instance: M. Burri, *Cross-border data flows and privacy in global trade law: has trade trumped data protection?*, in *Oxford Review of Economic Policy*, 39(1), 2023, 85 ss.; E. Fahey, *Does the EU's Digital Sovereignty Promote Localisation in Its Model Digital Trade Clauses?*, in *European Papers*, 8(2), 2023, 503 ss.; L. Brännström, *Global Inequality and the EU International Law Position on Cross-Border Data Flows*, in *Nordic Journal of International Law*, 92, 2023, 119 ss.

[105] WTO, *Joint Statement on Electronic Commerce – EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce – Communication from the European Union*, 2019, INF/ECOM/22. On the point see: M. Burri, *A WTO Agreement on Electronic Commerce: An Enquiry into its Substance and Viability*, in *Georgetown Journal of International Law*, 53, 2023, 565 ss.

the pressure on the Commission and on the other institutional players would decrease, and they would be more independent in their actions. In brief, such clauses can be regarded as the result of the EU's growing attention to privacy and personal data protection as fundamental rights, as well as of its intention to make the EU agreements as consistent as possible with the high standards of protection enshrined in the GDPR[106].

Moreover, some examples of their implementation are encouraging: not only is the EU attempting to include similar clauses in several agreements currently under negotiation, but it has also incorporated them in the final text of certain instruments such as the EU-New Zealand FTA, entered into force in 2024[107], and the EU-Chile Interim Trade Agreement, entered into force in 2025.

However, there are also reasons to doubt that horizontal clauses will actually be included in all future trade agreements with third countries. The case of the EU-UK TCA is emblematic: its art. 202 departs from the horizontal provisions in the most important aspects. Due to its different wording, such article does not fully safeguard how the EU regulates the protection of personal data and privacy, and it does not prevent the EU from having to justify its legal framework on the matter. There is still uncertainty as to the possibility for the EU to autonomously apply its domestic rules on personal data protection without suffering consequences at international level: a circumstance that provoked criticisms from the EDPS[108]. These considerations can also be reiterated with regard to the EU-Japan deal on data flows, which entered into force in 2024 and amended the abovementioned EU-Japan EPA: this deal, too, was heavily criticised by the EDPS for reasons analogous to those raised in relation to the TCA[109]. As someone pointed out, such cases can be considered as «revealing of the limited influence of the EU position»[110].

Furthermore, something similar also happened with reference to WTO rules on e-commerce: the "stabilised text" achieved in 2024 includes "Personal Data Protection" provisions that, however, differ in the key elements from the 2019 EU proposal[111].

Therefore, given the breadth of the exception contained in the horizontal clauses[112], the counterparts of the EU would hardly accept their exact

[106] On the point see, for instance: S. Yakovleva-K. Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, in *AJIL Unbound*, 114, 2020, 10 ss.

[107] On the EU-New Zealand FTA, see for instance: M. Burri-K. Kugler-A.D. Ker, *Digital Trade in the EU–New Zealand Free Trade Agreement: An Appraisal*, in *Legal Issues of Economic Integration*, 51(1), 2024, 11 ss.

[108] European Data Protection Supervisor, *Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement*, 2021.

[109] European Data Protection Supervisor, *Opinion 3/2024 on the signing and conclusion on behalf of the European Union, of the Protocol amending the Agreement between the European Union and Japan for an Economic Partnership regarding free flow of data*, 2024.

[110] L. Brännström, *Global Inequality and the EU International Law Position on Cross-Border Data Flows*, cit., 128.

[111] WTO, *Joint Statement Initiative on Electronic Commerce*, 2024, INF/ECOM/87, art. 16 («Personal Data Protection») and art. 25 («Personal Data Protection Exception»).

[112] F. Velli, *The Issue of Data Protection in EU Trade Commitments*, cit., 893; S. Yakovleva-K.

wording, and would likely ask for modifications. In other words, there are no reasons to be excessively optimistic about the effectiveness of such instruments: they could fail to prevent the EU approach on personal data from being undermined by trade commitments made by the Union. All the described criticisms remain unsolved.

4. Conclusions and suggestions

This article has shown that the current EU internal legal framework on personal data flows to third countries – as designed by the EU legislators in the GDPR, as interpreted by the CJEU in its rulings and as implemented by the Commission through the adoption of some of its acts – gives priority to the fundamental right to personal data protection. To rephrase it, the internal approach of the EU consists of creating around personal data a true "fortress": to get in, and obtain personal data from it, it is necessary to comply with the extremely high protection standards set by the Union.

The abovementioned approach has several aims: not only preventing data flows from undermining the protection ensured in Europe by the GDPR, but also exporting EU standards abroad. Such exportation has multiple objectives: there is the will to promote fundamental rights globally, but there is also a strategic aim, i.e. trying to confer a competitive advantage to EU enterprises over non-EU competitors.

The article has also shown that such an approach is contradicted by the one of some EU international trade commitments, some concerning in general the liberalisation of trade in services, some others devoted more specifically to data flows. It is true that such commitments are counterbalanced by clauses that contemplate exceptions aimed at protecting personal data and privacy. However, it is also true that the scope and effectiveness of similar safeguards are questionable. Therefore, it can be stated that the trade agreements concluded by the EU clearly prioritise trade necessities.

Such divergence between the two approaches leads to several considerations. The various institutional players of the Union, and even the various internal branches of the same institution (namely, of the Commission) sometimes have extremely different views and strategies. This, in truth, happens not only in the field covered by this work, but also in other matters of competence of the EU. The statement according to which the external action of the Union is always inspired by the same approach of the EU internal legal framework should probably be questioned. On the contrary, the values and the principles that the Union "injects" in its international agreements seem often different from the ones of its legislation, precisely because of the diverging views among the various institutional players.

Going back to the field discussed in the article, there are, on the one hand, some EU institutional players that adopt a data-protection-centred approach. Among them, we must mention the Court of Justice of the EU, that always privileged privacy and personal data protection over competing in-

Irion, *Pitching trade against privacy*, cit., 219-220.

terests, and turned out to be absolutely uncompromising; the European Parliament, that is often very attentive to the protection of human rights; but also the EDPB and the EDPS (unsurprisingly, since they were established with the specific aim to protect personal data). Lastly, in this category we can include the Commission with reference to DG JUST, that inter alia was in charge of the drafting of the GDPR and is responsible for the adoption of adequacy decisions: indeed, such DG is much more consumer-oriented rather than market-oriented.

On the other hand, there is also a free-trade-centred approach, that characterises in particular another branch of the Commission, i.e. DG TRADE, responsible for the policies on trade with countries outside the EU. Such DG, due not only to its aims but also to the personal backgrounds and sensitivities of its components, ends up not to be particularly attentive to the protection of personal data; probably, it overestimates the scope of the safeguards inserted in trade agreements, while it underestimates the risks that the data at stake might encounter.

The contribution, however, has not only highlighted such divergences. It has also shown that the two approaches cannot coexist peacefully: the approach of EU trade agreements risks undermining the one of the EU internal legal framework. At international level trade agreements have strong enforcement mechanisms that create a risk of a de facto supremacy of trade law. The fear of the consequences deriving from such mechanisms could determine some heavy pressure on several institutional players, undermining their independence in protecting personal data.

This is abstractly true for national supervisory authorities and for the CJEU. However, above all, it is true for the Commission that was actually induced, more than once, to adopt – or not to repeal – adequacy decisions even in the absence of a protection "essentially equivalent" to that of the EU. In other words, we could say that the approach of DG TRADE influenced DG JUST: the latter, under the pressure of the consequences that the Union could suffer due to the trade commitments made by DG TRADE, multiple times did not pursue in the best way possible the interest of protecting personal data.

The abovementioned "fortress", built by the EU through its internal legal framework, risks collapsing, and this would also end up affecting its aims: we refer to the exportation of EU standards worldwide, and even to the protection of EU enterprises from foreign competition.

At this point, please allow the writer to conclude this article with a suggestion. We believe that, for the Union, it would be preferable to choose more firmly the approach to adopt, regardless of whether it is one or the other. Once the decision is made, the chosen approach should be consistently pursued by all institutional players, without exception.

Obviously, the choice of the approach cannot be random, since it must take into account not only the values, but also the interests of the EU. Inter alia, one has to wonder if it is true that transborder flows of personal data are so convenient for EU firms from the economic point of view; or if, on the contrary, they predominantly benefit the big players of the global market of digital services (mainly located outside Europe, especially in the United States): the latter, being also powered by personal data coming

from the Union, could create an unbridgeable gap between them and EU businesses. For these reasons, transborder flows of personal data could be considered even harmful for the European digital economy that consequently would need more protection.

Evaluations of this kind, it must be said, are ongoing worldwide. Even the US, that have always supported the free flow of information and benefited from such flow, have introduced limitations to international transfers of personal data, with specific reference to the ones towards China. Consistently with the US approach, such measures are motivated not by privacy reasons, but by national security ones. However, this does not change the fact that similar limitations are also aimed at further promoting national digital industry, and at making sure that the value of citizens' data remains within the borders of the country, without being exploited by competitors in third States[113].

Therefore, also for the EU it is indispensable to question the convenience for its digital economy of transborder flows of personal data. At the end of such assessment, if similar flows were considered not only consistent with EU values, but also more convenient than hazardous for EU enterprises, the Union should probably rethink the GDPR and its mechanisms, and should adopt an approach in line with its trade agreements.

On the contrary, if cross-border data transfers were deemed harmful not only for the fundamental rights of European but also for the EU digital economy, the EU should try to follow the path traced by the CJEU and avoid making at international level further commitments to allow the flow of information (getting rid, where possible, of the already existing ones). What is certainly illogical for the EU, instead, is to keep intact its internal legal framework, while continuing at the same time to make inconsistent data flows commitments. Without a clear choice, indeed, trade commitments would anyhow undermine the aims of the EU legislation.

[113] On the point see, for instance: S. Yakovleva, *Editorial: On Digital Sovereignty, New European Data Rules, and the Future of Free Data Flows*, in *Legal Issues of Economic Integration*, 49(4), 2022, 339 ss.; S. Yakovleva, *EU's trade policy on cross-border data flows in the global landscape: navigating the thin line between liberalizing digital trade, "digital sovereignty" and multilateralism – Institute for Information Law Research Paper No. 2022-12*, Amsterdam, 2022; S. Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy – Institute for Information Law Research Paper No. 2022-09*, Amsterdam, 2022; K. Irion-M.E. Kaminski-S. Yakovleva, *Privacy Peg, Trade Hole: Why We (Still) Shouldn't Put Data Privacy in Trade Law*, in *University of Chicago Law Review Online*, 2023.

Abstract

The article focuses on how the European Union deals with personal data flows to third countries, the regulation of which attempts to balance two conflicting interests: on the one hand, the need to facilitate cross-border data transfers for commercial reasons; on the other, the need to protect personal data and privacy. Preliminarily, it will be shown that the current EU internal legal framework on the matter, as designed by EU legislators, interpreted by the Court of Justice and implemented by the Commission, gives top priority to the protection of individuals, at the expense of economic needs. Subsequently, the contribution will explain that certain international commitments made by the EU in the field of trade law – some concerning in general the liberalisation of trade in services, some others devoted more specifically to data flows – are not consistent with the balance designed by the EU internal legal framework. Finally, it will be also demonstrated that the approach of EU trade commitments seriously risks undermining the one of the EU internal legal framework.

L'articolo si concentra su come l'Unione Europea affronta la tematica dei flussi di dati personali verso paesi terzi, la cui regolamentazione cerca di bilanciare due interessi contrastanti: da un lato, l'esigenza di facilitare i trasferimenti oltrefrontiera di dati per motivi commerciali; dall'altro lato, la necessità di proteggere i dati personali e la privacy. Preliminarmente, verrà illustrato che l'attuale disciplina interna UE in materia, per come delineata dai legislatori UE, interpretata dalla Corte di Giustizia e attuata dalla Commissione, dà priorità alla protezione degli individui, a discapito delle esigenze economiche. In seguito, il contributo illustrerà che certi impegni internazionali assunti dall'UE in ambito commerciale – alcuni concernenti in generale la liberalizzazione dei servizi, altri più specificamente dedicati ai flussi di dati – non risultano coerenti con il bilanciamento operato dalla disciplina interna UE. Infine, verrà altresì dimostrato che l'approccio degli impegni commerciali dell'Unione rischia seriamente di compromettere quello della disciplina interna UE.

Keywords

transborder flows of personal data – GDPR – international trade law – EU trade agreements – Brussels effect

Regulatory Sandboxes. Spazi di sperimentazione normativa per l'intelligenza artificiale*

Eugenia Perrone

Sommario

1. Introduzione. – 2. Regulatory sandboxes: un modello innovativo di regolazione. – 2.1. Il complesso rapporto fra regolazione e innovazione. – 2.1.1. Differenti approcci alla regolazione delle nuove tecnologie: prospettive statunitense, europea e cinese a confronto. – 2.2. La sperimentazione a fini di regolazione. – 2.2.1. Principali caratteristiche degli spazi di sperimentazione normativa. – 2.2.2. Regulatory sandboxes: potenzialità, limiti e sfide future. - 3. Regulatory sandboxes nel regolamento europeo sull'intelligenza artificiale. – 3.1. Il contesto internazionale. – 3.2. Lo scenario europeo. – 3.2.1. Spazi di sperimentazione normativa per l'intelligenza artificiale. - 4. Regulatory sandboxes per l'intelligenza artificiale nell'ordinamento italiano. – 4.1. Lo scenario nazionale. – 4.2. Disegni di legge in materia di sperimentazione normativa per l'intelligenza artificiale e prospettive future. – 5. Conclusioni.

1. Introduzione

Il rapido sviluppo delle tecnologie emergenti e, in particolare, dell'intelligenza artificiale, anima il dibattito giuridico nell'era digitale: la posizione di chi ritiene che la regolazione rappresenti un freno per lo sviluppo tecnologico si contrappone a quella di chi ritiene, invece, che l'innovazione comporti un numero talmente elevato di rischi da dover essere necessariamente regolata.

Per raggiungere un bilanciamento fra tali opposte posizioni e creare un adeguato equilibrio fra regolazione e innovazione, è importante che il diritto evolva al pari dello sviluppo tecnologico e che, a tal fine, il legislatore individui – accanto ai tradizionali metodi di regolazione – strumenti normativi innovativi e sperimentali.

Fra questi, assumono rilievo le regulatory sandboxes, spazi di sperimentazione normativa che favoriscono la collaborazione tra regolatori e innovatori, la definizione di processi di regolazione trasparenti e flessibili e, non da ultimo, la possibilità di testare – sotto il controllo delle autorità competenti e con deroghe temporanee alle normative vigenti – le nuove

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

tecnologie prima della loro immissione sul mercato.
Il saggio si pone l'obiettivo di approfondire l'analisi di tali innovativi strumenti di regolazione per l'intelligenza artificiale, con specifico riferimento al rilievo che essi assumono nello scenario europeo e italiano. Tale rilievo emerge in maniera evidente se si considera che il regolamento europeo sull'intelligenza artificiale disciplina le regulatory sanboxes fra le misure a sostegno dell'innovazione e che, inoltre, esso prevede che gli Stati membri provvedano affinché le loro autorità competenti istituiscano almeno uno spazio di sperimentazione a livello nazionale, che sia operativo entro il 2 agosto 2026.
Nel paragrafo che segue, dopo una breve introduzione sul complesso rapporto che lega regolazione e innovazione e sui differenti approcci a questa tematica che vengono assunti, rispettivamente, nel contesto statunitense, europeo e cinese, vengono illustrati le caratteristiche e i limiti delle regulatory sandboxes.
Fra gli elementi caratterizzanti gli spazi di sperimentazione normativa vi è la loro capacità di coniugare e promuovere la sperimentazione sia di nuove tecnologie sia di nuovi strumenti di regolazione, consentendo in tal modo al legislatore di acquisire competenze tecniche e regolamentari in costante dialogo con gli innovatori.
Fra i limiti associati all'utilizzo delle regulatory sandboxes, uno dei principali è costituito dal pericolo di frammentazione nell'intera Unione europea, il che vanificherebbe gli sforzi fatti dal legislatore europeo per la creazione del mercato unico e per la promozione dell'innovazione.
Nel terzo paragrafo, fatta una breve premessa sulla rilevanza che le regulatory sandboxes assumono anche a livello internazionale, si illustra la disciplina sugli spazi di sperimentazione normativa contenuta nel regolamento europeo sull'intelligenza artificiale.
Nel quarto paragrafo, si esamina l'approccio italiano all'uso delle regulatory sandboxes: dopo un cenno ai precedenti normativi nel settore FinTech e nel settore della digitalizzazione della pubblica amministrazione, vengono illustrate alcune proposte di legge che attengono all'istituzione di spazi di sperimentazione normativa per l'intelligenza artificiale.
In conclusione, si riporta la considerazione secondo cui per cogliere pienamente i benefici derivanti dall'introduzione delle regulatory sandboxes per l'intelligenza artificiale negli ordinamenti nazionali, occorrerà attendere l'adozione, da parte della Commissione europea, degli specifici atti di esecuzione con i quali saranno precisati le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione di tali spazi di sperimentazione normativa.

2. *Regulatory sandboxes:* un modello innovativo di regolazione

2.1. Il complesso rapporto fra regolazione e innovazione

Il rapido sviluppo delle tecnologie emergenti[1] e, in particolare, dell'intelligenza artificiale ("IA", oppure, in inglese, "AI" da artificial intelligence), ha rivoluzionato il tradizionale dibattito giuridico – incentrato sulla dicotomia fra diritto positivo e diritto naturale[2] – e ha messo in luce il complesso rapporto che lega regolazione e innovazione.

Le ragioni di tale complessità sono principalmente due e attengono entrambe all'esigenza di promuovere l'evoluzione tecnologica nel rispetto degli individui, delle imprese, della democrazia, dello Stato di diritto e della sostenibilità ambientale[3].

La prima ragione consiste nella necessità di creare un «equilibrio dinamico fra regolazione e innovazione»[4], anche al fine di contemperare la posizione

[1] Sulla qualificazione normativa delle tecnologie emergenti, v. G. Centemero - P. Longo, *Regulatory sandbox. Analisi e prospettive parlamentari della sperimentazione normativa nel nuovo millennio*, Rimini, 2024, 19: «Per la qualificazione normativa di "tecnologie emergenti" si rimanda all'elencazione contenuta nell'articolo 8, comma 2, lettera c), del decreto-legge 1° marzo 2021, n. 22, convertito, con modificazioni, dalla legge 22 aprile 2021, n. 22, che ha istituito presso la Presidenza del Consiglio dei ministri il Comitato interministeriale per la transizione digitale (CITD), con il compito di assicurare il coordinamento e il monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle pubbliche amministrazioni competenti in via ordinaria. Nelle materie di competenza del Comitato, infatti, sono ricomprese prioritariamente le attività di coordinamento e monitoraggio dell'attuazione delle iniziative relative anche allo sviluppo e alla diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'Internet delle cose (*Internet of Things*) e della *blockchain* (per tale intendendosi la *Distributed Ledger Technology* o *DLT*)». Con specifico riferimento all'intelligenza artificiale, v. O. Pollicino - P. Dunn, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Milano, 2024, 6, ove si osserva che «sarebbe quanto meno riduttivo definire l'IA come una mera tecnologia», dal momento che «siamo di fronte in questo caso a un qualcosa di assai più complesso, che può forse essere definito un "ecosistema digitale" in cui gli ingredienti più importanti sono la quantità di dati a disposizione e la forza computazionale, che si traduce, anche, nella capacità di automazione e nella velocità di apprendimento. Un ecosistema, in ultima analisi, dove l'ingrediente mancante […] è il "fattore umano"».

[2] Sul dibattito giuridico relativo al rapporto tra diritto e tecnica che ha interessato la scienza giuridica nella seconda metà del secolo scorso, in particolare in Italia, v. A. Merlino, *Regulatory sandbox. Una nuova prospettiva ordinamentale*, Napoli, 2022, 15 ss.

[3] Si precisa che l'oggetto del presente saggio è focalizzato sull'analisi delle *regulatory sandoboxes* quali strumenti normativi facilitatori di innovazione. Al contrario, le questioni etiche e quelle connesse ai profili di responsabilità e alla tutela dei principi dell'ordinamento giuridico, che pur rilevano in generale nell'esame del rapporto fra diritto e tecnica, non sono oggetto della presente trattazione.

[4] Sulla necessità di assicurare un equilibrio fra regolazione e innovazione, v. L. Torchia, *Lo Stato digitale. Una introduzione*, Bologna, 2023, 83, «Il legislatore europeo è consapevole del fatto che i sistemi di intelligenza artificiale sono ben lontani dal costituire un settore maturo e sono, anzi, in continua evoluzione. Questa evoluzione produce vantaggi come rischi ed è di conseguenza necessario assicurare un equilibrio dinamico fra regolazione e innovazione, fra costi e sviluppo, fra vincoli e incentivi»; L. Torchia, *Regolazione e innovazione nel mondo digitale: un equilibrio dinamico*, in *irpa.eu*, 3 giugno 2024.

di chi considera la regolazione un ostacolo all'innovazione con quella di chi, invece, ritiene l'innovazione tecnologica talmente rischiosa da dover essere necessariamente regolata.

La seconda consiste, invece, nella necessità che il diritto non sia «in ritardo, rispetto ad una realtà tecnologica e giuridica che si è già rapidamente trasformata altrove»[5], ma, al contrario, risulti adeguato a regolare fenomeni che pervadono ormai ogni ambito della vita quotidiana, pubblica e privata[6] (si pensi al settore sanitario, alla formazione scolastica e universitaria, alla digitalizzazione della pubblica amministrazione, solo per citarne alcuni)[7].

Nella prassi applicativa, infatti, è difficile che il diritto si innovi di pari passo con lo sviluppo tecnologico «almeno per due fattori che sono sotto gli occhi di tutti: la velocità del ciclo evolutivo»[8] – che spesso si scontra con la lentezza dei tradizionali procedimenti legislativi – e «la tendenza delle tecnologie più recenti a diffondersi trasversalmente, in più campi di applicazione, rompendo i confini tradizionali anche tra i settori oggetto di disciplina giuridica»[9].

In altri termini, per far fronte all'impatto disruptive[10] delle tecnologie emergenti e al carattere pervasivo con cui queste sono diventate protago-

---

[5] A. Merlino, *Regulatory sandbox*, cit., 23.

[6] Il recente rapido sviluppo tecnologico ed il suo impatto sulla vita quotidiana di privati, imprese e pubbliche amministrazioni conducono, sempre con maggior frequenza, ad analizzare il fenomeno attraverso la lente del diritto e, in particolare, del diritto amministrativo. L'emergere dirompente dell'innovazione solleva, infatti, importanti questioni in materia di *governance* delle nuove tecnologie, relative alla trasformazione dei poteri pubblici ed anche alla sempre più frequente affermazione di soggetti privati che operano come pubblici poteri. Sui temi legati alla *governance* delle nuove tecnologie, v. S. Del Gatto, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. Il caso del riconoscimento facciale*, in *Rivista italiana di diritto pubblico comunitario*, 1, 2023, 37 ss.. Sulla regolazione digitale, v. L. Torchia, *Lo Stato digitale*, cit. e, inoltre, i seguenti saggi del *Simposio: la regolazione digitale nell'Unione europea*, in *Rivista trimestrale di diritto pubblico*, 4, 2022: G. Resta, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, 971 ss.; B. Carotti, *La politica europea sul digitale: ancora molto rumore*, 997 ss.; G. Sgueo, *La visione e la voce nella transizione digitale dei governi democratici*, 1015 ss.; A. Simoncini, *La co-regolazione delle piattaforme digitali*, 1031 ss.; O. Pollicino, *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione on line*, 1051 ss.; G. Finocchiaro, *La regolazione dell'intelligenza artificiale*, 1085 ss.; L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, 1101 ss. Sul tema della regolamentazione europea dell'innovazione tecnologica nel settore finanziario, v. B. Barmann, *L'innovazione digitale e la finanza: esperimenti con le regole*, in *irpa. eu*, 11 novembre 2024.

[7] Sulla *governance* del mondo digitale, v. L. Floridi, *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, 31, 2018, che avvia la propria analisi partendo dal seguente assunto «Today, in any mature information society (Floridi 2016), we no longer live online or offline but *onlife*, that is, we increasingly live in that special space, or *infosphere*, that is seamlessly analogue and digital, offline and online».

[8] G. Lo Sapio, *Il regolatore alle prese con le tecnologie emergenti. La regulatory sandbox tra principi dell'attività amministrativa e rischio di illusione normativa*, in *Federalismi.it. Rivista di diritto pubblico italiano, comparato europeo*, 30, 2022, 91.

[9] *Ibid.*

[10] *Ivi*, 88, dove si chiarisce che «Secondo la nomenclatura economica, *disruptive* sono quelle applicazioni tecnologiche che portano sul mercato nuove offerte di valore, "interrompono" le traiettorie di miglioramento progressivo delle tecnologie fino ad allora utilizzate, creano nuovi modelli di business, nuovi clienti, nuove professionalità».

niste in ogni ambito della vita di ciascun individuo, occorre che il diritto si innovi rapidamente anch'esso, pur sempre nel rispetto della divisione dei poteri tipica di un ordinamento giuridico[11].

Un esempio emblematico della complessa interazione fra diritto e innovazione è contenuto nel regolamento europeo sull'intelligenza artificiale[12] ("Regolamento", "Regolamento (UE) 2024/1689" o "AI Act") – di cui si tratterà nel paragrafo 3 che segue – ed è relativo alla definizione stessa di «sistema di IA»: con l'intento di riflettere le innovazioni che si sono affermate durante l'iter di approvazione del testo normativo[13], tale definizione è mutata sensibilmente dal 2021 – anno in cui è stata adottata la proposta di Regolamento – al 2024 – anno in cui, invece, è stato approvato il testo finale del Regolamento medesimo.

Per definire meglio il contesto sopra delineato, occorre considerare che il legislatore spesso non è in possesso di conoscenze tecniche adeguate e sufficienti per «regolare dettagliatamente innovazioni tecnologiche e finanziarie complesse e in rapidissima evoluzione, né tanto meno può prevedere, al pari dei mercati stessi e dei suoi attori, i rischi connessi all'introduzione di una nuova tecnologia»[14].

Al fine di rispondere alle necessità fin qui delineate, si è di recente diffuso – a livello internazionale – un approccio normativo di tipo sperimentale, che mira a regolamentare l'innovazione attraverso l'esperienza[15] («cd. learning legislation»[16]), «anche mediante un'ampia e costante cooperazione tra legislatore e imprese e un attento monitoraggio dei risultati ottenuti (cd. "evidence-based policy")»[17].

Tale approccio consente al legislatore di individuare – accanto ai tradizio-

---

[11] Sulla fragilità delle due varianti del positivismo giuridico – normativismo e decisionismo – nel contesto dell'innovazione, v. A. Merlino, *Regulatory sandbox*, cit., 23, secondo cui i tradizionali strumenti della regolamentazione normativa «si rivelano spesso inadeguati a tenere il passo con l'incalzante rapidità dell'evoluzione tecnologica e finanziaria e rischiano di diventare un deterrente all'innovazione e al suo impatto sociale».

[12] 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), Gazzetta Ufficiale dell'Unione europea Serie L, 12.7.2024.

[13] Ci si riferisce, in particolare, all'immissione sul mercato di *Chat Generative Pre-Trained Transformer* ("*ChatGPT*") avvenuta il 30 novembre 2022, ad opera di OpenAI, un laboratorio di ricerca statunitense sull'intelligenza artificiale. ChatGPT rappresenta un cd. *Large Language Model* ("*LLM*") «una particolare realizzazione di intelligenza artificiale generativa (capace cioè di generare nuovi ed "originali" contenuti) specializzata per interagire con gli esseri umani attraverso la conversazione». Così S. B. Grenci, *Le applicazioni di Intelligenza artificiale a supporto dell'automazione del procedimento amministrativo*, in *Rivista italiana di informatica e diritto*, 1, 2024, 223-224.

[14] A. Merlino, *Regulatory sandbox*, cit., 24.

[15] Il pensiero giuridico italiano, già nella seconda metà del secolo scorso, era consapevole che la "conoscenza" costituisse un presupposto della regolazione, come testimoniato dall'autorevole espressione «Prima conoscere, poi discutere, poi deliberare», di L. Einaudi, *Prediche inutili*, Torino, 1956.

[16] G. Centemero - P. Longo, *Regulatory sandbox*, cit., 20.

[17] *Ibid.*

nali strumenti giuridici – soluzioni normative innovative, sperimentali e flessibili[18] e, in tal modo, di adeguare l'ordinamento giuridico alla realtà.
Fra le soluzioni più innovative che consentono di mettere in pratica tale approccio, assumono sempre maggior rilievo i cd. "spazi di sperimentazione normativa" (o "regulatory sandboxes"), da intendersi quali strumenti di ausilio per il legislatore, in primo luogo, per sperimentare la tecnologia e, in secondo luogo, per raggiungere una «"composizione sperimentale" di problematiche regolamentari specifiche e/o settoriali non diversamente gestibili, sulla scorta del tradizionale sistema delle fonti»[19].
L'espressione inglese sandbox evoca il recinto di sabbia protetto nel quale i bambini possono giocare e imparare in sicurezza e ben si addice a identificare, in ambito giuridico, uno

«spazio di "sperimentazione normativa" che consente agli operatori interessati di testare le innovazioni tecnologiche, in un ambiente reale, ma con due sostanziali peculiarità: beneficiando di deroghe temporanee alla disciplina cui sarebbero sottoposte tali attività e restando sotto la supervisione dell'autorità competente per il settore»[20].

Così definite, le regulatory sandboxes – «istituto giuridico»[21] nato in ambito FinTech[22] «in Gran Bretagna intorno al 2015, diffusosi globalmente e infine approdato negli ordinamenti europei e nel 2021 in quello italiano»[23] – appaiono, dunque, utili per configurare quell'equilibrio fra regolazione e innovazione a cui si ambisce nell'ambito del dibattito giuridico sopra citato[24].
Nel seguito saranno illustrate le principali caratteristiche degli spazi di spe-

[18] «Il riconoscimento dell'inadeguatezza degli strumenti giuridici tradizionali […] non va tuttavia confuso con l'aspirazione – spesso latente – a sospendere o ad abolire l'ordinamento giuridico *tout court*, il che spezzerebbe sciaguratamente una lancia a favore di una malsana anarchia giuridica (che anarchia vera e propria non è, giacché si adegua alla "decisione" del detentore della forza politica o economica che sia)» così A. Merlino, *Regulatory sandbox*, cit., 24.

[19] M. T. Paracampo, *Il percorso evolutivo ed espansivo delle regulatory sandboxes da FinTech ai nuovi lidi operativi del prossimo futuro*, in *Federalismi.it. Rivista di diritto pubblico italiano, comparato europeo*, 18, 2022, 208.

[20] G. Lo Sapio, *Il regolatore alle prese con le tecnologie emergenti*, cit., 90.

[21] A. Merlino, *La regulatory sandbox in un recente parere del Consiglio di Stato*, in *giustizia-amministrativa.it*, 2021.

[22] Sulla definizione di *Financial Technology* (cd. "*FinTech*"), v. *Risoluzione del Parlamento europeo del 17 maggio 2017 sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario (2016/2243(INI))* in cui si precisa «la tecnologia finanziaria (FinTech) dovrebbe essere intesa come un'attività finanziaria resa possibile o offerta attraverso le nuove tecnologie, che interessa l'intero settore finanziario in tutte le sue componenti, dal settore bancario a quello assicurativo, i fondi pensione, la consulenza in materia di investimenti, i servizi di pagamento e le infrastrutture di mercato», in *europarl.europa.eu*. Sulla *regulatory sandbox* in ambito *FinTech*, v. M.T. Paracampo, *Dalle regulatory sandboxes al network dei facilitatori di innovazione tra decentramento sperimentale e condivisione europea*, in *Rivista di diritto bancario*, II, 2019, 219 ss.

[23] A. Merlino, *Regulatory sandbox*, cit., 7.

[24] Sull'esigenza di guidare lo sviluppo tecnologico, v. L. Floridi, *Soft Ethics and the Governance of the Digital*, cit., che fa riferimento alla necessità «*to shift from chasing to leading*».

rimentazione normativa, pur nella consapevolezza che i contorni dell'istituto sono ancora indefiniti e suscettibili di ulteriori esiti e che, pertanto, l'analisi di seguito riportata è da considerarsi relativa ad un fenomeno nuovo ancora in fieri[25].
Nei paragrafi 3 e 4 del presente saggio, si esaminerà, poi, la rilevanza che le regulatory sandboxes assumono nel contesto europeo e nazionale, con particolare riferimento agli spazi di sperimentazione normativa per la regolazione dei sistemi di intelligenza artificiale.

2.1.1. Differenti approcci alla regolazione delle nuove tecnologie: prospettive statunitense, europea e cinese a confronto

Prima di approfondire l'analisi delle regulatory sandboxes, appare utile fare una breve analisi comparata dei principali modelli di regolazione delle nuove tecnologie in ambito internazionale.
Come ben illustrato dall'autrice del libro "Digital Empires. The Global Battle to Regulate Technology"[26], a livello globale è possibile individuare tre distinti approcci alla regolazione: il modello normativo americano guidato dal mercato, il modello normativo europeo guidato dai diritti[27] e il modello normativo cinese guidato dallo Stato. Tali differenti approcci sono il frutto di diverse teorie sul rapporto tra mercati, diritti individuali e collettivi e Stato e, non di rado, entrano in conflitto nell'intento di dominare lo scenario internazionale nell'era digitale.
Il modello statunitense (cd. "American market-driven regulatory model") privilegia un approccio guidato dal mercato, favorendo l'innovazione, la concorrenza e una regolamentazione ridotta, con le aziende tecnologiche al centro dello sviluppo digitale. Il modello europeo (cd. "European rights-driven regulatory model"), invece, pone al centro i diritti, con norma-

[25] Sul dibattito giuridico tuttora in corso sulla natura delle *regulatory sandboxes*, v. Paracampo, *Il percorso evolutivo ed espansivo delle regulatory sandboxes*, cit., 208: «la *regulatory sandbox*, che già si presta ad essere esaminata da più angolazioni, involgendo implicazioni di tipo giuridico, economico e sociale, sta facendo emergere ulteriori elementi meritevoli di opportuna considerazione, ciascuno legato al carattere multiforme, multifunzionale e multidimensionale del modello in questione. *Ad adiuvandum*, sta ponendo in particolare evidenza i due macro orientamenti del dibattito in corso, che si spinge ora verso il lido della "regolazione" sperimentale, ora verso quello della "sperimentazione" normativa».

[26] A. Bradford, *Digital Empires. The Global Battle to Regulate Technology,* New York, 2023. Della stessa autrice, sulla capacità dell'Unione europea di influenzare la regolazione a livello globale, v. A. Bradford,*The Brussels Effect: How the European Union Rules the World*, Oxford, 2020.

[27] Con specifico riferimento alla diversità di approccio fra l'ordinamento europeo e l'ordinamento americano, v. E. Chiti - B. Marchetti, *Divergenti? Le strategie di Unione europea e Stati Uniti in materia di intelligenza artificiale*, in *Rivista della regolazione dei mercati*, 1, 2020, 29 ss.; G. Alpa, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021; M. Macchia - A. Mascolo, *Intelligenza artificiale e regolazione*, in A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?, vol. 2, Amministrazione, responsabilità, giurisdizione*, Bologna, 2022, 97 ss.

tive come il General Data Protection Regulation ("GDPR")[28] che valorizzano la privacy, la protezione dei diritti individuali e standard etici rigorosi, volti a tutelare i cittadini digitali e a promuovere un uso responsabile della tecnologia. Infine, il modello cinese (cd. "Chinese state-driven regulatory model"), incentrato sul controllo statale, assegna al governo un ruolo primario nella gestione e nello sviluppo tecnologico, spesso subordinando i diritti individuali agli interessi statali e agli obiettivi collettivi.

L'analisi comparata sin qui svolta, seppur delineata nei suoi tratti essenziali[29], consente di definire la cornice giuridica all'interno della quale agisce il legislatore europeo[30].

Per quanto qui rileva, tale comparazione consente, in particolare, di osservare come il legislatore europeo orienti ogni sua scelta sulla base del proprio patrimonio costituzionale, che rappresenta una vera e propria «bussola valoriale, scolpita nell'articolo 2 del Trattato sull'Unione europea per il futuro (e il presente) dell'Unione»[31].

---

[28] 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).

[29] Sulla *governance* delle nuove tecnologie e sui differenti approcci alla regolazione nelle prospettive statunitense, europea e cinese, v. Del Gatto, *La governance delle nuove tecnologie*, cit., 37 ss.:

[30] Sulla regolazione del «nuovo ecosistema digitale», con particolare riferimento all'ambito - che qui maggiormente rileva – dell'intelligenza artificiale, v. O. Pollicino – P. Dunn, *Intelligenza artificiale e democrazia,* cit., 9, «Gli ultimi mesi si sono caratterizzati, anche da un punto di vista più strettamente giuridico, per una corsa o, meglio rincorsa alla regolazione del nuovo ecosistema digitale: una competizione geopolitica di natura globale che ha visto l'emergere di una serie di normative dentro e fuori l'Europa. Dal nuovo Regolamento europeo sull'intelligenza artificiale […] che conferma il primato dal punto di vista regolatorio – ma non tecnologico – passando per il tentativo cinese (a forte traino dirigista) di trasformare i propri campioni nazionali dell'intelligenza artificiale in campioni globali, giungendo all'ordine esecutivo di Biden di ottobre 2023, che per la prima volta segna un clamoroso passaggio negli Stati Uniti da un meccanismo di *self-regulation* a una parziale co-regolamentazione del settore, si è assistito di recente ad un vertiginoso incremento degli sforzi regolativi in materia di intelligenza artificiale. La Dichiarazione di *Bletchley*, adottata a Londra a novembre 2023, ha inoltre rappresentato essa stessa un tentativo di promuovere sul piano internazionale un approccio quanto più cooperativo possibile nell'adozione di strategie di *governance* nel settore. Nel frattempo, il 17 maggio 2024, durante la riunione annuale del Comitato dei Ministri del Consiglio d'Europa, è stata approvata la Convenzione Quadro sull'Intelligenza Artificiale, primo trattato internazionale giuridicamente vincolante in materia di IA». Per una più ampia analisi comparativa della regolamentazione dell'intelligenza artificiale nel contesto internazionale, v. O. Pollicino – P. Dunn, *Intelligenza artificiale e democrazia,* cit., 67-72. Di recente, il dibattito giuridico sulla regolamentazione dell'intelligenza artificiale è animato anche dalle vicende connesse all'*iter* di approvazione, nello Stato della California, del *SB-1047 Safe and Secure Innovation for Frontier Artificial Intelligence Models Act*. In particolare, il veto su tale atto - espresso nel settembre 2024 dal Governatore Gavin Newsom e le cui ragioni sono spiegate dallo stesso Governatore nel messaggio pubblicato in gov.ca.gov - ha acceso il dibattito a livello internazionale su come i governi possano regolamentare tecnologie avanzate come l'intelligenza artificiale senza ostacolare il progresso.

[31] O. Pollicino – P. Dunn, *Intelligenza artificiale e democrazia,* cit., 7.

2.2. La sperimentazione a fini di regolazione

Nel paragrafo 2.1 è stato esaminato il complesso rapporto tra regolazione e innovazione e sono state messe in luce le difficoltà che, a livello normativo, derivano dall'interazione fra diritto e innovazione tecnologica. In tale contesto, si è dato evidenza al fatto che – fra gli strumenti normativi facilitatori dell'innovazione[32] – gli spazi di sperimentazione normativa, o regulatory sandboxes, possono assumere un ruolo di grande rilievo.
Al fine di comprendere meglio la portata dell'utilizzo delle sandboxes nel contesto giuridico, appare importante richiamare l'etimologia del termine, cui si è già brevemente accennato.

«Nella lingua inglese sandbox indica letteralmente un recinto di sabbia, ossia uno spazio protetto e ben delimitato all'interno del quale i bambini hanno la possibilità di giocare, sperimentando con la propria creatività. Tale termine è dapprima entrato nel lessico del mondo tecnologico, più precisamente dell'informatica, indicando un ambiente di prova, spesso differenziato dagli ordinari spazi impiegati per testare le applicazioni e nel quale poter sperimentare progetti che non necessariamente si concluderanno con lo sviluppo di un prototipo»[33].

In ambito giuridico, il termine inglese sandbox «indica un "perimetro protetto", all'interno del quale è possibile testare innovazioni»[34] in determinati settori e in regime derogatorio.
Più in dettaglio, nella realtà giuridica, con il termine sandbox si intende

«uno spazio, virtuale oppure fisico, all'interno del quale è possibile testare per un periodo di tempo limitato progetti innovativi da un punto di vista tecnologico, con la possibilità di derogare la normativa di settore, in modo da consentire ai promotori del progetto di svolgere i test nella maniera più esaustiva, completa ed efficiente possibile»[35].

Ai fini del presente saggio, giova richiamare anche le definizioni in uso a livello europeo. Il Consiglio dell'Unione europea (anche il "Consiglio")[36]: (i) considera gli spazi di sperimentazione normativa (i.e. regulatory sandboxes) come «quadri concreti che, fornendo un contesto strutturato per la sperimentazione, consentono, se del caso in un ambiente reale, di testare tecnologie, prodotti, servizi o approcci innovativi – al momento soprattutto nel contesto della digitalizzazione – per un periodo di tempo limitato

[32] M.-T. Paracampo, *Dalle regulatory sandboxes al network dei facilitatori di innovazione*, cit.

[33] G. Centemero - P. Longo, *Regulatory sandbox*, cit., 26.

[34] A. Merlino, *Regulatory sandbox*, cit., 67.

[35] M. Trapani, *L'utilizzo delle sandboxes normative: una ricognizione comparata delle principali esperienze di tecniche di produzione normativa sperimentali e il loro impatto sull'ordinamento,* in *Osservatorio sulle fonti*, 3, 2022, 216 e ss..

[36] Si vedano le *Conclusioni del Consiglio sugli spazi di sperimentazione normativa e le clausole di sperimentazione come strumenti per un quadro normativo favorevole all'innovazione, adeguato alle esigenze future e resiliente che sia in grado di affrontare le sfide epocali nell'era digitale (2020/C 447/01)*, in *eur-lex.europa.eu*.

e in una parte limitata di un settore o di un ambito soggetto a vigilanza regolamentare, garantendo la messa in atto di opportune misure di salvaguardia»; (ii) interpreta le clausole di sperimentazione (i.e. experimentation clauses) come «disposizioni giuridiche che consentono alle autorità incaricate di attuare e applicare la legislazione di esercitare, caso per caso, un certo grado di flessibilità in relazione alla sperimentazione di tecnologie, prodotti, servizi o approcci innovativi» e, inoltre, (iii) osserva che «le clausole di sperimentazione costituiscono spesso la base giuridica degli spazi di sperimentazione normativa e sono già utilizzate nella legislazione dell'UE e nei quadri giuridici di molti Stati membri».
Come fin qui definite, le regulatory sandboxes rappresentano, dunque, un innovativo modello normativo a mezzo del quale il legislatore può superare il tradizionale approccio che mira a regolamentare in modo astratto le materie caratterizzate da un considerevole fattore tecnologico[37].
Attraverso l'uso degli spazi di sperimentazione normativa, infatti, il legislatore – anche grazie alla collaborazione con le imprese e gli stakeholder – può elaborare regole generali partendo dall'analisi di casi concreti.
Il modello così delineato reca in sé notevoli potenzialità ed anche alcuni rischi, come si vedrà meglio nei paragrafi che seguono.

2.2.1. Principali caratteristiche degli spazi di sperimentazione normativa

Una prima peculiare caratteristica delle regulatory sandboxes consiste nella capacità di tali strumenti di agevolare la sperimentazione delle tecnologie emergenti e, allo stesso modo, di verificare – compito assai complesso – quanto un impianto normativo sia adeguato a regolare le tecnologie stesse.
Gli altri elementi essenziali degli spazi di sperimentazione normativa possono essere così riassunti:
al loro interno sono ammessi partecipanti che desiderano sperimentare un prodotto o servizio innovativo utilizzando nuove tecnologie. In questa «sabbiera giuridica»[38], è possibile derogare a determinate norme giuridiche; conformemente ai principi di proporzionalità, di trasparenza, di pubblicità e di parità di trattamento, l'ammissione è «subordinata alla verifica di requisiti prefissati e alla conseguente autorizzazione e iscrizione in un apposito registro da parte dell'Autorità di vigilanza»[39];
al fine di testare prodotti e servizi in un ambiente protetto e, al contempo, gli spazi di sperimentazione normativa sono soggetti a «limiti temporali, entro i quali l'Autorità di vigilanza rinuncia alla sua funzione sanzionatoria

[37] Su una prima disamina delle differenti tipologie di *sandboxes* a livello globale (i.e. finanziaria, tecnologica, regolatoria, sanitaria, ambientale, geografica), v. G. Centemero - P. Longo, *Regulatory sandbox*, cit., 70-79: «Le differenti tipologie di sandbox […] dimostrano, anche dal mero punto di vista temporale, un'evoluzione costante dell'istituto, seppur eterogenea in relazione al proprio ambito applicativo. In un'epoca soggetta a continui cambiamenti, infatti, l'impiego di modelli di sperimentazione normativa rappresenta una nuova modalità di regolare la relazione inscindibilmente bilaterale tra diritto e tecnologia».

[38] A. Merlino, *Regulatory sandbox*, cit., 28.

[39] *Ibid.*

ed entra invece in dialogo (guidance) con gli attori che operano nel "recinto"»[40];
l'istituto «deroga alle ordinarie norme regolamentari per la durata della sperimentazione. Al termine del periodo di sperimentazione tornano a vigere le norme ordinarie»[41].

2.2.2. *Regulatory sandboxes*: potenzialità, limiti e sfide future

Come può dedursi da quanto illustrato fin qui, gli spazi di sperimentazione normativa hanno il pregio di coniugare e promuovere: (i) la sperimentazione, che può riguardare separatamente o congiuntamente sia tecnologie in rapida evoluzione, sia una regolamentazione elaborata in contesti temporali differenti e divenuta ormai inadeguata rispetto alle opportunità offerte dall'era digitale[42]; (ii) l'acquisizione – per così dire – sul campo, da parte del legislatore, sia di competenze tecnologiche, sia di adeguate tecniche di regolazione delle tecnologie emergenti, in costante dialogo con stakeholders e operatori di mercato. In sintesi, il modello sandbox introduce un approccio regolamentare pragmatico sul mercato, mirato a «"seguire e conformare" il framework normativo[43]» in base all'analisi delle tecnologie testate e ai risultati delle sperimentazioni.
L'uso delle regulatory sandboxes consente, inoltre, di adottare una prospettiva preventiva (cd. "ex ante") che, se da un lato anticipa la regolamentazione prima della commercializzazione del prodotto, dall'altro non esclude un successivo intervento normativo. I risultati della sperimentazione possono infatti portare a una conferma o modifica del quadro normativo esistente, oltre a sostenere una nuova proposta basata sui dati empirici raccolti[44].
Accanto alle indubbie potenzialità degli spazi di sperimentazione normativa sopra delineate, occorre tuttavia rilevare anche alcuni limiti che caratterizzano le regulatory sandboxes.
Innanzitutto, si consideri che gli spazi di sperimentazione normativa si configurano fin dall'inizio come un modello versatile e ricco di sfumature, derivanti «predetta mancanza di una codificazione e di una definizione univoca»[45], tale da metterne in luce le differenti «dimensioni funzionali e nel contempo le connotazioni distintive»[46].
Nel contesto europeo, tali caratteristiche si traducono in limiti e, di conseguenza, anche nel rischio che, in assenza di una vera e propria normativa di riferimento, la regolamentazione di dettaglio delle regulatory sandboxes

40 *Ibid.*

41 *Ibid.*

42 M.-T. Paracampo, *Il percorso evolutivo ed espansivo delle regulatory sandboxes*, cit., 213.

43 Ivi, 214.

44 *Ibid.*

45 *Ibid.*

46 *Ibid.*

sia lasciata alla discrezionalità dei singoli Stati membri, con ciò vanificando gli sforzi fatti dall'Unione europea a favore della creazione del mercato unico e dell'innovazione.

Fra le sfide che l'introduzione delle regulatory sandboxes pone al legislatore europeo vi è, dunque, non soltanto la capacità di individuare strumenti adeguati ad incentivare lo sviluppo tecnologico nel rispetto del proprio patrimonio costituzionale, ma anche la necessità di fornire agli Stati membri indicazioni applicative e assistenza per l'istituzione e il funzionamento degli spazi di sperimentazione normativa, al fine ultimo di scongiurare il rischio che un'eccessiva frammentazione normativa di fatto ostacoli lo sviluppo tecnologico europeo[47].

Senza considerare, poi, che l'utilizzo delle regulatory sandboxes spesso pone alcuni ordinamenti – caratterizzati da un'impostazione di hard law e da rigidi procedimenti normativi – nella difficoltà di accogliere un'innovazione normativa senza una preventiva decisione del legislatore o, in ogni caso, in uno dei modi previsti a livello costituzionale e nel rispetto della gerarchia delle fonti.

Inoltre, fra i potenziali limiti connessi all'utilizzo delle regulatory sandboxes, vi sono quelli associati: all'eventuale assenza di adesione dei privati agli spazi di sperimentazione normativa (anche per ragioni legate all'ingente impegno economico che la partecipazione a tali spazi implica); alle possibili difficoltà di instaurare delle collaborazioni fra i soggetti istituzionali coinvolti; alle difficoltà emerse nel momento in cui si è resa necessaria l'eventuale proposta di deroga a una normativa e alla complessità del relativo sistema autorizzativo, «oltre ad una evidente difficoltà di inquadramento di questo strumento nel sistema di produzione delle fonti»[48] di un ordinamento giuridico.

Nel paragrafo 3 che segue si vedrà come, a fronte delle potenzialità e dei limiti delle regulatory sandboxes, e delle sfide derivanti dell'utilizzo delle stesse, il legislatore europeo ne abbia disciplinato l'istituzione nell'ambito delle misure a sostegno dell'innovazione.

[47] Proprio a tal fine, nell'ambito del regolamento europeo sull'intelligenza artificiale di recente approvazione, di cui *infra*, si prevede che «La Commissione può fornire assistenza tecnica, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA», art. 57, par. 1, Regolamento (UE) 2024/1689. In tale contesto, assume poi peculiare rilievo l'art. 58 del Regolamento medesimo, con il quale, per evitare la frammentazione legislativa all'interno dell'Unione europea, si prevede che la Commissione possa adottare atti di esecuzione - ai sensi dell'art. 291 del Trattato sul funzionamento dell'Unione europea ("TFUE") – per garantire che «le modalità dettagliate e le condizioni relative agli spazi di sperimentazione normativa per l'IA sostengano la flessibilità, nella massima misura possibile, affinché le autorità nazionali competenti istituiscano e gestiscano i loro spazi di sperimentazione normativa per l'IA».

[48] M. Trapani, *L'utilizzo delle sandboxes normative*, cit., 226

3. *Regulatory sandboxes* nel regolamento europeo sull'intelligenza artificiale

3.1. Il contesto internazionale

Il complesso rapporto tra regolazione e innovazione anima il dibattito giuridico nell'era digitale.
Come illustrato nel paragrafo 2, al fine di promuovere l'innovazione è necessario che il diritto si innovi anch'esso e accolga l'utilizzo di nuovi strumenti di regolazione, fra i quali assumono particolare rilevanza le regulatory sandboxes (o spazi di sperimentazione normativa).
Nei capitoli che seguono, l'analisi degli spazi di sperimentazione normativa sarà condotta in relazione, in particolare, allo sviluppo dei sistemi di intelligenza artificiale nell'ordinamento europeo e nazionale.
A tal fine, appare utile inquadrare prima, brevemente, il contesto internazionale di riferimento.
A livello globale è ormai diffusa la consapevolezza che gli spazi di sperimentazione normativa siano in grado di promuovere l'innovazione e, allo stesso tempo, accrescere la qualità della regolazione dell'innovazione medesima. Lo dimostrano le indicazioni di recente illustrate nel rapporto "Regulatory sandboxes in artificial intelligence"[49] dell'Organizzazione per la cooperazione e lo sviluppo economico ("Ocse"), la quale, in più occasioni, ha confermato l'esigenza che la regolazione assuma carattere di flessibilità per favorire lo sviluppo digitale[50].
Sempre di recente, anche i lavori condotti nel contesto del G7 Digital and Technology Working Group hanno messo in luce il rilievo che le regulatory sandboxes assumono per le finalità di sviluppo e uso – etico e responsabile – delle applicazioni di intelligenza artificiale nel settore pubblico[51].

---

[49] *Organisation for economic co-operation and development* ("*OECD*") (2023), "*Regulatory sandboxes in artificial intelligence*", *OECD Digital Economy Papers, No. 356, OECD Publishing, Paris*, in *oecd.org*. Sul tema, v. G. Taraborrelli, *Le regulatory sandboxes tra dinamiche di mercato e innovazione tecnologica*, in *Osservatorio sull'Analisi di Impatto della Regolazione (AIR), Rassegna trimestrale, Anno XIV*, 4, 2023, 17-25.

[50] Per una panoramica sulle iniziative in materia di qualità normativa e *better regulation* intraprese dall'Ocse e dalla Commissione europea nel corso del 2021, nonché sugli strumenti di *better regulation* nella giurisprudenza amministrativa, v. V. Di Porto - E. Espa (a cura di) *L'analisi di impatto e gli altri strumenti per la qualità della regolazione*, *Annuario 2021*, in *Osservatorio sull'Analisi di Impatto della Regolazione (AIR)*, Napoli, 2021.

[51] «*Policy tools like regulatory sandboxes can be used to set controlled environments for piloting AI solutions under regulatory supervision*», in *OECD/UNESCO (2024), G7 Toolkit for Artificial Intelligence in the Public Sector, OECD Publishing, Paris*, in *oecd.org*, 78. A riprova della rilevanza a livello istituzionale del tema si noti che nel documento citato si legge, inoltre: «*The report was prepared by the Organisation for Economic Co-operation and Development (OECD) Directorate for Public Governance and the United Nations Educational, Scientific and Cultural Organisation (UNESCO) for the 2024 Italian G7 Presidency and the G7 Digital and Technology Working Group. It was launched during the G7 Digital and Technology Ministerial Meeting in Como, Italy, on 15 October 2024*».

3.2. Lo scenario europeo

Con l'intento di incentivare l'utilizzo di strumenti di better regulation[52], negli ultimi anni anche l'Unione europea ha intensificato gli sforzi per promuovere lo sviluppo delle tecnologie emergenti attraverso la sperimentazione normativa[53].
In relazione all'adozione di strumenti per migliorare la legislazione, nel novembre del 2020 il Consiglio dell'Unione europea ha evidenziato che

«la flessibilità e la sperimentazione possono costituire elementi importanti per un quadro normativo agile, favorevole all'innovazione, adeguato alle esigenze future, basato su dati concreti e resiliente che promuova la competitività, la crescita, la sostenibilità, l'apprendimento normativo nonché la sovranità tecnologica e la leadership dell'Europa e che contribuisca ad affrontare gli shock sistemici e le sfide future epocali e a lungo termine».[54]

In quell'occasione, il Consiglio ha anche sottolineato l'importanza di considerare il «principio di innovazione» quale elemento fondamentale per creare strumenti normativi efficienti e adeguati alle esigenze di innovazione dell'Unione europea.
Sul sentiero tracciato dal Consiglio si pone anche la Commissione europea, come chiarito nel programma di better regulation[55] illustrato nella comunicazione «Legiferare meglio: unire le forze per produrre leggi migliori» del 29 aprile 2021[56] e, più di recente, nel Better Regulation Toolbox del 20 luglio 2023[57]. In tale ultimo documento, per quanto qui rileva, si annovera la regulatory sandbox fra gli strumenti innovativi utili per elaborare regole "future-proof" e creare una disciplina uniforme al livello europeo.
Come accennato nel paragrafo 2, il primo utilizzo delle regulatory sandboxes è avvenuto nel settore del FinTech.[58].

---

[52] Nel contesto istituzionale europeo, il rilievo delle *regulatory sandboxes* quale misura di sostegno all'innovazione è stato messo in evidenza recentemente anche da M. Draghi, in M. Draghi, *The future of European competitiveness*, il rapporto commissionato dalla Commissione europea e presentato il 9 settembre 2024, in *commission.europa.eu*.

[53] Su alcuni esempi di utilizzo degli spazi di sperimentazione normativa a livello europeo, v. G. Centemero - P. Longo, *Regulatory sandbox*, cit., 79-115.

[54] *Conclusioni del Consiglio sugli spazi di sperimentazione normativa*, cit.

[55] Per una panoramica sulla *better regulation* quale fattore chiave per la competitività dei sistemi economici, v. Lo Sapio, *Il regolatore alle prese con le tecnologie emergenti,* cit., 89 ss.

[56] *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni* «*Legiferare meglio: unire le forze per produrre leggi migliori*", COM (2021) 219 *final*», in *eur-lex.europa.eu*. Sul tema, M. Picchi, *Legiferare meglio: a proposito della nuova comunicazione della commissione europea*, in *Osservatorio sulle fonti*, 3, 2021.

[57] Come indicato dalla Commissione europea, «*the regulatory sandbox can inform possible future approaches to tackle these barriers and make the corresponding rules more adaptive and future-proof*», in «*Better regulation' toolbox – July 2023 edition*», 599-604 («*Tool #69. Emerging methods and policy instruments*»), ad oggi disponibile, assieme alle *Better regulation guidelines* del 3 novembre 2021, in *commission.europa.eu*.

[58] Per una disamina diffusa sulle iniziative delle istituzioni europee nel settore *FinTech*, v. A. Merlino, *Regulatory sandbox*, cit., 29-65, G. Centemero - P. Longo, *Regulatory sandbox, cit.,* 79-86. Sul tema, anche v. M. Trapani, *L'utilizzo delle sandboxes normative*, cit., 225, secondo

Successivamente, a fronte dei notevoli benefici ottenuti grazie all'utilizzo di questo strumento di sperimentazione normativa e della repentina accelerazione dello sviluppo tecnologico, l'Unione europea ne ha incentivato l'utilizzo per la regolazione delle tecnologie emergenti e, in particolare, dell'intelligenza artificiale[59], come emerge dall'analisi del regolamento europeo sull'intelligenza artificiale, di recente approvazione[60]. Quest'ultimo contiene, infatti, specifiche previsioni sugli «Spazi di sperimentazione normativa per l'IA» nel Capo VI dedicato alle «Misure a sostegno dell'innovazione».

Il procedimento di approvazione del Regolamento è stato lungo e si è svolto nel contesto della definizione della Strategia digitale dell'Unione europea[61].

Già nel 2017, il Consiglio europeo aveva formulato alla Commissione europea l'invito a individuare le iniziative utili per accrescere la posizione strategica industriale europea e, allo stesso tempo, per garantire elevati

il cui non è casuale che, nello scenario europeo, la *sandbox* si sia sviluppata a partire dal settore del *FinTech* nel Regno Unito, «in quanto è risultato più naturale creare una cornice giuridica adeguata in un ordinamento che si basa su regole di *common law* ed in un settore in continua evoluzione, contraddistinto da una forte *territorialità* degli effetti (in gran parte economici e non legati, ad esempio, a beni della vita). Il progetto fu lanciato nel 2016 e interessò subito la *Financial Conduct Authority*; i requisiti che devono essere soddisfatti al fine di accedere ad una *sandbox* sono principalmente tre: l'innovatività, il beneficio sociale o economico per la collettività e la effettiva necessità di superare una norma al fine della sperimentazione e della messa in commercio di un prodotto».

[59] V.F. Di Porto, *Algorithmic disclosure rules,* in *Artificial Intelligence and Law,* 31, 2023, 36: «*Regulatory sandboxes are not new […]. They exist in the Fintech industry, where new rules are experimented in controlled environments (thanks to simulations run over big data) before being implemented at large scale […] Regulatory sandboxes can be conceptualized as venues for experimenting with co-regulation, in the sense that they foster collaboration between the regulator (which takes the lead) and the stakeholders to experiment with new avenues for rule production […]. Given their increasing relevance, they are being disciplined by the forthcoming EU Regulation on Artificial Intelligence […]*».

[60] Nel caso «dell'*Artificial Intelligence Act,* così come di altre emanande normative […] si sta passando da un approccio regolatorio focalizzato sul controllo successivo, da parte delle autorità amministrative, ad una cooperazione tra differenti *stakeholder* antecedente al lancio di un determinato prodotto o servizio o di una nuova tecnologia», v. G.M. Riccio, *Intelligenza artificiale e regulatory sandbox: prime osservazioni critiche*, in S. Scaglirini-I. Senatori (a cura di), *Lavoro, Impresa e Nuove Tecnologie dopo l'AI Act,* Modena, 2024, 50. Sulle altre normative europee che prevedono il ricorso a *regulatory sandboxes* – non obbligatorio come per l'*AI Act*, ma facoltativo - lo stesso autore cita l'*Interoperability Act* (art. 2.14) e il *Cyber Resilience Act* (art. 33.2).

[61] «*Digital technologies are profoundly changing our daily life, our way of working and doing business, and the way people travel, communicate and relate with each other. Digital communication, social media interaction, e-commerce, and digital enterprises are steadily transforming our world. They are generating an ever-increasing amount of data, which, if pooled and used, can lead to a completely new means and levels of value creation. It is a transformation as fundamental as that caused by the industrial revolution. In her political guidelines, Commission President von der Leyen stressed the need for Europe to lead the transition to a healthy planet and a new digital world. This twin challenge of a green and digital transformation has to go hand-in-hand. It requires, as set out in the European Green Deal, an immediate change of direction towards more sustainable solutions which are resource-efficient, circular and climate-neutral. It requires that every citizen, every employee, every business person has a fair chance, wherever they live, to reap the benefits of our increasingly digitised society*», in *Communication: Shaping Europe's digital future* della Commissione europea, del 19 febbraio 2020, in *commission.europa.eu*.

standard etici e la protezione dei diritti individuali[62].
La proposta di Regolamento è stata adottata il 21 aprile 2021[63]

«dopo un lungo processo di analisi e di consultazione da parte delle istituzioni europee e a seguito dell'adozione di numerosi atti di soft law – linee guida, libri bianchi, risoluzioni – mediante i quali si sono via via definiti la ratio, l'oggetto e l'ambito di applicazione delle nuove regole»[64].

Da allora, l'iter che ha condotto all'approvazione del Regolamento si è articolato in più fasi ed ha coinvolto le istituzioni, gli Stati membri e gli stakeholder, fino a giungere alla pubblicazione in Gazzetta Ufficiale dell'Unione europea – il 12 luglio 2024[65] – della prima regolamentazione organica dell'intelligenza artificiale a livello internazionale[66].
Gli obiettivi del Regolamento consistono nel miglioramento del funzionamento del mercato interno[67] e nella promozione della diffusione di un'IA

[62] «*Bruxelles, 19 ottobre 2017 (OR. en) EUCO 14/17 CO EUR 17 CONCL 5*», in *consilium.europa.eu*.

[63] *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, del 21 aprile 2021, COM (2021) 206 final*, in *eur-lex.europa.eu*.

[64] L. Torchia, *Lo Stato digitale*, cit., 83.

[65] Per una prima analisi dell'*iter* di approvazione del Regolamento, v. R. Petruso - G. Smorto, *Il Regolamento europeo sull'intelligenza artificiale: una prima lettura*, in *La Nuova giurisprudenza civile commentata*, 4, 2024, 989-1004; G. Rugani, *La "legge sull'intelligenza artificiale" dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, in *Osservatorio sulle fonti*, 1, 2024.

[66] «In modo complementare, l'ambizione del legislatore è anche di influenzare il modo in cui le soluzioni per la sfera digitale sono sviluppate a livello globale e di esportare il modello al di fuori del Vecchio Continente promuovendo così` i valori europei e diventando una sorta di *gold standard* in tema di regolazione dell'intelligenza artificiale», v. R. Petruso – G. Smorto, *Il Regolamento europeo sull'intelligenza artificiale*, cit., 990. Sul cd. *Brussel effect*, v. Bradford, *The Brussels Effect,* cit. Si veda anche O. Pollicino – P. Dunn, *Intelligenza artificiale e democrazia*, cit., 62-63, «Si tratta, questo, del primo caso a livello internazionale di regolamentazione organica dell'intelligenza artificiale a, come tale, ha coagulato intorno a sé un importante dibattito dottrinale, sociale e politico» e «peraltro, la Corte dei Conti europea ha rilasciato una relazione contenente un'analisi critica dell'approccio dell'Unione all'IA, sottolineando tra l'altro la necessità di finanziare e incentivare la ricerca in tale settore». Si veda Corte dei Conti europea, *Relazione speciale 08/2024: Le ambizioni dell'UE in materia di intelligenza artificiale – Per il futuro, una governance più forte e investimenti più consistenti e mirati sono essenziali» del 29 maggio 2024*, in *eca.europa.eu*. Sul punto, si evidenzia che il 5 novembre 2024, il Consiglio dell'Unione europea ha approvato conclusioni su una relazione della Corte dei conti europea volte a rafforzare le ambizioni dell'Unione europea in materia di IA, in particolare potenziando la *governance* e garantendo investimenti più consistenti e mirati per il futuro in questo settore, come evidenziato nel comunicato stampa 812/24, in *consilium.europa.eu*.

[67] La base giuridica Regolamento è «individuata nell'art. 114 TFUE sul ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno» e, inoltre, l'art. 16 TFUE costituisce «un'ulteriore base legittimante la nuova regolamentazione. Il legislatore prevede infatti regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, «consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota a fini di attività di contrasto, dell'uso dei sistemi di IA per le valutazione dei rischi delle persone fisiche a fini di attività di contrasto

antropocentrica e affidabile e, al contempo, nella protezione della salute, della sicurezza e dei diritti fondamentali tutelati nell'Unione e nella promozione dell'innovazione[68].

Non sarà oggetto del presente saggio l'analisi di dettaglio dell'intera complessa disciplina contenuta nel Regolamento, né l'elaborazione di considerazioni di carattere generale sui temi della regolazione dell'intelligenza artificiale, per le quali si rimanda a trattazioni che affrontano tali questioni in maniera diffusa[69].

Lo scopo del presente saggio è, invece, quello di analizzare le innovative previsioni del Regolamento che disciplinano la creazione di spazi di sperimentazione normativa per l'intelligenza artificiale al fine ultimo di accrescere la competitività delle imprese e lo sviluppo tecnologico nell'Unione europea[70].

Prima di avviare tale analisi, appare, però, indispensabile illustrare brevemente la definizione stessa dei sistemi di intelligenza artificiale oggetto di regolazione, insieme ad alcuni elementi che caratterizzano il Regolamento.

Considerata la difficoltà di regolamentare un fenomeno in rapida evoluzione ed in continuo cambiamento, la suddetta definizione è piuttosto ampia e assume per lo più una natura descrittiva. Inoltre, come in parte già osservato nel paragrafo 2, essa è stata modificata nel corso dell'iter di approvazione del Regolamento per includervi anche i cd. sistemi di IA per finalità generali – la cui introduzione sui mercati è successiva all'elaborazione della proposta della Commissione del 2021 – ed oggi risulta coerente con l'approccio dell'Ocse[71].

Attualmente, la definizione di «sistema di IA» contenuta nell'art. 3, n. 1), del Regolamento è la seguente:

---

e dell'uso dei sistemi di IA di categorizzazione biometrica a fini di attività di contrasto» (cfr. considerando 3)», così R. Petruso - G. Smorto, *Il Regolamento europeo sull'intelligenza artificiale,* cit., 989-990.

[68] Art. 1 del Regolamento (UE) 2024/1689.

[69] Per un'analisi generale dei problemi connessi alla regolamentazione dell'intelligenza artificiale, v. i saggi raccolti in A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?,* vol. 1, *Diritti fondamentali, dati personali e regolazione*; vol. 2, *Amministrazione, responsabilità, giurisdizione;* vol. 3, *Proprietà intellettuale, società e finanza,* Bologna, 2022; G. Natale - A.M. Lazzè, *AI Act, il regolamento europeo sull'intelligenza artificiale: punti di forza e punti di debolezza*, in *Rassegna Avvocatura dello Stato*, 2023.

[70] «È questo un altro punto cruciale. Pare infatti plausibile il rischio che l'UE si limiti a regolare una tecnologia principalmente prodotta da altri. Per evitarlo, le regole sulla sperimentazione, anche se necessarie, non paiono sufficienti. Servono anzitutto fondi. E in tal senso i numeri dell'AI Index di Stanford del 2023 propongono un quadro eloquente: sono sempre gli Stati Uniti a investire maggiormente sull'IA. Nel 2022 i fondi privati americani per questo settore sono stati più di 47 miliardi di dollari. Oltre il triplo dei fondi cinesi (13,4) e dieci volte più dei britannici (4,3); per non parlare della Germania (2,3) e della Francia (1,7). Purtroppo, l'Italia non è menzionata, proprio per l'irrisorietà dei fondi. Eppure, questo è uno degli aspetti chiave per lo sviluppo di una tecnologia affidabile e competitiva, che, non dimentichiamoci, rappresenta da tempo un fondamentale asset di sviluppo economico», così AIRIA Associazione per la regolazione dell'Intelligenza Artificiale, AA.VV. (a cura di), *Navigare l'European AI Act,* Milano, 2024, 50.

[71] *OECD (2024), Explanatory memorandum on the updated OECD definition of an AI system*, *OECD Artificial Intelligence Papers*, No. 8, OECD Publishing, Paris, in *oecd.org*.

«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».

L'elencazione di specifici sistemi di intelligenza artificiale è demandata, invece, non al Regolamento, ma ad un allegato dello stesso, e può essere modificata mediante l'adozione di atti delegati da parte della Commissione europea, senza riattivare l'intero processo regolamentare. Tale peculiarità deriva dall'esigenza di disporre di un'elencazione che sia aggiornata di pari passo con i rapidi mutamenti del contesto tecnologico di riferimento.
Solo al fine di delineare l'ambito giuridico di interesse della presente trattazione, appare necessario, inoltre, definire alcuni elementi essenziali del Regolamento, per quanto ciò sia difficile alla luce della complessità del testo e della materia in esame.
Così come la definizione dei sistemi di IA, anche l'ambito di applicazione del Regolamento è definito secondo criteri molto ampi.
Dal punto di vista territoriale, il Regolamento si applica a qualsiasi sistema di IA commercializzato o utilizzato all'interno del mercato unico, a prescindere dalla sua origine o costruzione fuori dall'Unione europea.
In relazione, invece, al criterio soggettivo di applicazione, il legislatore europeo ha preso in considerazione la cosiddetta «catena del valore»[72] dell'intelligenza artificiale, dal momento che il Regolamento si applica a tutti i soggetti a qualsiasi titolo coinvolti nella produzione, nella commercializzazione o nell'utilizzazione dei sistemi di IA, indipendentemente dal fatto che siano stabiliti nell'Unione europea o in un paese terzo. Tale criterio soggettivo, inoltre, è «esteso ai soggetti pubblici come ai soggetti privati, indipendentemente dalle diverse regole di azione in genere valide per l'azione pubblica rispetto all'attività privata»[73].
È importante sottolineare, inoltre, che l'approccio regolatorio della disciplina in esame è basato sul livello di rischio dei sistemi di IA e fa riferimento sia a sistemi basati su algoritmi deterministici, sia ai sistemi di cd. machine learning [74].

---

[72] L. Torchia, *Lo Stato digitale*, cit., 84.

[73] *Ibid.*

[74] Per una definizione non «*tecnicamente rigorosa*», ma utile a fornire informazioni di base, v. L. Torchia, *Lo Stato digitale*, cit., 185, 188, 189, in cui si indica che il termine «algoritmo» «deriva, secondo un'opinione diffusa, dal nome dello studioso mediorientale Al-Khuwarizmi, vissuto nel IX secolo d.C., che per primo ha ipotizzato un procedimento matematico capace di organizzare e gestire processi decisionali, il cui esito conclusivo risulta calcolabile e prevedibile *ex ante*. Si tratta, dunque, di un procedimento di calcolo costruito dal programmatore in modo che esso svolga una sequenza di passi e operazioni, volta a risolvere un compito in un tempo finito. All'interno di questa categoria, si possono distinguere diverse tipologie. Gli algoritmi più semplici funzionano seguendo istruzioni definite e non ambigue e producono un risultato certo, definito e prevedibile. Sono stati elaborati anche algoritmi più complessi, che tentano di mimare le reti neurali del cervello umano, impiegano *big data* e sono in grado di apprendere autonomamente, anche basandosi su sistemi di *machine learning* […], producendo così risultati indipendentemente da una predeterminazione di passaggi rigida e controllabile»; inoltre, si specifica che l'espressione «*machine learning*» è utilizzata quale «espressione con cui si identifica un

Mediante l'adozione di tale approccio regolatorio – secondo cui tanto maggiore è il rischio, quanto più rigorose sono le regole – il Regolamento stabilisce regole specifiche a seconda del livello di rischio che l'IA può generare e, in particolare: i) un rischio inaccettabile; ii) un rischio alto; iii) un rischio limitato o minimo.

In sintesi: le pratiche di IA che comportano un rischio inaccettabile sono vietate (salvo deroghe espresse); i sistemi di IA ad alto rischio sono soggetti a obblighi specifici (ad esempio, relativi alla presenza di un sistema di gestione del rischio, alla qualità dei dati e delle informazioni e alla trasparenza) e, infine, per i sistemi di IA a rischio limitato o minimo sono previsti solo oneri di informazione e l'adesione volontaria a codici di condotta[75].

Di particolare rilievo nell'ambito della disciplina in argomento è anche la previsione di un controllo di conformità prima dell'immissione sul mercato, cui si aggiunge l'obbligo di monitoraggio che i fornitori di sistemi di IA ad alto rischio devono «svolgere *ex post*, ai fini di una valutazione costante della conformità del sistema ai requisiti prescritti dal regolamento e ai fini della segnalazione di incidenti o disservizi o malfunzionamenti»[76].

Secondo quanto anticipato in precedenza, l'assetto regolatorio definito dall'*AI Act* è molto ampio e articolato[77], tuttavia nel presente paragrafo si è cercato di definire solo gli elementi essenziali del Regolamento che maggiormente rilevano ai fini della trattazione successiva la quale, come già sottolineato, è prettamente dedicata all'analisi delle disposizioni relative agli spazi di sperimentazione normativa per l'intelligenza artificiale[78].

---

campo di ricerca su algoritmi che agiscono sulla base di criteri predefiniti e un *training set* di dati specifico con l'obiettivo di realizzare previsioni collegando una mole complessa di dati. La caratteristica principale di tali sistemi di intelligenza artificiale […] consiste nell'abilità di migliorare progressivamente le correlazioni fra dati, giungendo a risultati precisi in tempi estremamente ridotti. I sistemi di *machine learning* sono bipartiti in sistemi di *machine learning* "supervisionato", che apprendono da un set di dati già ordinati da un informatico e perseguono obiettivi predefiniti, e sistemi di *machine learning* "non supervisionato", che assumono invece un approccio indipendente, non necessitando di una guida umana costante. Per questi ultimi diventa pressoché impossibile ricostruire il processo di calcolo attraverso il quale si arriva all'esito finale».

[75] Sul punto, più diffusamente G. Rugani, *La "legge sull'intelligenza artificiale" dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, cit.

[76] L. Torchia, *Lo Stato digitale*, cit., 91.

[77] Fra gli elementi essenziali del Regolamento, meriterebbero apposita trattazione anche i profili *governance* (delineata sia livello di Unione europea sia a livello di autorità nazionali da individuarsi a cura degli Stati membri), i profili sanzionatori e quelli che prevedono un'applicabilità del Regolamento secondo un approccio graduale. Inoltre, fra i profili di rilievo nella trattazione più generale dell'*AI Act*, di sicuro merita evidenza anche la disciplina specifica per i sistemi di IA per cd. finalità generali (*General purpose AI*), introdotta nel Regolamento corso del relativo *iter* di approvazione. Sul Regolamento, v. AIRIA Associazione per la regolazione dell'Intelligenza Artificiale, Aa. Vv. (a cura di), *Navigare l'European AI Act,* cit.; P. Dunn, *Intelligenza artificiale e democrazia,* cit., 62-67; B. Marchetti, *Intelligenza artificiale, poteri pubblici e rule of law*, in *Rivista italiana di diritto pubblico comunitario*, 1, 2024, 49 ss.; A. Pajno, *La governance dell'intelligenza artificiale tra regolamento europeo e disciplina nazionale*, in ASTRID Rassegna n. 13/2024; S. Cantisani, *Le nuove tecnologie e il mondo del diritto: la sfida della regolamentazione dell'intelligenza artificiale*, in *ildirittoamministrativo.it*, 28 agosto 2024; R. Petruso – G. Smorto, *Il Regolamento europeo sull'intelligenza artificiale,* cit.

[78] Sul tema, F. Bagni, *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial*

3.2.1. Spazi di sperimentazione normativa per l'intelligenza artificiale

Le *regulatory sandboxes* sono state fin qui descritte come strumenti innovativi utili per elaborare regole *"future-proof"*, ovvero regole resilienti e delineate per principi genericamente validi.
Nel contesto dell'*AI Act*, la previsione di spazi di sperimentazione normativa risponde all'esigenza di consentire agli Stati membri di sperimentare sistemi di IA potenzialmente rischiosi prima della loro immissione sul mercato e, pertanto, mira a promuovere l'innovazione, favorire la cooperazione tra autorità nazionali e la condivisione delle migliori pratiche anche al fine di un'applicazione armonizzata delle norme sull'IA a livello europeo, migliorare la certezza del diritto, contribuire all'apprendimento normativo basato su dati concreti e facilitare l'accesso al mercato in particolare per le piccole e medie imprese ("PMI") e per le *start-up*[79]. La suddetta previsione rappresenta, al contempo, un esempio tipico del coinvolgimento degli *stakeholder* – al pari di quanto del resto già avvenuto nel corso dell'*iter* di approvazione del Regolamento – nella regolazione (o co-regolazione) dell'intelligenza artificiale[80].
L'analisi della disciplina parte dalla lettura del considerando numero 138, che sottolinea come l'intelligenza artificiale sia una

«una famiglia di tecnologie in rapida evoluzione che richiede sorveglianza regolamentare e uno spazio sicuro e controllato per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi. Al fine di garantire un quadro giuridico che promuova l'innovazione, sia adeguato alle esigenze future e resiliente alle perturbazioni, gli Stati membri dovrebbero garantire che le rispettive autorità nazionali competenti istituiscano almeno uno spazio di sperimentazione normativa in materia di IA a livello nazionale

Intelligence Act to the Cyber Resilience Act, in *Rivista italiana di informatica e diritto*, 2, 2023. 202 ss.; G. Rugani, *La "legge sull'intelligenza artificiale" dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, cit.; Id., *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'AI Act, con particolare riferimento alle regulatory sandboxes*, in *Quaderni Associazione Italiana Studiosi di Diritto dell'Unione Europea (AISDUE) – Rivista quadrimestrale*, fasc. spec. 2, 2024; G.M. Riccio*, Intelligenza artificiale e regulatory sandbox*, cit.

[79] Art. 57, par. 9, Regolamento (UE) 2024/1689.

[80] La disciplina attualmente contenuta prevista dall'*AI Act* è il frutto del lungo *iter* che ha condotto all'approvazione del testo finale. In seguito alla definizione della proposta da parte della Commissione europea, nel corso della procedura legislativa il Consiglio e il Parlamento europeo hanno espresso la propria posizione in materia di *sandboxes*. Sul punto, v. G. Rugani, *La promozione di strumenti di co-regolazione dell'intelligenza artificiale*, cit., 8-9, secondo cui, in generale, «con riferimento all'approccio complessivamente tenuto dalle due istituzioni di cui sopra durante l'intero i*ter legis* dell'*AI Act*, si potrebbe semplificare dicendo che, se il Consiglio è parso più attento a promuovere lo sviluppo dei sistemi di IA e a rendere il testo più vicino alle esigenze delle imprese, il Parlamento europeo è sembrato invece più sensibile alle istanze di protezione dei diritti dei cittadini e dei consumatori, circostanza che ha poi reso necessari rilevanti sforzi per negoziare un testo condiviso»; e, inoltre, per quel che riguarda «più nello specifico gli spazi di sperimentazione normativa, tuttavia, entrambe le istituzioni si sono dimostrate d'accordo nel favorirli, andando addirittura oltre rispetto a quanto proposto dalla Commissione».

per agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio»[81].

Come sopra accennato, le specifiche disposizioni che qui rilevano sono contenute nel Capo VI del Regolamento, relativo alle «Misure a sostegno dell'innovazione».
La presente trattazione sarà rivolta all'analisi, in particolare, delle caratteristiche e delle modalità di funzionamento delle *regulatory sandboxes*, disciplinate negli articoli 57 «Spazi di sperimentazione normativa per l'IA» e 58 «Modalità dettagliate e funzionamento degli spazi di sperimentazione normativa per l'IA».
Prima di approfondire tale peculiare disciplina, occorre, però, richiamare la definizione di «spazio di sperimentazione normativa per l'IA» contenuta nel Regolamento:

«un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare»[82].

Così definite, le *regulatory sandboxes* sono poi disciplinate dall'art. 57 del Regolamento, ai sensi del quale gli Stati membri devono provvedere affinché le loro autorità competenti istituiscano – anche congiuntamente con le autorità competenti di altri Stati membri – «almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale»[83], che sia operativo entro 24 mesi dalla data di entrata in vigore del Regolamento (i.e. entro il 2 agosto 2026)[84].
Assume rilievo per la presente trattazione anche la previsione secondo cui la Commissione europea «può fornire assistenza tecnica, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA»[85]. Tale disposizione, assieme all'art. 58 dell'*AI Act* di cui *infra*, appare di particolare importanza perché esprime la necessità che l'Unione europea fornisca degli indirizzi agli Stati membri per evitare il rischio di frammentazione normativa paventato nel paragrafo 2.2.2.
L'articolo 57 in esame prevede, poi, la possibilità – in tal caso non l'ob-

[81] Considerando 138, Regolamento (UE) 2024/1689.

[82] Art. 3, n. 55, Regolamento (UE) 2024/1689.

[83] Art. 57, par. 1, Regolamento (UE) 2024/1689.

[84] È interessante notare come l'obbligo per gli Stati membri di istituire almeno uno spazio di sperimentazione normativa non fosse previsto nella proposta di Regolamento elaborata dalla Commissione europea. All'interno di quest'ultima gli spazi di sperimentazione normativa erano comunque previsti quali misure a sostegno dell'innovazione; tuttavia, non se ne prevedeva la necessaria istituzione da parte degli Stati membri (obbligo, appunto, attualmente previsto nel Regolamento). Ciò a riprova della fiducia che le istituzioni ripongono nelle *regulatory sandbox*es nel contesto dello sviluppo tecnologico europeo.

[85] Art. 57, par. 1, Regolamento (UE) 2024/1689.

bligo – che siano «istituiti ulteriori spazi di sperimentazione normativa a livello regionale o locale, o congiuntamente con le autorità competenti di altri Stati membri»[86]. E, inoltre, che anche il Garante europeo della protezione dei dati possa «istituire uno spazio di sperimentazione normativa per l'IA per le istituzioni, gli organi e gli organismi dell'Unione» e «esercitare i ruoli e i compiti delle autorità nazionali competenti»[87] conformemente al Capo VI in esame.
Appare di rilievo anche la previsione secondo cui le autorità competenti degli Stati membri «assegnino risorse sufficienti per conformarsi al presente articolo in maniera efficace e tempestiva»[88], a riprova dell'importanza anche degli aspetti finanziari connessi all'implementazione degli spazi di sperimentazione normativa. Gli impegni economici per la creazione delle *regulatory sandboxes* e per la partecipazione delle imprese a queste ultime sono ingenti e, pertanto, è fondamentale che a livello nazionale sia prevista una collaborazione fra settore pubblico e settore privato, anche allo scopo di agevolare l'accesso al mercato da parte delle PMI e delle *start-up*.
La finalità degli spazi di sperimentazione normativa – i quali «possono comprendere prove in condizioni reali»[89] – consistono, come sopra rappresentato, nell'assicurare

«un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e l'autorità competente»[90].

Considerata la rilevanza per la valutazione di conformità dei sistemi di IA alla quale si è fatto cenno nel paragrafo che precede, le *regulatory sandboxes* per l'IA assumono particolare rilievo nel contesto del Regolamento anche perché quest'ultimo prevede la possibilità che – su richiesta del fornitore o del potenziale fornitore del sistema di IA – le autorità nazionali competenti forniscano una «prova scritta delle attività svolte con successo nello spazio di sperimentazione», oltre a «una relazione di uscita che illustra in dettaglio le attività svolte nello spazio di sperimentazione e i relativi risulta-

[86] Art. 57, par. 2, Regolamento (UE) 2024/1689.

[87] Art. 57, par. 3, Regolamento (UE) 2024/1689.

[88] Art. 57, par. 4, Regolamento (UE) 2024/1689.

[89] Art. 57, par. 5, Regolamento (UE) 2024/1689. La definizione della «prova in condizioni reali» è fornita dall'art. 3 n. 57, del Regolamento medesimo come segue: «la prova temporanea di un sistema di IA per la sua finalità prevista in condizioni reali al di fuori di un laboratorio o di un ambiente altrimenti simulato al fine di raccogliere dati affidabili e solidi e di valutare e verificare la conformità del sistema di IA ai requisiti del presente regolamento e che non è considerata immissione sul mercato o messa in servizio del sistema di IA ai sensi del presente regolamento, purché siano soddisfatte tutte le condizioni di cui all'articolo 57 o 60».

[90] Art. 57, par. 5, Regolamento (UE) 2024/1689, che riprende le finalità anticipate nel considerando 139 del Regolamento stesso.

ti e le conclusioni dell'apprendimento»[91]. Il rilievo di tale documentazione è tale se si considera, inoltre, che essa è presa «favorevolmente in considerazione dalle autorità di vigilanza del mercato e dagli organismi notificati, al fine di accelerare le procedure di valutazione della conformità in misura ragionevole»[92].
Le previsioni sopra illustrate consentono di mettere in luce il ruolo centrale che dovranno assumere le autorità nazionali competenti

«sia in una fase di avvio (supporto nell'identificazione dei rischi, delle modalità di testing più idonee, delle misure di mitigazione dei rischi) sia in una fase successiva del progetto (elaborazione dei documenti relativi alle attività svolte e dell'exit report, con i risultati della sperimentazione)»[93].

Inoltre, a riprova dell'intento del legislatore di assicurare il rispetto dei diritti tutelati nell'Unione europea, è importante evidenziare le previsioni secondo cui: (i) le autorità nazionali per la protezione dei dati personali[94] e le autorità che forniscono o sostengono l'accesso a tali dati devono essere associate al funzionamento della *regulatory sandbox* e partecipare al controllo nei limiti dei rispettivi compiti e poteri[95]; (ii) gli spazi di sperimentazione normativa per l'IA

«non pregiudicano i poteri correttivi o di controllo delle autorità competenti che controllano gli spazi di sperimentazione, anche a livello regionale o locale. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi di IA comporta adeguate misure di attenuazione»[96];

(iii) infine, i

«fornitori e i potenziali fornitori partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione. Tuttavia, a condizione che i potenziali fornitori rispetti-

[91] Art. 57, par. 7, Regolamento (UE) 2024/1689.

[92] Art. 57, par. 7, Regolamento (UE) 2024/1689.

[93] V. AIRIA Associazione per la regolazione dell'Intelligenza Artificiale, Aa.Vv. (a cura di), *Navigare l'European AI Act*, cit., 57.

[94] Definiti dall'art. 3 n. 50 del Regolamento (UE) 2024/1689 come: «i dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679».

[95] Art. 57, par. 10, del Regolamento (UE) 2024/1689. Sul trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa, si veda anche l'art. 59 del Regolamento, che lascia «impregiudicate le disposizioni del diritto dell'Unione o nazionale che escludono il trattamento dei dati personali per fini diversi da quelli espressamente menzionati in tali disposizioni, nonché il diritto dell'Unione o nazionale che stabilisce la base per il trattamento dei dati personali necessario ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi o qualsiasi altra base giuridica, conformemente al diritto dell'Unione in materia di protezione dei dati personali».

[96] Art. 57, par. 11, del Regolamento (UE) 2024/1689.

no il piano specifico e i termini e le condizioni di partecipazione e seguano in buona fede gli orientamenti forniti dall'autorità nazionale competente, quest'ultima non infligge alcuna sanzione amministrativa in caso di violazione»[97]

del Regolamento.

Dal punto di vista della *governance* degli spazi di sperimentazione normativa, è importante sottolineare l'attenzione che il legislatore europeo pone alla collaborazione fra i livelli nazionale ed europeo: il Regolamento prevede che le autorità nazionali competenti debbano presentare all'«Ufficio per l'IA» (istituito dalla Commissione europea)[98], nonché al «consiglio per l'IA europeo per l'intelligenza artificiale» (composto di un rappresentante per Stato membro) – istituiti, rispettivamente, ai sensi degli artt. 64 e 65 del Regolamento medesimo– relazioni annuali sui progressi e sui risultati dell'attuazione delle *regulatory sandboxes*[99].

Come sopra accennato, la presente analisi non può prescindere da quella dell'art. 58 dell'*AI Act*, che mira a scongiurare uno dei rischi potenzialmente derivanti dall'introduzione nell'ordinamento europeo di spazi di sperimentazione normativa per l'IA: la frammentazione nell'Unione europea che potrebbe determinarsi nel caso in cui i singoli Stati membri non fossero adeguatamente supportati nell'adozione di tali strumenti.

Emerge chiaramente, infatti, l'intenzione del legislatore europeo di lasciare spazio a al legislatore nazionale al fine di definire la disciplina di dettaglio della materia. Tuttavia, proprio tale libertà impone che sia previsto e ben disciplinato anche un ruolo di necessario coordinamento a livello europeo. In tale contesto, l'art. 58 citato prevede espressamente che, onde «evitare la frammentazione nell'intera Unione, la Commissione adotta atti di esecuzione che precisano le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa per l'IA»[100] e, al contempo, definisce i principi comuni e le finalità che devono essere rispettate da tali atti di esecuzione.

Fra le previsioni principali del citato art. 58 del Regolamento si segnalano, in particolare quelle che prevedono che gli atti di esecuzione garantiscano: che gli spazi di sperimentazione siano aperti a qualsiasi fornitore o poten-

[97] Art. 57, par. 12, del Regolamento (UE) 2024/1689. Sebbene il testo sembri limitare la responsabilità ai danni successivi alla fase di sperimentazione, sarebbe opportuno estenderne l'applicazione anche ai danni verificatisi durante questa stessa fase. Ciò risponderebbe all'esigenza di una protezione estesa per le terze parti coinvolte, anche in considerazione dell'eventuale impatto dei sistemi sperimentali sull'incolumità degli utenti..

[98] In tema di *governance*, sul ruolo centrale assunto a livello europeo dall'Ufficio per l'IA, v. AIRIA Associazione per la regolazione dell'Intelligenza Artificiale, Aa.Vv. (a cura di), *Navigare l'European AI Act*, cit., 51, secondo cui «Non secondario poi è il ruolo dell'ufficio europeo nella creazione di sandbox regolamentari in cui le aziende possono testare i sistemi di IA in un ambiente controllato e la competenza (accanto alle autorità nazionali) nel fornire informazioni e risorse alle piccole e medie imprese per aiutarle a conformarsi alle norme».

[99] Art. 57, par. 16, del Regolamento (UE) 2024/1689.

[100] Art. 58, par. 1, del Regolamento (UE) 2024/1689.

ziale fornitore che soddisfi criteri di ammissibilità trasparenti ed equi[101]; che gli spazi di sperimentazione consentano un accesso ampio e paritario, tenendo il passo con la domanda di partecipazione[102]; che l'accesso agli spazi di sperimentazione sia gratuito per le PMI e le *start-up*, salvo costi straordinari che possono essere recuperati in maniera equa e proporzionata[103]; che

«i fornitori e i potenziali fornitori siano agevolati, attraverso i risultati dell'apprendimento degli spazi di sperimentazione normativa per l'IA, a conformarsi agli obblighi di valutazione della conformità di cui al presente regolamento e all'applicazione volontaria dei codici di condotta»[104]
di cui al Regolamento medesimo; che

«gli spazi di sperimentazione normativa per l'IA facilitino il coinvolgimento di altri attori pertinenti nell'ambito dell'ecosistema dell'IA, quali organismi notificati e organizzazioni di normazione, PMI, comprese start-up, imprese, innovatori, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione e poli europei dell'innovazione digitale, centri di eccellenza e singoli ricercatori, al fine di consentire e facilitare la cooperazione con i settori pubblico e privato»[105].

Solo per completezza, si segnala che il successivo art. 59 del Regolamento – non oggetto della presente trattazione la quale, come accennato, è prettamente dedicata all'analisi delle caratteristiche e delle modalità di funzionamento delle *regulatory sandboxes* – disciplina l'«Ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico» e pone alcune peculiari condizioni al ricorrere delle quali «i dati personali legalmente raccolti per altre finalità possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione»[106].
Da ultimo, merita un cenno anche l'art. 60 del Regolamento, in quanto esso prevede che «Prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA possono essere effettuate da fornitori o potenziali fornitori di sistemi di IA ad alto rischio», secondo le specifiche condizioni e il piano di prova in condizioni reali previsti dal medesimo articolo. Nuovamente, si prevede che la Commissione europea adotti specifici atti di esecuzione, in tal caso, per delineare nel dettaglio gli elementi del piano di prova in condizioni reali.
Così delineate le caratteristiche e le finalità delle *regulatory sandboxes* per l'IA, nel paragrafo che segue sarà illustrato l'approccio italiano all'utilizzo degli spazi di sperimentazione quali strumenti per «creare e gestire nuove

[101] Art. 58, par. 2 lett. *a)*, del Regolamento (UE) 2024/1689.

[102] Art. 58, par. 2 lett. *b)*, del Regolamento (UE) 2024/1689.

[103] Art. 58, par. 2 lett. *d)*, del Regolamento (UE) 2024/1689.

[104] Art. 58, par. 2 lett. *e)*, del Regolamento (UE) 2024/1689.

[105] Art. 58, par. 2 lett. *f)*, del Regolamento (UE) 2024/1689.

[106] Art. 59, par. 1, del Regolamento (UE) 2024/1689.

fattispecie giuridiche in modo flessibile, con l'obiettivo di stimolare la nascita di *legal framework*»[107].

4. *Regulatory sandboxes* per l'intelligenza artificiale nell'ordinamento italiano

4.1. Lo scenario nazionale

Il termine inglese sandbox – letteralmente "recinto di sabbia", usato comunemente per indicare uno spazio sicuro dove i bambini possono giocare – è stato adottato in ambito giuridico per descrivere un "ambiente protetto" all'interno del quale è possibile sperimentare innovazioni, in un regime di deroga rispetto alle norme ordinarie.

«Il "recinto di sabbia" assume tratti regolamentari (*regulatory*), seppur non nel senso di una tradizionale sistemazione delle fonti: esso infatti ha forza derogatoria, seppure la sua introduzione nel diritto italiano necessiti evidentemente di un appiglio normativo e di una specificazione regolamentare, in questo senso, sì, nell'ambito di un tradizionale concetto di costruzione a gradi dell'ordinamento»[108].

Il legislatore italiano ha introdotto per la prima volta nel proprio ordinamento una *regulatory sandbox* con il decreto-legge n. 34 del 30 aprile 2019, "Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi", convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58 (cd. "Decreto Crescita")[109], per la sperimentazione delle attività di innovazione tecnologica nei settori bancario, finanziario e assicurativo. In particolare, con l'art. 36, c. 2-*bis*, del decreto-legge citato, il legislatore ha previsto che, al fine di

«promuovere e sostenere l'imprenditoria, di stimolare la competizione nel mercato e di assicurare la protezione adeguata dei consumatori, degli investitori e del mercato dei capitali, nonché di favorire il raccordo tra le istituzioni, le autorità e gli operatori del settore»,

il Ministro dell'economia e delle finanze – sentiti la Banca d'Italia, la Commissione nazionale per le società e la borsa ("CONSOB") e l'Istituto per la vigilanza sulle assicurazioni ("IVASS") – adottasse entro il 31 gennaio 2021

[107] L. Torchia, *Lo Stato digitale*, cit., 189.

[108] A. Merlino, *Regulatory sandbox*, cit., 67.

[109] La disciplina della sperimentazione normativa è stata introdotta, in particolare, dall'art. 36, c. da 2 *bis* a 2 *novies*, del d.l. 34/2019. Per un'ampia ricostruzione del primo esempio di *sandbox* nell'ordinamento italiano nel settore *FinTech*, v. E. Corapi, *Regulatory sandbox nel Fintech?*, in E Corapi - R. Lener (a cura di), *I diversi settori del Fintech*, Milano, Padova, 2019, 13 ss.; A. Merlino, *Regulatory sandbox*, cit., 67 ss., Id., *La regulatory sandbox in un recente parere del Consiglio di Stato*, cit.

«uno o più regolamenti per definire le condizioni e le modalità di svolgimento di una sperimentazione relativa alle attività di tecno-finanza (FinTech) volte al perseguimento, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati»[110].

Nel definire la disciplina della sperimentazione nel settore della tecno-finanza, l'art. 36 del d.l. 34/2019 – al c. 2-*octies* – ha previsto, inoltre, l'istituzione del cd. "Comitato *FinTech*" presso il Ministero dell'economia e delle finanze, con il compito di individuare gli obiettivi, definire i programmi e porre in essere le azioni per favorire lo sviluppo del *FinTech*, nonché di formulare proposte di carattere normativo e agevolare le interlocuzioni fra operatori, istituzioni ed autorità di vigilanza e regolazione.
Al fine di regolamentare la sperimentazione, con decreto ministeriale 30 aprile 2021, n. 100, in attuazione del citato art. 36, c. 2-*bis*, del d.l. 34/2019, il Ministero dell'economia e delle finanze ha adottato il "Regolamento recante attuazione dell'articolo 36, c. 2-bis ss., del decreto-legge 30 aprile 2019, n. 34, convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58, sulla disciplina del Comitato e della sperimentazione FinTech" (il "Regolamento *FinTech*").
Per i fini che qui rilevano, appare utile richiamare quanto osservato dal Consiglio di Stato in occasione della formulazione del parere favorevole sullo schema del suddetto decreto nel gennaio 2021[111]. Dopo aver richiamato gli orientamenti dalla Commissione europea relativi alla definizione di una strategia in materia di finanza digitale[112], il Consiglio di Stato ha sottolineato la necessità di adottare un approccio regolamentare e di vigilanza che sia coordinato e condiviso tra le autorità a livello nazionale, europeo e globale, al fine di favorire l'innovazione e superare gli ostacoli al suo sviluppo, garantendo al contempo l'integrità dei mercati e la protezione degli utenti e dei risparmiatori.
Nel delineare gli elementi essenziali del primo esempio di sperimentazione in Italia[113], giova qui evidenziare che la disciplina sopra richiamata ha consentito agli operatori del settore *FinTech* di testare progetti e servizi innovativi, in un regime semplificato, transitorio, e in costante dialogo con

---

[110] Sulla sperimentazione *FinTech* in Italia, si vedano le ricognizioni pubblicate da Ministro dell'economia e delle finanze, Banca d'Italia, CONSOB e IVASS, rispettivamente: «Sperimentazione Fintech» in: *dt.mef.gov.it*; «Sandbox regolamentare», in *bancaditalia.it*; «FINTECH», in *consob.it*; «Sandbox regolamentare» in *ivass.it*.

[111] Consiglio di Stato, Sezione consultiva per gli atti normativi n. 109 del 29 gennaio 2021 (adunanza del 12 gennaio 2021). Per un esame approfondito del parere, v. A. Merlino, *La regulatory sandbox in un recente parere del Consiglio di Stato*, cit.

[112] *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE, Com/2020/591 final,* in *eur-lex.europa.eu*.

[113] Per una trattazione diffusa sul tema e, in particolare, sull'ambito di applicazione, sui requisiti di ammissione e sulla durata della sperimentazione, nonché sui compiti del Comitato *FinTech*, v. A. Merlino, *Regulatory sandbox*, cit., 67 ss. Sui primi risultati della sperimentazione, v. la relazione annuale sulle attività del Comitato *FinTech* per l'anno 2022, elaborata ai sensi dell'art. 3, c. 3, del decreto ministeriale 30 aprile 2021, n. 100, in *dt.mef.gov.it*.

le autorità di vigilanza. Al contempo, l'istituzione della suddetta *regulatory sandbox* ha consentito alle autorità responsabili per la regolamentazione di osservare da vicino le dinamiche dello sviluppo tecnologico, individuare gli interventi normativi più adeguati ed efficaci per agevolare lo sviluppo del settore di riferimento e, non da ultimo, di contenere sin dai primi momenti la diffusione di potenziali rischi.

Ai fini dell'ammissione alla sperimentazione – e nell'arco di due distinte finestre temporali, l'ultima delle quali si è conclusa nel dicembre 2023 – gli operatori interessati sono stati chiamati a presentare all'autorità di vigilanza competente per materia dei progetti dotati di specifiche caratteristiche di innovazione per il settore bancario, finanziario o assicurativo (come meglio definito dall'art. 5 del Regolamento *FinTech*), finalizzati ad arrecare benefici per gli utenti finali o a contribuire all'efficienza del mercato.

Da ultimo, è opportuno sottolineare che, per quanto la suddetta disciplina risulti innovativa nel contesto italiano, la portata derogatoria della sperimentazione è stata limitata esclusivamente agli orientamenti di vigilanza o agli atti di carattere generale dell'autorità di vigilanza e che, in ogni caso, la sperimentazione deve svolgersi nel rispetto del diritto dell'Unione europea e dei principi di proporzionalità e parità concorrenziale tra operatori (ai sensi dell'art. 14 del Regolamento *FinTech*).

Nello scenario nazionale italiano, inoltre, merita un breve cenno anche il progetto cd. "Sperimentazione Italia", introdotto con l'art. 36 del decreto-legge 16 luglio 2020 n. 76, che reca «Misure urgenti per la semplificazione e l'innovazione digitale», convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120[114].

La tipologia di tale sperimentazione normativa è stata definita multisettoriale[115], dal momento che – a differenza della *sandbox* in ambito *FinTech* – incide su più settori ed è finalizzata a favorire a «la trasformazione digitale della pubblica amministrazione, nonché lo sviluppo, la diffusione e l'impiego delle tecnologie emergenti e di iniziative ad alto valore tecnologico» (così l'art. 36, c. 1, d.l. 76/2020).

Il suddetto progetto è nato con lo scopo di incentivare *start-up*, imprese, università e centri di ricerca a sperimentare progetti tecnologicamente innovativi, per agevolare la digitalizzazione della pubblica amministrazione, creare benefici per l'ambiente e per le realtà socioeconomiche del Paese, nonché nuove opportunità di *business* per gli operatori economici e, inoltre, per migliorare la competitività e l'aggiornamento della normativa in funzione del progresso tecnologico. A tal fine, il legislatore ha previsto che l'ammissione alla sperimentazione fosse subordinata ad apposita autorizzazione della struttura della Presidenza del Consiglio dei ministri competente per la trasformazione digitale, da ottenersi previa presentazione di una «domanda di temporanea deroga alle norme dello Stato, diverse da quelle di cui al c. 3, che impediscono la sperimentazione» (art. 36, c. 1, d.l. 76/2020). In relazione a tale deroga, il legislatore ha precisato, in particolare, che essa non potesse riguardare le

[114] Sul tema, v. la descrizione del progetto "Sperimentazione Italia" fornita dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, in innovazione.gov.it.

[115] M. Trapani, *L'utilizzo delle sandboxes normative*, cit., 231.

«disposizioni a tutela della salute, dell'ambiente, dei beni culturali e paesaggistici ovvero di disposizioni penali o del codice delle leggi antimafia e delle misure di prevenzione di cui al decreto legislativo 6 settembre 2011, n. 159, né possono essere violati o elusi vincoli inderogabili derivanti dall'appartenenza all'Unione europea o da obblighi internazionali» (art. 36, c. 3, d.l. 76/2020).

In via generale, tale iniziativa reca in sé il pregio di favorire l'innovazione mediante l'introduzione di misure di semplificazione amministrativa[116]. Tuttavia, così come nel caso della sperimentazione in ambito *FinTech*, occorre notare che i limiti al potere derogatorio della sperimentazione di fatto rischiano di rappresentare un ostacolo al buon esito della sperimentazione stessa, come in parte accennato nel paragrafo 2 della presente trattazione. Dopo queste premesse sul contesto in cui si inserisce la sperimentazione normativa in Italia[117], nel paragrafo che segue saranno brevemente illustrate le iniziative presentate nel corso dell'attuale legislatura in relazione alla creazione di *regulatory sandboxes* per l'intelligenza artificiale.

4.2. Disegni di legge in materia di sperimentazione normativa per l'intelligenza artificiale e prospettive future

Le misure a sostegno dell'innovazione previste dall'*AI Act* disciplinano gli spazi di sperimentazione normativa per l'intelligenza artificiale al fine di creare i presupposti per la definizione di un quadro giuridico anche da parte dei singoli Stati membri[118].
Nel contesto nazionale, è evidente l'esigenza di agevolare lo sviluppo e la validazione di soluzioni di intelligenza artificiale anche attraverso la definizione di spazi di sperimentazione normativa controllati, come si può ricavare anche dalla lettura della «Strategia italiana per l'intelligenza artificiale

[116] Tra i progetti portati avanti nell'ambito del progetto "Sperimentazione Italia", di rilievo quelli riguardanti le cd. "smart cities", («i.e. luoghi in cui le reti e i servizi tradizionali sono resi più efficienti attraverso l'utilizzo di soluzioni digitali a beneficio dei cittadini e delle imprese»), come meglio osservato da G. Rugani, *La "legge sull'intelligenza artificiale" dell'UE come punto di arrivo e di partenza dei processi di co-regolazione*, cit., 524, 525.

[117] Per completezza sui precedenti italiani di sperimentazione normativa, si segnala che lo «*Schema definitivo di Codice dei contratti pubblici in attuazione dell'articolo 1 della legge 21 giugno 2022, n. 78, recante "Delega al Governo in materia di contratti pubblici"*» elaborato dal Consiglio di Stato nel dicembre 2022 - in *giustizia-amministrativa.it* - recava l'art. 223, dedicato alle «*Procedure sperimentali autorizzate dall'ANAC*». Tuttavia, tale articolo non è stato incluso nel testo del «*Codice dei contratti pubblici*» di cui al decreto legislativo 31 marzo 2023 n. 36. Sul punto, v. Autorità nazionale anticorruzione (ANAC), *Osservazioni di ANAC in relazione all' Atto del Governo sottoposto a parere parlamentare n. 19,* in *anticorruzione.it*.

[118] Fra gli Stati membri, la Spagna ha avviato un progetto pilota per la sperimentazione normativa nel settore dell'intelligenza artificiale (si veda il «Real Decreto 817/2023*, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial*», in *boe.es*.

2024-2026», laddove – fra le azioni strategiche per lo sviluppo di *start up* in ambito IA – si precisa che «si dovranno infine incentivare progetti mirati all'implementazione di *sandboxes*»[119].

Più nello specifico, preme qui segnalare che la suddetta esigenza è ben rappresentata anche nell'ambito delle iniziative – governativa e parlamentari – presentate nel corso dell'attuale legislatura.

Ci si riferisce, in primo luogo, al disegno di legge di iniziativa governativa recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale"[120] (il "Disegno di legge"), approvato in Consiglio dei ministri il 23 aprile 2024 e presentato al Senato il successivo 20 maggio[121].

Ai fini della presente analisi, si sottolinea che il Disegno di legge contiene specifiche previsioni in materia di spazi di sperimentazione nell'articolo dedicato alle «Autorità nazionali per l'intelligenza artificiale».

In particolare, tale articolo «al fine di garantire l'applicazione e l'attuazione della normativa nazionale e dell'Unione europea in materia di intelligenza artificiale» prevede la designazione dell'Agenzia per l'Italia digitale (AgID) e dell'Agenzia per la cybersicurezza nazionale (ACN)[122] quali Autorità nazionali per l'intelligenza artificiale e, inoltre, per quanto qui maggiormente rileva, prevede che tali Autorità «ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea».

Il Disegno di legge prevede, poi, una delega al Governo per l'adeguamento della normativa nazionale all'*AI Act* (il cui art. 57, come indicato nel precedente paragrafo 3, dispone l'obbligo per ciascuno Stato membro di istituire almeno uno spazio di sperimentazione normativa per l'intelligenza artificiale, a livello nazionale o congiuntamente con le autorità competenti di altri Stati membri). In tale ambito, per quel che qui rileva, inoltre, si segnala che, fra i principi e i criteri direttivi specifici a cui deve attenersi il Governo nell'esercizio della suddetta delega, vi è anche «la valorizzazione delle attività di ricerca e di trasferimento tecnologico in materia di intelligenza artificiale […] mediante disposizioni finalizzate» anche al perseguimento del seguente obiettivo: agevolare il coinvolgimento del sistema dell'università e della ricerca nella promozione, nella realizzazione e nell'utilizzo di spazi di sperimentazione normativa in collaborazione con il mondo produttivo.

Al fine di sottolineare il rilievo che il tema assume nel contesto nazionale,

---

[119] *Strategia italiana per l'intelligenza artificiale 2024-2026*, pubblicata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri, in *innovazione.gov.it*, 28.

[120] Atto Senato ("A.S.") n. 1146, in *senato.it*

[121] Le considerazioni svolte nella presente trattazione sono basate sul testo presentato al Senato e non riguardano gli emendamenti che potranno essere elaborati nel corso dell'*iter* legislativo, non conoscibili al momento in cui si scrive. Il fine della presente trattazione è, infatti, quello di testimoniare l'attenzione per l'utilizzo degli spazi di sperimentazione normativa nel contesto dell'ordinamento italiano, indipendentemente dalla formulazione definitiva che avranno le previsioni in esame.

[122] Ai sensi del medesimo articolo del Disegno di legge, dedicato alle Autorità nazionali per l'intelligenza artificiale, «Restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali».

occorre fare un breve cenno, inoltre, alle iniziative parlamentari che, nel corso dell'attuale legislatura, hanno anch'esse messo in risalto la necessità di creare spazi di sperimentazione per favorire l'innovazione e lo sviluppo dei sistemi di intelligenza artificiale.

Ci si riferisce, innanzitutto, alla proposta di legge recante "Disposizioni concernenti l'adozione di una disciplina temporanea per la sperimentazione dell'impiego di sistemi di intelligenza artificiale"[123], presentata l'11 aprile 2023. Essa, che si compone di due articoli, prevede la creazione di uno spazio tecnico-normativo sperimentale e temporaneo per le attività che impiegano sistemi di intelligenza artificiale, con l'obiettivo di promuovere l'innovazione e consentire lo sviluppo dell'intelligenza artificiale nel territorio nazionale. A tale scopo, essa prevede, inoltre, l'adozione di uno o più regolamenti – con decreto del Presidente del Consiglio dei ministri – per definire le condizioni e le modalità di svolgimento della sperimentazione e, inoltre, prevede l'istituzione di un Comitato permanente per l'intelligenza artificiale presso la Presidenza del Consiglio dei ministri.

Un'altra proposta di legge significativa è quella presentata il 2 ottobre 2023 e reca "Disposizioni concernenti la fornitura e l'impiego dei sistemi di intelligenza artificiale"[124]. Tale proposta ha un contenuto più complesso e articolato, suddiviso in quattordici articoli e, *inter alia*, prevede – come la proposta precedentemente citata – la creazione di uno spazio tecnico-normativo sperimentale e temporaneo per le attività che sviluppano i sistemi di IA, finalizzato a testare l'impatto di queste tecnologie in Italia. Inoltre, prevede anch'essa l'istituzione di un Comitato nazionale per i sistemi di intelligenza artificiale presso la Presidenza del Consiglio dei ministri.

Da ultimo, si segnalano il disegno di legge recante "Norme per lo sviluppo e l'adozione di tecnologie di intelligenza artificiale", presentato il 12 marzo 2024[125], e il disegno di legge – congiunto a quest'ultimo – recante "Disposizioni concernenti l'adozione di una disciplina temporanea per la sperimentazione dell'impiego di sistemi di intelligenza artificiale", presentato il 23 aprile 2024[126].

Le iniziative fin qui illustrate dimostrano la crescente attenzione delle istituzioni italiane per il tema della sperimentazione normativa[127], quale strumento fondamentale per creare un adeguato bilanciamento fra regolazione e innovazione, nel più ampio ambito della definizione di una strategia italiana per l'intelligenza artificiale.

In conclusione, può affermarsi che l'utilizzo delle *regulatory sandboxes* rappresenta una risorsa strategica per l'Italia, poiché consente di creare un ambiente favorevole ad attrarre talenti imprenditoriali e stimolare la crescita del sistema produttivo. Questo strumento permette alle aziende di testare soluzioni e prodotti nuovi in un contesto regolamentato, ma flessibile, riducendo i costi e i rischi normativi legati all'innovazione.

Le *regulatory sandboxes*, dunque, non solo possono accelerare il processo di

---

123 Atto Camera ("A.C.") n. 1084, in *camera.it*.

124 A.C. n. 1444, in *camera.it*.

125 A.S. n. 1066, in *senato.it*.

126 A.S. n. 1166, in.*senato.it*.

127 G. Centemero - P. Longo, *Regulatory sandbox*, cit., 128-133.

sperimentazione, ma hanno anche il pregio di facilitare la collaborazione tra le istituzioni e il mercato e la nascita di un ecosistema favorevole all'innovazione. Inoltre, gli spazi di sperimentazione normativa – se ben progettati e regolamentati – possono agevolare il posizionamento dell'Italia nel contesto europeo e internazionale, quale polo di innovazione tecnologica e imprenditoriale e, per l'effetto, attirare imprese, talenti e investimenti anche oltre i confini nazionali, con un potenziale positivo impatto su settori strategici per la crescita del Paese.

5. Conclusioni

La regolamentazione dell'intelligenza artificiale pone il legislatore di fronte a sfide complesse: è difficile regolamentare una tecnologia in fase di sviluppo iniziale, quando ancora non sono note le sue caratteristiche tecniche e non è chiaro se essa provochi dei rischi né, in ipotesi, quale sia il livello di tali rischi; è altrettanto complicato, però, intervenire quando ormai la tecnologia è diffusa e radicata[128].

Per risolvere tale dilemma, il regolamento europeo sull'intelligenza artificiale sostiene l'innovazione prevedendo l'istituzione, a livello nazionale, di spazi di sperimentazione normativa ("*regulatory sandboxes*"), in considerazione della capacità di questi ultimi di agevolare la creazione di un equilibrio tra lo sviluppo tecnologico e la tutela dei diritti fondamentali e della sicurezza pubblica. Le *regulatory sandboxes* permettono, infatti, di testare – in un ambiente controllato da un'autorità competente - nuove applicazioni di intelligenza artificiale prima che queste siano immesse sul mercato, conformemente ad un piano dello spazio di sperimentazione e per un periodo di tempo limitato.

Inoltre, gli spazi di sperimentazione normativa hanno il pregio di coniugare e promuovere la sperimentazione di nuove tecnologie e di nuovi approcci normativi, consentendo così al legislatore di acquisire competenze tecniche e regolamentari in costante dialogo con gli innovatori.

Tuttavia, ci sono anche alcuni limiti associati all'utilizzo delle *regulatory sandboxes*, fra cui – per quanto rileva ai fini della presente trattazione – uno dei principali è costituito dal pericolo di frammentazione nell'intera Unione europea, il che vanificherebbe gli sforzi fatti dal legislatore europeo per la creazione del mercato unico e per la promozione dell'innovazione. Per cogliere pienamente i benefici derivanti dall'introduzione delle *regulatory sandboxes* negli ordinamenti nazionali, occorrerà, dunque, attendere l'adozione, da parte della Commissione europea, degli specifici atti di esecuzione con i quali saranno precisati le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa per l'intelligenza artificiale.

[128] G.M. Riccio, *Intelligenza artificiale e regulatory sandbox*, cit., 59.

Abstract

Il rapido progresso delle tecnologie emergenti, in particolare dell'intelligenza artificiale, anima il dibattito giuridico nell'era digitale: la posizione di chi ritiene che la regolazione rappresenti un freno per lo sviluppo tecnologico si contrappone a quella di chi ritiene, al contrario, che l'innovazione comporti un numero talmente elevato di rischi da dover essere necessariamente regolata. Per bilanciare queste posizioni ed al fine di creare un equilibrio tra regolazione e innovazione, occorre che il diritto si evolva al pari della tecnologia. Strumenti normativi innovativi, come le regulatory sandboxes, favoriscono la collaborazione tra regolatori e innovatori e consentono di testare nuove tecnologie sotto la supervisione delle autorità competenti. Il presente contributo si propone di analizzare le caratteristiche distintive delle regulatory sandboxes e di valutarne il rilievo nel contesto del Regolamento europeo sull'intelligenza artificiale e delle iniziative normative intraprese a livello italiano.

The rapid advancement of emerging technologies, particularly artificial intelligence, fuels the legal debate in the digital era. The stance of those who believe regulation hinders technological development contrasts with the view that innovation entails such a high number of risks that it must necessarily be regulated. To balance these positions and create equilibrium between regulation and innovation, the law must evolve alongside technology. Innovative regulatory tools, such as regulatory sandboxes, foster collaboration between regulators and innovators, allowing new technologies to be tested under the supervision of competent authorities. This paper aims to analyse the distinctive characteristics of regulatory sandboxes and assess their relevance in the context of the European Regulation on Artificial Intelligence and the regulatory initiatives undertaken at the national level in Italy

Keywords: regulatory sandboxes – sperimentazione normativa - intelligenza artificiale – AI Act – better regulation

Note a sentenza

Diritto di cronaca e limiti alla pubblicazione della corrispondenza telematica: note a margine del provvedimento del Garante per la protezione dei dati personali del 12 febbraio 2025*

Pietro Villaschi

Autorità garante per la protezione dei dati personali, provvedimento del 12 febbraio 2025, doc. web 10103541

Con il provvedimento del 12 febbraio 2025, il Garante per la protezione dei dati personali si occupa di un caso in cui a venire in rilievo sono i limiti alla pubblicazione della messaggistica telematica di natura privata. Trattasi di una decisone sintetica, ma foriera di innumerevoli spunti di riflessione. Dal tema dell'applicazione della legge sul diritto d'autore, a quello della valutazione del requisito dell'essenzialità dell'informazione pubblicata rispetto a fatti di interesse pubblico, a quello della tutela dei dati personali, il provvedimento intercetta una serie di profili di rilievo costituzionale di particolare interesse, nel tentativo di tracciare una linea di confine tra il diritto del giornalista di informare (e il correlato diritto dell'opinione pubblica ad essere informata), da una parte, e quello alla riservatezza delle persone coinvolte, dall'altra. La delicatezza di tale bilanciamento si rende, peraltro, evidente, se si considera che i messaggi in questione sono stati estrapolati dalle chat WhatsApp del gruppo parlamentare di Fratelli d'Italia, ossia del partito attualmente di maggioranza relativa, e che a venire in rilievo sono forme di comunicazione, quelle telematiche, che per le loro intrinseche caratteristiche sono idonee ad aprire squarci particolarmente significativi sull'intimità dei corrispondenti.

Sommario

1. Premessa. – 2. Una decisione sintetica, ma foriera di spunti di riflessione. – 2.1. La qualificazione delle *chat* come corrispondenza. – 2.2. La legge sul diritto d'autore e i limiti alla pubblicazione della corrispondenza

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

privata. – 2.3. Il diritto di cronaca e la tutela dei dati personali: un binomio difficile, ma non impossibile. – 3. Considerazioni finali.

1. Premessa

Il 6 febbraio scorso veniva messo in vendita il volume "Fratelli di chat. Storia segreta del partito di Giorgia Meloni" di Giacomo Salvini, edito da *PaperFirst* ("by SEIF S.p.A." – Società editoriale il Fatto) e diretto – come si evince dalla presentazione disponibile sul sito dell'editore stesso – a ricostruire la storia «del partito di Giorgia Meloni attraverso le chat dei parlamentari, ministri e dirigenti di Fratelli d'Italia».
In particolare, all'interno del volume vengono riportate le trascrizioni, con virgolettati, di diversi messaggi scambiati sui gruppi *WhatsApp* dei gruppi parlamentari del partito dal 2018 al 2024.
Il Garante per la protezione dei dati personali, con provvedimento del 12 febbraio 2025[1], inviava un avvertimento formale alla società, ritenendo che la pubblicazione delle suddette *chat* violasse la disciplina sul diritto d'autore, la normativa in materia di protezione dei dati personali, le regole deontologiche della professione giornalistica, nonché i principi generali di liceità, correttezza, minimizzazione ed essenzialità dell'informazione.
Il ragionamento del Garante muove dal presupposto che, come recentemente statuito dalla Corte costituzionale con la sentenza n. 170 del 2023[2] e, in seguito, anche dalla giurisprudenza di legittimità[3], le comunicazioni scambiate sui servizi di messagistica telematica debbono essere qualificate a tutti gli effetti come "corrispondenza", godendo, pertanto, della protezione offerta dall'art. 15 Cost. per la generalità dei cittadini e delle garanzie ulteriori di cui all'art. 68, c. 3, Cost. quando mittente e/o destinatario della conversazione sia un parlamentare.
Da quanto precede discenderebbe, anzitutto, secondo il Garante, l'appli-

[1] Garante per la protezione dei dati personali, provvedimento del 12 febbraio 2025, iscritto al Registro dei provvedimenti n. 60 del 12 febbraio 2025.

[2] Sulla sentenza 27 luglio 2023, n. 170, che ha segnato un punto di svolta nella giurisprudenza costituzionale in materia di corrispondenza, cfr., tra gli altri, G. Guzzetta, *La nozione di comunicazione e altre importanti precisazioni della Corte costituzionale sull'art. 15 della Costituzione nella sentenza n. 170 del 2023*, in *Federalismi*, 21, 2023, 81 ss.; N. D'Anza, *La Corte costituzionale estende ai soggetti non parlamentari l'immunità di cui all'art. 68, comma 3, Cost. con riguardo alla corrispondenza scambiata con membri del Parlamento*, in *Forum di Quaderni costituzionali*, 2, 2023, 105 ss.; E. Furno, *Libertà di comunicazione e diritto alla riservatezza del parlamentare nelle sentenze nn. 157 e 170 del 2023 della Corte Costituzionale in tema di intercettazioni*, in *Federalismi*, 25, 2023, 37 ss.; L. M. Tonelli, *Un'estensione (eccessiva?) della nozione di «corrispondenza» in una recente sentenza della Corte costituzionale*, in *Osservatorio Aic*, 1, 2024, 266 ss.; A. Iacoviello, *I riflessi della sentenza n.170/2023 della Corte costituzionale sulle procedure per il sequestro della corrispondenza elettronica e delle comunicazioni archiviate su dispositivi di tipo informatico e telematico*, in *Nomos*, 1, 2024, 1 ss.; sia consentito, infine, un rinvio anche a P. Villaschi, *La sentenza n. 170 del 2023: la Corte costituzionale chiarisce il perimetro della nozione di corrispondenza e torna sull'interpretazione della legge n. 140 del 2003*, in questa *Rivista*, 2, 2023, 360 ss.

[3] In particolare, ci si riferisce a Cass. pen., sez. VI, 13 gennaio 2025, n. 1269 (rv. 287504-01), a commento della quale v. F. Ballesi, *La sentenza n. 1269/2025 della Corte di cassazione ed i limiti all'acquisizione nel processo penale della messaggistica istantanea mediante screenshot*, in *Giurisprudenza penale*, 2, 2025, 1 ss.

cazione dell'art. 93 della legge n. 633 del 1941 (ossia la legge sul diritto d'autore), che subordina al consenso dell'autore e del destinatario – nel caso di specie insussistenti – la pubblicazione della corrispondenza qualora questa abbia «carattere confidenziale o si riferisca alla intimità della vita privata».

Inoltre, la pubblicazione delle *chat* in questione avrebbe determinato una violazione della disciplina in materia di protezione dei dati personali. Ad avviso del Garante, infatti, la pubblicazione dei virgolettati di tali *chat* – seppur in alcuni casi per ricostruire le vicende politiche e personali che hanno caratterizzato la storia del partito – non può ritenersi conforme al criterio dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico di cui all'art. 137, c. 3, del "Codice in materia di protezione dei dati personali"[4] e all'art. 6 delle "Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica"[5], integrando, invece, una violazione di tali disposizioni, rilevante ai sensi dell'art. 2-quater, c. 4, del "Codice in materia di protezione dei dati personali", che qualifica il rispetto delle regole deontologiche come «condizione essenziale per la liceità e correttezza del trattamento». Nella prospettiva del Garante, la narrazione dei contenuti delle conversazioni, anche riportando virgolettati di *chat* private, non costituirebbe, infatti, un elemento necessario in rapporto alla finalità informativa perseguita, potendosi piuttosto ricorrere a soluzioni maggiormente conformi alla disciplina in materia di protezione dei dati personali, considerando anche le implicazioni che tale forma narrativa avrebbe rispetto alla dignità dei soggetti terzi citati. Muoverebbe in questa direzione anche il fatto che l'essenzialità dell'informazione è da interpretarsi con particolare rigore in relazione a notizie con le quali, nell'affrontare e descrivere temi anche di pubblico interesse, vengano riportati dettagli che riguardano minori ai sensi dell'art. 7 delle Regole deontologiche.

Infine – osserva il Garante – la pubblicazione in oggetto avrebbe determinato la violazione del diritto alla riservatezza e alla protezione dei dati personali non solo dei soggetti autori o destinatari delle *chat*, ma anche dei terzi citati all'interno delle comunicazioni.

Di qui la decisione di inviare un avvertimento formale all'editore, riservandosi l'adozione di ulteriori provvedimenti in esito all'istruttoria.

---

[4] D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)".

[5] "Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica", pubblicate, ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, nella Gazzetta ufficiale del 4 gennaio 2019, n. 3 (v. provvedimento del Garante per la protezione dei dati personali del 29 novembre 2018, pubblicato nel Registro dei provvedimenti n. 491 del 29 novembre 2018). In seguito, con il Decreto del Ministro della Giustizia del 31 gennaio 2019, pubblicato nella Gazzetta Ufficiale n. 35 dell'11 febbraio 2019, tali Regole deontologiche sono state riportate nell'allegato A del decreto legislativo 30 giugno 2003, n. 196 in sostituzione del corrispondente Codice di deontologia.

2. Una decisione sintetica, ma foriera di spunti di riflessione

Il caso esaminato dal Garante per la protezione dei dati personali ha ad oggetto i limiti che il giornalista incontra nella pubblicazione di *chat* private, intercettando il delicato equilibrio che sussiste tra esercizio del diritto di cronaca e tutela della riservatezza in un contesto, quello digitale, segnato dall'uso massivo di comunicazioni di natura telematica.
Trattasi di un tema dal quale si irradiano profili di particolare interesse, che, tuttavia, nel corpo di una motivazione piuttosto concisa, faticano ad emergere con chiarezza.

2.1. La qualificazione delle *chat* come corrispondenza

Anzitutto, a porsi è il tema della qualificazione giuridica delle *chat* in questione.
Sul punto, il Garante non può che richiamare la recente giurisprudenza costituzionale che, con la sentenza n. 170 del 2023, ha sussunto le comunicazioni telematiche, ancorché inviate e conservate nel dispositivo del destinatario, sotto la nozione di corrispondenza.
In quell'occasione, la Corte costituzionale era stata adita dal Senato, che aveva sollevato un conflitto di attribuzione tra poteri dello Stato nei confronti della Procura della Repubblica di Firenze a seguito dell'acquisizione da parte di quest'ultima di plurime comunicazioni telematiche del senatore Matteo Renzi nell'ambito di un procedimento penale a suo carico, assumendo che la Procura avesse leso le proprie attribuzioni costituzionali, dal momento che aveva acquisito la corrispondenza di un membro del Parlamento in assenza della necessaria autorizzazione preventiva della Camera di appartenenza, richiesta dall'art. 68, c. 3, Cost.
La Corte costituzionale, nell'accogliere il ricorso, ha segnato un precedente di indubbio rilievo, destinato – come il provvedimento del Garante qui in commento dimostra – ad avere riflessi ben al di là dei confini del caso specifico dal quale era originato il conflitto.
La questione di fondo su cui la Corte era chiamata a pronunciarsi riguardava, infatti, il perimetro della nozione di corrispondenza e, in particolare, la qualificazione da darsi alle comunicazioni telematiche (come *e-mail*, *sms*, *WhatsApp*). Un consolidato orientamento della giurisprudenza di legittimità[6] era, infatti, costante nell'affermare che gli *sms*, i *WhatsApp* e le *e-mail* avrebbero cessato di essere "corrispondenza" una volta recapitati sul dispositivo del destinatario, dovendo, al contrario, essere considerati come meri "documenti", sicché sarebbe stata legittima la loro libera acquisizione mediante riproduzione fotografica ai sensi dell'art. 234 c.p.p., non trovando applicazione né le garanzie previste per le intercettazioni ex art. 266 ss.

[6] Tra le ultime, Cass. pen., sez. II, 19 ottobre 2022, n. 39529, in *Quotidiano Giuridico*, 2022; Cass. pen., sez. VI, 8 giugno 2022, n. 22417, in *Quotidiano Giuridico*, 2022; Cass. pen., sez. V, 6 maggio 2021, n. 17552, in *Quotidiano Giuridico*, 2021.

c.p.p., né quelle relative al sequestro di corrispondenza di cui all'art. 254 c.p.p.[7].

La Corte ha ribaltato questa impostazione, qualificando come corrispondenza i messaggi *WhatsApp* e di posta elettronica anche (e soprattutto) nella loro dimensione "statica", con conseguente applicazione, per la generalità dei cittadini, delle garanzie costituzionali di cui all'art. 15 Cost. – ossia la riserva di legge e quella di giurisdizione[8] – e, per i parlamentari, di quelle ulteriori di cui all'art. 68, c. 3, Cost., ossia l'autorizzazione al sequestro da parte della Camera di appartenenza[9].

La nozione di corrispondenza, infatti, è, ad avviso della Consulta, da intendersi in senso piuttosto ampio, così da abbracciare «ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati, notizie) tra due o più persone determinate»[10], che non sia in presenza e a prescindere dalle caratteristiche tecniche del mezzo utilizzato. Decisivo piuttosto è il fatto che la comunicazione sia mantenuta riservata, il che è garantito, per la corrispondenza epistolare-cartacea, dalla chiusura in una busta del testo scritto e, per quella elettronica, dalla visibilità esclusiva del messaggio da parte dei soggetti legittimati ad avere accesso al sistema informatico.

Ma, soprattutto, è un argomento di ordine logico a fare breccia. Osserva la Corte costituzionale che, escludendo dal perimetro della nozione di corrispondenza le comunicazioni telematiche (e in particolare quelle conservate nel dispositivo del destinatario), si svuoterebbero di senso le guarentigie

---

[7] Sui diversi regimi acquisitivi si veda F. Zacchè, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.*, 4, 2013, 106; M. Pittitutti, *Profili processuali della prova informatica*, in L. Marafioti-G. Paolozzi (a cura di), *Incontri ravvicinati con la prova penale. Un anno di seminari a Roma Tre*, Torino, 2014, 59 ss.

[8] Sulla libertà di corrispondenza, sebbene con riferimento a quella, tradizionale, cartacea-epistolare, si vedano le riflessioni di P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 163 ss.; P. Barile-E. Cheli, *Corrispondenza (libertà di)*, in *Enc. Dir.*, X, Milano, 1962, 743 ss.; P. Caretti, *Corrispondenza (libertà di)*, in *Digesto pubbl.*, IV, Torino, 1989, 200 ss..; A. Pace, *Art. 15*, in *Comm. Cost. Branca*, Bologna-Roma, 1977, 80 ss.; A. Pace, *Problematica delle libertà costituzionali. II. Parte speciale*, Padova, 1992, 1 ss.; P. Caretti, *Diritto dell'informazione e della comunicazione: stampa, radiotelevisione, telecomunicazioni, teatro e cinema*, Bologna, 2005; G. M. Salerno, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in R. Nania-P. Ridola (a cura di), *I Diritti costituzionali*, Torino, I, 2001, 417 ss.; F. Donati, *Art. 15*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Commentario alla Costituzione*, vol. 1, Torino, 2006, spec. 362 ss.

Per un primo inquadramento delle nuove forme di comunicazione elettronica, v. A. Valastro, *Libertà di comunicazione e nuove tecnologie*, Milano, 2001; A. Albanesi-A. Valastro-R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Padova, 2013.

[9] Sulle guarentigie di cui all'art. 68, c. 3, Cost. la letteratura è particolarmente ampia con riguardo al tema delle intercettazioni telefoniche, su cui, *ex plurimis*, cfr. N. Zanon, *Il regime delle intercettazioni "indirette" e "occasionali" fra principio di parità di trattamento davanti alla giurisdizione e tutela della funzione parlamentare*, in *Federalismi*, 23, 2007, 1 ss.; T. F. Giupponi, *Le intercettazioni «indirette» nei confronti dei parlamentari: cronaca di un'illegittimità costituzionale (pre)annunciata*, in *Quaderni costituzionali*, 1, 2008, 150 ss.; V. Grevi, *Sui limiti di utilizzabilità delle intercettazioni «indirette» (casuali e non casuali) operate nei confronti di un membro del Parlamento*, in *Giur. cost.*, 6, 2007, 4391 ss.; M. Cerase, *Intercettazioni parlamentari: entra la Corte*, in *Il Foro it.*, 1, 2008, 15 ss. Il profilo del sequestro di corrispondenza è stato, invece, più di rado affrontato dalla dottrina, nonché, prima della sentenza n. 170 del 2023, anche dalla Corte costituzionale, cfr. M. Cerase, *Art. 68*, in R. Bifulco-A. Celotto-M. Olivetti (a cura di), *Commentario alla Costituzione*, Torino, 2006, 1304 ss.

[10] Corte cost., sent. 27 luglio 2023, n. 170, *Considerato in diritto* n. 4.2.

costituzionali in materia, dal momento che nel caso degli *sms*, delle *e-mail* e dei messaggi *WhatsApp* all'invio segue immediatamente la ricezione. Resterebbero, quindi, coperte esclusivamente ipotesi minoritarie e residuali (data, ormai, la marginalità della corrispondenza cartacea).

In definitiva, nel caso delle comunicazioni telematiche, il requisito dell'attualità della comunicazione non si esaurisce, ad avviso della Consulta, automaticamente con la ricezione del messaggio e la presa di cognizione del suo contenuto da parte del destinatario, ma permane finché la comunicazione conservi attualità e interesse per i corrispondenti, venendo meno solo quando il decorso del tempo o altra causa abbia trasformato il messaggio in un documento storico, cui attribuire un valore retrospettivo, affettivo, collezionistico, artistico, scientifico o probatorio[11].

La svolta operata dalla Corte è stata, in seguito, accolta anche dalla giurisprudenza di legittimità.

Con la sentenza n. 1269 del 13 gennaio 2025[12], la Corte di Cassazione ha, infatti, qualificato i messaggi di natura telematica come corrispondenza, rivedendo il precedente orientamento. In quella circostanza, gli ermellini dovevano, in particolare, verificare l'utilizzabilità o meno in giudizio di una serie di *chat* estrapolate dall'archivio telefonico dell'imputato, senza che fosse stato disposto un provvedimento di sequestro dall'autorità giudiziaria[13].

La Suprema Corte ha rilevato che «le garanzie di salvaguardia del diritto alla riservatezza dei dati archiviati nella memoria di un telefono cellulare, a seguito della sentenza della Corte cost. numero 170 del 2023, hanno visto ampliare il loro campo di applicazione attraverso la riconosciuta natura di corrispondenza anche alle comunicazioni non più in itinere ma acquisite dopo la loro ricezione da parte del destinatario».

Ne consegue che, ad avviso dei giudici di legittimità, anche a queste forme di comunicazione si debbono applicare le garanzie di cui all'art. 15 Cost. – e in particolare la possibilità di limitarle soltanto per atto motivato dall'autorità giudiziaria – e ciò finché la comunicazione conservi carattere di attualità e di interesse per i corrispondenti. La messaggistica archiviata nei telefoni cellulari non può essere considerata, nella prospettiva degli ermellini, un mero documento liberamente acquisibile nel procedimento, ma richiede l'assoggettamento alla disciplina dell'art. 254 c.p.p., che impone un provvedimento motivato dell'autorità giudiziaria, al fine di giustificare il sacrificio della segretezza della corrispondenza. È così esclusa la possibilità di un accesso diretto da parte della polizia giudiziaria, che ha solo il potere di acquisire materialmente il dispositivo elettronico analogamente a quanto previsto per l'invio della corrispondenza postale[14].

---

[11] In definitiva, pertanto, la Corte costituzionale ritiene sussistenti nel caso delle comunicazioni di natura telematica tutti i requisiti integranti la nozione di corrispondenza, ossia la segretezza, l'inter-subiettività e l'attualità della comunicazione. Su questi elementi, si veda, più diffusamente, l'analisi di P. Caretti, *Corrispondenza (libertà di*), cit., 200 ss.

[12] Cass. pen., sez. VI, 13 gennaio 2025, n. 1269 (rv. 287504-01).

[13] L'acquisizione dei contenuti delle *chat* era avvenuta sulla base di un rilievo fotografico operato dalla stessa polizia giudiziaria, ossia uno *Screenshot*, delle *chat WhatsApp*, senza che vi fosse stato un provvedimento di sequestro di competenza dell'autorità giudiziaria.

[14] Sulle ricadute in termini di garanzie di cui al codice di procedura penale, cfr. F. Ballesi,

Orbene, questa digressione risulta necessaria per contestualizzare il provvedimento qui in commento.
La qualificazione come corrispondenza, infatti, dei messaggi risulta preliminare, nella prospettiva del Garante, al prosieguo del ragionamento.
Va qui precisato che trattasi, in verità, di una questione non sconosciuta all'autorità deputata a garantire l'osservanza della disciplina in tema di protezione dei dati personali. In qualche rara pronuncia[15], il tema della qualificazione dei messaggi telematici era, infatti, già emerso. Anche in quelle ipotesi, pur senza approfondire la questione della natura giuridica di tali forme di comunicazione, il Garante aveva dato per scontato che fossero forme di corrispondenza.
Ora, la certa sussunzione dei messaggi telematici sotto la nozione di corrispondenza consentirebbe, nella prospettiva del Garante, di innalzare il livello di tutela nei confronti dei corrispondenti, siano essi parlamentari che non[16].
A venire qui in rilievo non è, tuttavia, l'art. 68, c. 3, Cost.: la disposizione costituzionale in parola – diretta a tutelare lo *status* del parlamentare e, di riflesso, l'istituzione cui questi fa parte – si applica, infatti, alla particolare ipotesi del sequestro di corrispondenza di membri del Parlamento, postulando, a tal fine, che l'autorità giudiziaria richieda l'autorizzazione della Camera di appartenenza prima di procedere al sequestro[17].
In questo caso, la sussunzione sotto la nozione di corrispondenza delle comunicazioni di natura elettronica apre, piuttosto, all'applicazione della legge sul diritto d'autore, che, nella prospettiva del Garante, si configura come una disciplina aggiuntiva e supplementare rispetto a quella, più generale, in tema di protezione dei dati personali.
Trattasi, come si dirà meglio in seguito (*infra*, §§ 2.2, 2.3), di una linea argomentativa che convince, tuttavia, solo in parte.

La sentenza n. 1269/2025 della Corte di cassazione, cit., 1 ss.

[15] Si fa qui riferimento al provvedimento del 6 maggio 2013 del Garante per la protezione dei dati personali, iscritto al Registro dei provvedimenti n. 229 del 2013, e al provvedimento del 2 febbraio 2017 sempre del Garante per la protezione dei dati personali, iscritto al Registro dei provvedimenti n. 36 del 2 febbraio 2017 (su cui, più diffusamente, *infra* §§ 2.2 e 2.3).

[16] Le *chat* pubblicate nel volume riguardano, infatti, non solo membri del Parlamento, ma anche ministri, dirigenti o iscritti al partito e, infine, terzi privati cittadini.

[17] Sulle specifiche modalità, ai sensi dell'art. 68, c. 3, Cost. e della l. n. 140 del 2003, con cui richiedere l'autorizzazione alla Camera competente nel caso di un sequestro di corrispondenza di membri del Parlamento, si è espressa la Corte costituzionale, sempre con la sent. 27 luglio 2023, n. 170, elaborando il seguente modulo procedurale, applicabile specie qualora, come sovente accade, la corrispondenza sia rinvenuta su dispositivi in uso a terzi (come nel caso oggetto della pronuncia della Consulta): a) nessuna preclusione discende dall'art. 68, c. 3, Cost. per disporre il sequestro del dispositivo di proprietà di un terzo; b) qualora ciò avvenga, nessuna verifica in merito alla direzione dell'atto di indagine è necessaria da parte dell'autorità inquirente; c) tuttavia, nel caso in cui siano rinvenute all'interno del dispositivo sequestrato conversazioni con un parlamentare, il pubblico ministero è tenuto a richiedere, immediatamente, l'autorizzazione preventiva, *ex* art. 4 della l. 140 del 2003, alla Camera di appartenenza, altrimenti l'estrazione della corrispondenza tra terzo e parlamentare è illegittima. A commento della soluzione individuata dalla Corte e delle conseguenti ricadute applicative, sia consentito rinviare a P. Villaschi, *La sentenza n. 170 del 2023*, cit., spec. 379-381.

2.2. La legge sul diritto d'autore e i limiti alla pubblicazione della corrispondenza privata

L'art. 93 della legge n. 633 del 1941 (c.d. legge sul diritto d'autore) prevede che, per pubblicare corrispondenza di carattere confidenziale o che si riferisca all'intimità privata della persona, occorre munirsi del consenso dei corrispondenti. Il testo della legge, risentendo del periodo storico in cui fu redatto, fa riferimento esclusivamente agli epistolari, alle corrispondenze epistolari, alle memorie familiari e personali e, infine, a tutti gli altri scritti della medesima natura.
Il Garante, con un'interpretazione estensiva, che persuade e che è coerente con l'indirizzo inaugurato dalla Corte costituzionale con la sentenza n. 170 del 2023 (*retro* § 2.1), estende la disciplina anche alle forme di corrispondenza più moderne, ossia quelle telematiche.
La legge sul diritto d'autore pone tale limite alla pubblicazione, muovendo dal presupposto che se oggetto della corrispondenza sono scritti creativi ed originali, ovvero riproduzioni di opere d'arte appartenenti al campo della letteratura, l'autore sarà titolare dei diritti di natura morale ed economica secondo la disciplina generale in tema di diritto d'autore. Se, al contrario, come nel caso delle *chat* riprodotte nel volume "Fratelli di chat. Storia segreta del partito di Giorgia Meloni", tali caratteristiche manchino, la corrispondenza è, ai sensi del diritto d'autore, liberamente riproducibile, a patto, tuttavia, di salvaguardare il diritto al segreto e alla riservatezza di quanto in essa contenuto. Proprio per tale ragione, quando la corrispondenza ha carattere confidenziale o è relativa all'intimità della vita privata, i diritti dello scrittore-autore delle lettere sono vincolati alla prestazione del consenso della persona cui tali fatti si riferiscono. In altre parole, il limite posto alla pubblicazione è rappresentato dalla tutela del diritto alla segretezza della corrispondenza e dei fatti personali ivi narrati[18].
Tale diritto al segreto epistolare è bilaterale, poiché devono prestare il proprio consenso alla pubblicazione sia lo scrivente sia il destinatario delle missive; è disponibile, in quanto il titolare può liberamente rinunciarvi autorizzando la pubblicazione; è, infine, irrevocabile, poiché una volta reso noto il contenuto segreto delle missive viene meno il segreto su certi fatti privati, ossia il bene giuridico che la legge intende tutelare[19]. Il consenso che legittima la cessazione del segreto può essere anche dato dopo la morte dell'autore o del destinatario dal coniuge o dai figli; in loro mancanza, dai genitori; se questi mancano, dai fratelli e dalle sorelle; se non vi sono anche questi ultimi, dagli ascendenti e discendenti diretti fino al quarto grado. Nel caso di dissenso tra le persone sopra indicate decide l'autorità giudiziaria (art. 93, c. 2 e 3).
Ovviamente, se l'epistolario e gli altri scritti non hanno carattere confidenziale o non contengono fatti relativi all'intimità della vita privata, la pubblicazione è libera.
Anche il diritto al segreto epistolare, tuttavia, subisce alcune limitazioni, in

[18] Lo evidenzia, chiaramente, E. Poddighe, *Riserbo della corrispondenza e opera dell'ingegno postuma (a proposito delle lettere di Federico Fellini)*, in *Dir. informatica*, 2, 1999, 413.

[19] Cfr., sul punto, P. Greco-P. Vercellone, *I diritti sulle opere dell'ingegno*, Torino, 1974, 415.

particolare quando concorrono con esso interessi pubblici a che certi fatti siano resi noti: ad esempio, quando la conoscenza dello scritto sia richiesta ai fini di un giudizio civile o penale o per esigenze di difesa dell'onore o della reputazione personale o familiare (art. 94); o, ancora, quando si tratti di corrispondenze ufficiali o che presentino un interesse di Stato (art. 95).
In sintesi, secondo la legge sul diritto d'autore, i diritti esistenti e concorrenti in presenza di una corrispondenza privata sono il diritto d'autore (ma solo qualora si tratti di opere di carattere creativo) e il diritto dello scrivente, del destinatario e dei terzi a mantenere segreti fatti inerenti alla propria vita privata (diritto esistente anche quando gli scritti in questione non siano opere d'arte, ma a patto che abbiano carattere confidenziale e siano attinenti all'intimità privata; in caso contrario, nessun limite osta alla pubblicazione)[20].
Nella prospettiva del Garante, la qualificazione come corrispondenza delle *chat* è, pertanto, funzionale all'applicazione di tale disciplina, che si qualifica come aggiuntiva e supplementare rispetto a quella in tema di protezione dei dati personali, che – si badi – è invece applicabile a prescindere dalla qualificazione come corrispondenza delle comunicazioni (*infra* § 2.3).
Se, per le ragioni già espresse (*retro* § 2.1), può condividersi la premessa da cui il Garante muove (ossia la qualificazione come corrispondenza della *chat* suddette, qualificazione coerente con la giurisprudenza costituzionale e di legittimità più recente), più dubbi sorgono in merito alle conseguenze che, in termini di limiti all'esercizio del diritto di cronaca, l'autorità vi fa derivare.
Sotto questo profilo, il provvedimento sconta, anzitutto, una motivazione eccessivamente stringata.
In un'altra occasione, infatti, il Garante aveva escluso la necessità del consenso dal momento che le *e-mail* pubblicate contenevano solo valutazioni di carattere politico e non potevano, pertanto, essere considerate attinenti all'intimità della vita privata dei corrispondenti. Analogamente aveva ritenuto non confidenziali messaggi scambiati in gruppi *Whatsapp* e in *mailing list*, tenuto conto del cospicuo numero dei soggetti che vi facevano parte e dell'eterogeneità degli stessi, circostanze che portavano a ritenere del tutto assente ogni ragionevole aspettativa in ordine all'effettiva riservatezza delle conversazioni tenute[21].

---

[20] Per una più ampia ricostruzione in merito ai profili di diritto d'autore che qui vengono in rilievo, cfr. A. DeCupis*, I diritti della personalità*, in *Trattato di diritto civile e commerciale*, diretto da A. Cicu-F. Messineo-L. Mengoni, Milano, 1982, 358 ss. Per la disciplina in tema di pubblicazione di missive tra privati, v. G. DiMajo, *voce Corrispondenza (dir. priv.)*, in *Enc. dir.*, vol. X, 742; M. Dogliotti, *Le persone fisiche*, in *Tratt. Dir. priv.* diretto da G. U. Rescigno, vol. 2, t. I, Torino, 1992, 152 ss.

[21] Ci si riferisce al già citato provvedimento del Garante per la protezione dei dati personali del 2 febbraio 2017 (iscritto al Registro dei provvedimenti n. 36 del 2017) che, per le menzionate ragioni, aveva ritenuto legittima la pubblicazione di alcune *e-mail* di attivisti del Movimento 5 Stelle romano sul quotidiano "La Stampa". Su questo provvedimento si tornerà ancora *infra* § 2.3 in merito alla valutazione, operata sempre dal Garante, circa la sussistenza in quel caso del requisito dell'essenzialità dell'informazione pubblicata con riguardo a fatti di interesse pubblico di cui all'art. 137, c. 3, del "Codice in materia di protezione dei dati personali" e all'art. 6 delle "Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica".

Nel caso qui considerato, invece, manca un qualsivoglia riferimento in tal senso. Il Garante, al contrario, comprime il diritto di cronaca, limitandosi a richiamare la citata normativa in tema di diritto d'autore: non illustra, quindi, né quali limiti specifici alla diffusione della corrispondenza telematica deriverebbero dall'applicazione di tale disciplina, né per quali ragioni la pubblicazione delle *chat* in questione non sia conforme ai dettami della legge sul diritto d'autore, dando, quindi, per scontato che si tratti di comunicazioni confidenziali e intime e, di conseguenza, non pubblicabili.

Al capoverso successivo, infatti, il Garante passa a trattare un profilo distinto, evidenziando come, al caso di specie, si applichi, altresì, la normativa in tema di protezione dei dati personali.

Per quello che qui più interessa, tale disciplina pone come limite fondamentale all'esercizio del diritto di cronaca il requisito dell'essenzialità dell'informazione relativa a fatti di pubblico interesse, soddisfatto il quale la pubblicazione è consentita a prescindere dal consenso dell'interessato. Trattasi, quindi, di un complesso di regole che muove da presupposti differenti rispetto a quelli della legge sul diritto d'autore (più diffusamente *infra* § 2.3).

Il richiamo alle norme poste a tutela dei dati personali è coerente, avendo la pubblicazione ad oggetto in effetti dati identificativi dei corrispondenti. Tuttavia, il Garante omette di precisare quale rapporto vi sia tra le due forme di tutela (diritto d'autore e tutela della protezione dei dati personali). Il lettore è, così, indotto a ritenere che le garanzie di cui alla legge sul diritto d'autore risultino aggiuntive e supplementari rispetto a quelle in tema di *privacy* e che sia decisiva, a tal fine, la sussunzione delle *chat* sotto la nozione di corrispondenza, la quale è, come poc'anzi detto, condizione necessaria per l'applicazione della legge sul diritto d'autore.

In verità, come si illustrerà a breve (*infra* § 2.3), la disciplina a tutela dei dati personali – che si applica, al contrario, a prescindere dalla qualificazione di un dato contenuto come corrispondenza – appresta una tutela più completa e assorbente rispetto a quella della legge sul diritto d'autore. Ne consegue che la qualificazione delle *chat* come forme di corrispondenza telematica, pur condivisibile sotto il profilo teorico e in linea con la recente giurisprudenza costituzionale e di legittimità, non risulta decisiva quando si tratta di bilanciare, in concreto, il diritto di cronaca con la tutela della riservatezza.

2.3. Il diritto di cronaca e la tutela dei dati personali: un binomio difficile, ma non impossibile

Qualora oggetto di pubblicazione siano i dati personali dell'interessato, a venire in rilievo sono due posizioni giuridiche non facili da conciliare: la riservatezza, da una parte, e il diritto di cronaca, dall'altra[22].

[22] Sul rapporto tra libertà di informazione e tutela della riservatezza la letteratura è particolarmente ampia. Cfr., *ex plurimis*, G. Giacobbe, *Riservatezza (diritto alla)*, in *Enciclopedia del Diritto*, XL, Milano, 1989, 1243 ss.; J. Monducci-G. Sartor, *Il codice in materia di protezione dei dati personali, Commentario sistematico al d.lgs. 30 giugno 2003, n. 196*, Padova, 2004; A.

La tutela della riservatezza assicura il riserbo sulla vita privata di ciascuno e, dunque, si concretizza nell'evitare che questa sfera sia violata da indebite interferenze senza il consenso dell'interessato; al contrario, il diritto di cronaca (e quello di critica) sono posti a garanzia dell'attività giornalistica di narrare e commentare i fatti, cosa che, frequentemente, implica l'utilizzo di informazioni che riguardano la sfera personale altrui.

Diritto alla riservatezza e libertà di informazione costituiscono, pertanto, due libertà "antagoniste", in quanto diritti contenutisticamente di segno inverso[23]. Entrambi trovano, tuttavia, fondamento nel testo costituzionale: il diritto di informare, che presuppone l'utilizzo dei dati personali, non sarebbe veramente tale se fosse subordinato sempre e comunque al consenso dei protagonisti dei fatti narrati; ma, d'altro canto, la tutela della riservatezza non sarebbe effettiva se dovesse sempre cedere il passo a fronte dell'esercizio dell'attività giornalistica[24]. A ben vedere non c'è, in realtà,

Pace-R. Zaccaria-G. De Minico (a cura di), *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Napoli, 2008; P. Caretti-A. Cardone, *Diritto alla riservatezza e diritto all'informazione: premesse normative e sviluppi giurisprudenziali*, in *Diritti umani e diritto internazionale*, 1, 2010, 87 ss.; S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012; C. Melzi d'Eril-G. E. Vigevani, *sub. artt. 136-138*, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, 1520 ss.

[23] Così, ad esempio, si esprime Cass civ., sez. III, 9 giugno 1998, n. 5658 in *Foro It.*, 1998, I, 2387.

[24] Nell'interpretare la libertà di informazione, la Corte costituzionale si è col tempo allontanata da una lettura prevalentemente "individualista" dell'art. 21 Cost., che era prevalsa nella fase iniziale della sua giurisprudenza, per avvicinarsi ad un'interpretazione di tipo "funzionalista", ispirata alla visione del collegamento esistente tra la "libertà di informazione" e le forme proprie di una "democrazia pluralista". Sin dalla sent. 17 aprile 1969, n. 84 la libertà di informazione è stata, così, definita dalla Corte "pietra angolare" dell'ordinamento democratico, con la conseguenza che il "diritto dell'informazione" si è venuto sempre più a intrecciare con i principi ispiratori della nostra forma di Stato che, in quanto democratica, deve a sua volta trovare la sua base nell'esistenza di un'opinione pubblica "consapevole", cioè informata (Corte cost., sent. 26 marzo 1993, n. 112). Di qui, quindi, l'elaborazione da parte della Corte costituzionale di un diritto dei cittadini a ricevere un'informazione obiettiva, trasparente e corretta, diritto inteso quale volto passivo dell'art. 21 Cost., al quale è proprio preordinato l'esercizio del diritto di cronaca (da ultimo, Corte cost., sent. 12 luglio 2021, n. 150). Cfr., sul punto, tra gli studi di maggior rilievo, A. Loiodoce, *Contributo allo studio sulla libertà di informazione*, Napoli, 1969, 5 ss.; P. Barile, *Libertà di manifestazione del pensiero*, Milano, 1975, 34 ss.; L. Paladin, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, in L. Paladin (a cura di), *La libertà d'informazione*, Torino, 1979, 3 ss.; C. Chiola, *L'informazione nella Costituzione*, Padova, 1973, 7 ss.; R. Zaccaria-L. Capecchi, *La libertà di manifestazione del pensiero*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, XII, Padova, 1990, 300 ss.; v. P. Costanzo, *(voce) Informazione nel diritto costituzionale*, in *Dig. Pubb.*, VIII, Torino, 1992, 5 ss.
Al contrario, il diritto alla riservatezza è stato interpretato dalla giurisprudenza costituzionale come «manifestazione del diritto fondamentale all'intangibilità della sfera privata che attiene alla tutela degli individui nei suoi molteplici aspetti, che trova riferimenti nella Costituzione italiana (artt. 2, 14 e 15 Cost.)» (così, in particolare, Corte cost., sent. 21 febbraio 2019, n. 20). Sulla progressiva enucleazione del diritto alla riservatezza a partire da una lettura sistematica del testo costituzionale, v. A. De Cupis, *I diritti della personalità*, Milano, 1973, 256-257; A. Pizzorusso, *Sul diritto alla riservatezza nella Costituzione italiana*, in *Prassi e Teoria*, 1, 1976, 1 ss.; G. Giampiccolo, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.*, 1, 1958, 1 ss. Più di recente, si vedano le considerazioni di P. Passaglia, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consulta OnLine*, 3, 2016, 332 ss.

una vera sovrapposizione tra i due diritti, in quanto uno specifico dato personale non può essere contemporaneamente oggetto di entrambe le garanzie: in altri termini, riservatezza e libertà di informare sono diritti che occupano spazi diversi, spartendosi il campo dei dati personali senza che residui uno spazio "neutrale"[25].

Quel che, piuttosto, è difficile identificare è la linea di confine che corre tra questi due diritti. Su questo profilo si concentra il Garante, quando richiama il testo normativo di riferimento in materia, ossia il d.lgs. n. 196 del 2003 (c.d. "Codice in materia di protezione di dati personali"), così come riscritto dal d.lgs. n. 101 del 2018, il quale, a sua volta, ha dato attuazione alla normativa euro-unitaria (il regolamento UE 2016/679, "Regolamento generale sulla protezione dei dati personali", abbreviato in GDPR).

I limiti posti dalla disciplina in tema di protezione di dati personali valgono, difatti, a certe condizioni anche nei confronti dell'attività giornalistica. Rimangono, anzitutto, fermi i principi generali di cui all'art. 5 del GDPR e, in particolar modo, quelli di liceità, correttezza e trasparenza del trattamento. Ne consegue che il giornalista non può cercare di manipolare o pubblicare dati raccolti in modo non corretto e non trasparente, dovendo fornire alla persona interessata una precisa informazione di come e in quale sede verranno trattati i suoi dati. Inoltre, il trattamento deve trovare fondamento su una delle condizioni di cui all'art. 6 del GDPR, e, in particolare, sul consenso dell'interessato.

Tale disciplina generale va, tuttavia, bilanciata con la peculiarità dell'attività giornalistica. Non è un caso che l'art. 85 del GDPR stabilisca che gli Stati membri possono prevedere deroghe ed esenzioni che siano necessarie per conciliare la disciplina in tema di dati personali proprio con la libertà di espressione.

Le disposizioni che, in attuazione di quest'ultimo articolo, stabiliscono eccezioni alla normativa generale in tema di protezione dati personali sono contenute al Titolo XII della Parte II del "Codice in materia di protezione dai dati personali", rubricato "Giornalismo, libertà di informazione e di espressione".

Anzitutto, l'art. 136, "Finalità giornalistiche e altre manifestazioni del pensiero", circoscrive l'ambito di operatività della disciplina derogatoria, stabilendo che essa si applica al trattamento dei dati personali: a) effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità; b) svolto dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti; c) finalizzato alla pubblicazione o diffusione, anche occasionale, di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione accademica artistica e letteraria. Tali regole speciali sono, dunque, dirette a tutelare la libertà di informare o, comunque, l'esercizio della libera manifestazione del pensiero.

La disposizione più rilevante – richiamata, infatti, anche dal Garante a fondamento del suo provvedimento – è, tuttavia, l'art. 137 del "Codice in materia di protezione di dati personali"[26].

---

[25] Cfr. C. Melzi d'Eril, *Privacy e attività giornalistica*, in G. E. Vigevani-O. Pollicino-C. Melzi d'Eril-M. Cuniberti-M. Bassini (a cura di), *Diritto dell'informazione e dei media*, Torino, 2022, 131.

[26] Su cui, più diffusamente, C. Melzi d'Eril-G.E. Vigevani, *sub. artt. 136-138*, cit., 1520 ss.

I primi due commi di tale articolo escludono l'applicazione della disciplina generale nello specifico caso dell'attività giornalistica, consentendo il trattamento dei dati sensibili di cui agli articoli 9 e 10 del GDPR e dei dati relativi a condanne penali e reati anche senza il consenso dell'interessato. È questo il profilo di differenza maggiore rispetto alla disciplina generale: purché siano rispettate le regole deontologiche, il giornalista nell'esercizio della sua attività non è tenuto a richiedere un espresso consenso da parte dell'interessato al trattamento dei suoi dati[27].

È il terzo comma dell'art. 137 del Codice a porre, poi, la norma cardine dell'intera disciplina, stabilendo che restano, tuttavia, fermi i limiti del diritto di cronaca posti a tutela della protezione dei dati personali e, in particolare, quello dell'essenzialità dell'informazione concernente fatti di interesse pubblico.

Tale limite si spiega in ragione del fatto che la diffusione di dati personali in ambito giornalistico deroga alle regole generali volte a tutelare i diritti del singolo, tanto da non richiedere, come poc'anzi detto, il consenso dell'interessato in nome di un interesse generale della società alla diffusione delle notizie. È logicamente conseguenziale, però, che quelle stesse notizie siano realmente di interesse pubblico, altrimenti tale disciplina speciale perderebbe di giustificazione.

La nozione di interesse pubblico va, a sua volta, calata nel contesto della società di ogni dato momento storico, identificandosi negli argomenti e nei temi che, effettivamente, possono incidere sulla formazione delle opinioni collettive[28].

Ma non basta. L'art. 137 cit. richiede qualcosa in più rispetto ad un generico interesse pubblico e, in particolare, l'essenzialità dell'informazione riportata. I fatti narrati devono essere, pertanto, di interesse pubblico – ossia rilevanti per il contesto sociale di riferimento – e in relazione a tali fatti possono essere diffusi solo i dati personali indispensabili per rendere conoscibile la notizia. In altre parole, il giornalista deve individuare la notizia, verificarne il pubblico interesse e, infine, individuare i dati personali, raccolti secondo correttezza e veritieri, la cui diffusione sia indispensabile per rendere la notizia comprensibile al pubblico[29].

Il requisito dell'essenzialità è ribadito, altresì, dall'art. 6 delle "Regole de-

---

[27] Ad avviso della dottrina, l'esenzione per la quale il giornalista non è tenuto a chiedere il consenso al trattamento dei dati personali si riferisce non solo ai dati espressamente menzionati dall'art. 137 cit., ma, logicamente, a tutti i dati personali, senza quindi distinzioni di sorta, cfr. C. Melzi d'Eril, *Privacy e attività giornalistica*, cit., 143 ss.

[28] Sulla nozione di interesse pubblico si è espressa anche la giurisprudenza di legittimità, v., tra le altre, Cass. civ., sez. III, 21 giugno 2018, n. 16311 (rv. 649435-01), secondo cui «in tema di *privacy* i limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, che circoscrivono la pubblicazione di diffusione dei dati personali nell'esercizio dell'attività giornalistica, comporta il dovere di evitare riferimenti a congiunti del personaggio pubblico, non potendo la notorietà di quest'ultimo di affievolire i diritti dei primi». Sui limiti all'esercizio del diritto di cronaca, cfr. A. Bevere-P. Bevere-A. Cerri, *Il diritto di informazione e i diritti della persona*, Milano, 2022; E. Morresi, *L'onore della cronaca. Diritto all'informazione e rispetto delle persone*, Bellinzona, 2008, 264 ss.; G. Catalisano, *Il ruolo del diritto di cronaca e di critica nell'attività giornalistica: profili di diritto dell'informazione*, Milano, 2013.

[29] Cfr. C. Melzi d'Eril, *Privacy e attività giornalistica*, cit., 142.

ontologiche" citate, che stabilisce che un'informazione, anche dettagliata, sugli interessati è pubblicabile solo qualora sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

Orbene, applicando tali regole al caso in esame, il Garante ritiene che la narrazione dei contenuti pubblicati nel volume – mediante virgolettati di *chat* private – non costituisce un elemento necessario in rapporto alla finalità informativa perseguita. L'autore avrebbe, infatti, potuto ricorrere a soluzioni maggiormente conformi alla disciplina in materia di protezione dei dati personali, considerando anche le implicazioni che la pubblicazione, per esteso, della corrispondenza avrebbe avuto nei riguardi dei terzi. Si può ipotizzare che il Garante faccia qui riferimento al fatto che si sarebbe potuta pubblicare una sintesi, rielaborata dal giornalista, del contenuto delle *chat*, senza riportare il loro contenuto integrale per virgolettati. Si sarebbero, in tal modo, aperti squarci meno impattanti sulla riservatezza delle persone coinvolte. Se ne può logicamente derivare che non è stata ritenuta sufficiente la rassicurazione, riportata dall'autore a pagina 15 del volume, per cui dalla pubblicazione sarebbero stati «esclusi tutti gli elementi privati riconducibili ai partecipanti e il turpiloquio, che comprensibilmente viene utilizzato in una *chat* tra colleghi di lavoro e amici».

Non è questa chiaramente la sede per formulare un giudizio circa la sussistenza o meno di tale requisito nel caso specifico, stante l'assenza di elementi sufficienti a sostegno dell'una o dell'altra tesi.

Piuttosto, nel tentativo di astrarre il ragionamento, si può affermare che, in verità, il requisito dell'essenzialità riguardo a fatti di interesse pubblico appresta una tutela a tal punto ampia a protezione della riservatezza, da risultare assorbente rispetto a quella del diritto d'autore (*retro* § 2.2).

Fatte salve ovviamente eccezioni sempre possibili, contenuti attinenti alla vita privata o all'intimità degli interessati, per la cui pubblicazione la legge sul diritto d'autore richiede il consenso dell'interessato, non potrebbero riferirsi a fatti di interesse pubblico e, ancor meno, la loro pubblicazione sarebbe essenziale al fine di rendere conoscibile la notizia ai lettori.

Se si accoglie questa prospettiva, se ne deve, allora, dedurre che la qualificazione come corrispondenza – preliminare per l'applicazione dell'art. 93 della legge sul diritto d'autore, che tutela le sole missive (cartacee e, alla luce dell'evoluzione giurisprudenziale più recente, anche telematiche) – non è, in verità, decisiva. La disciplina in tema di protezione dei dati personali, infatti, si applica indipendentemente dal fatto che l'informazione sia contenuta all'interno di una corrispondenza privata (mirando a proteggere, piuttosto, i dati identificativi della persona). Essa, ponendo come condizione l'essenzialità dell'informazione rispetto a fatti di interesse pubblico, è, quindi, di per sé sufficiente a proteggere la riservatezza delle persone coinvolte e ad assorbire le garanzie poste dalla normativa in materia di diritto d'autore.

Piuttosto, l'aspetto più critico – che dal Garante non viene approfondito nel provvedimento qui in commento, ma che, in realtà, è centrale – riguarda il confine (labile) tra notizia di interesse pubblico e non nell'ipotesi in cui mittente e/o destinatario siano personaggi noti al pubblico (come nel caso in esame, ove tra le persone coinvolte figurano parlamentari, ministri,

dirigenti del partito attualmente di maggioranza relativa, la stessa Presidente del Consiglio).

Tracciare tale linea di demarcazione non è chiaramente possibile "in astratto" e "a priori", ma qualche precisazione sarebbe stata, in questo senso, utile, di modo da meglio definire sin dove può spingersi il diritto di cronaca e quando, invece, questo deve retrocedere per tutelare la *privacy* degli interessati, anche qualora questi siano personaggi conosciuti all'opinione pubblica.

In questo senso i già citati precedenti del Garante avevano, al contrario, fornito qualche valida indicazione in più. Ad esempio, nel provvedimento del 2013[30], era stata vietata ogni forma di pubblicazione e di trattamento dei dati contenuti in alcune *e-mail* di parlamentari del Movimento 5 Stelle, dal momento che queste erano state diffuse in Rete a seguito di un attacco *hacker* che illegittimamente le aveva rese di pubblico dominio, determinando una palese violazione della riservatezza dei soggetti coinvolti (peraltro, non solo dei parlamentari intestatari degli indirizzi di posta elettronica, ma di tutti coloro che erano entrati in contatto con essi, nonché dei terzi citati all'interno delle comunicazioni). In quel caso, quindi, era stata l'illiceità *ab origine* del trattamento dei dati personali ad estendere i suoi effetti anche ai successivi trattamenti, rendendo illecita ogni ulteriore operazione di raccolta, di conservazione e di utilizzo dei dati medesimi[31].

Al contrario, in un provvedimento del 2017[32], la pubblicazione di una serie di messaggi di posta elettronica di alcuni attivisti del Movimento 5 Stelle sul quotidiano "*La Stampa*" era stata considerata essenziale con riferimento a fatti di interesse pubblico, in quanto le *e-mail* erano afferenti alle dinamiche interne di un attore politico rilevante nel panorama nazionale, tenuto, altresì, conto dell'intervallo temporale in cui la pubblicazione era avvenuta e i fatti ivi narrati avevano avuto luogo (ossia nei mesi antecedenti alle elezioni amministrative del 2016)[33].

---

[30] Provvedimento del Garante per la protezione dei dati personali del 6 maggio 2013, iscritto al Registro dei provvedimenti n. 229 del 2013 (già richiamato *supra* § 2.1).

[31] Ad avviso del Garante, l'illecita diffusione *online* di corrispondenza telematica privata per mano degli *hackers* – oltre a poter integrare l'ipotesi di reato di cui all'art. 616 cod. pen., rubricato "Violazione, sottrazione e soppressione di corrispondenza", secondo il quale è punibile «chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta […]», la cui valutazione era, tuttavia, di competenza dell'autorità giudiziaria – precludeva agli organi di stampa di potere far uso e, soprattutto, di ripubblicare le *e-mail* in questione, stante il principio generale in base al quale, come detto in precedenza, i dati personali devono essere trattati in modo lecito, secondo correttezza e utilizzati per scopi legittimi.

[32] Provvedimento del Garante per la protezione dei dati personali del 2 febbraio 2017, iscritto al Registro dei provvedimenti n. 36 del 2 febbraio 2017 (sul quale si è già ragionato *supra* §§ 2.1 e 2.2).

[33] Il Garante osservava, infatti, che dalle *e-mail* si poteva ricavare uno "spaccato" interessante delle dinamiche interne al Gruppo di Lavoro del Movimento 5 Stelle romano, considerato, peraltro, che tra i soggetti coinvolti figurava il coordinatore del Tavolo dell'Urbanistica del Movimento 5 Stelle a Roma e un militante di lunga data, candidato alle elezioni amministrative in programma, come detto, quell'anno nella Capitale.

3. Considerazioni finali

In una società sempre più interconnessa la possibilità di avere accesso alle comunicazioni telematiche di natura privata è un elemento che sta acquisendo una rilevanza centrale, data la capacità di queste forme di corrispondenza di disvelare gli aspetti anche più intimi della vita delle persone.
Non è un caso, infatti, che la Corte costituzionale, con la sentenza n. 170 del 2023, abbia scelto di smentire un pur consolidato orientamento della giurisprudenza di legittimità proprio al fine di allargare le maglie delle garanzie costituzionali poste a presidio della corrispondenza, non solo qualora a venire in rilievo siano comunicazioni di membri del Parlamento, ma anche quelle di privati cittadini.
Tali questioni dimostrano, oggi, tutta la loro importanza anche con riferimento all'attività giornalistica.
Trattasi, qui, di adattare al nuovo contesto digitale un equilibrio antico e fragile tra diritto di cronaca e tutela della riservatezza. Il discrimine, infatti, tra essenzialità dell'informazione con riferimento a fatti di interesse pubblico e dati che riguardano aspetti della vita privata corre su una linea di confine piuttosto labile.
Dove collocare questa linea è scelta non facile per un ordinamento democratico.
Al fondo, vi è l'esigenza di individuare un punto di incontro tra il diritto del giornalista di informare (e il correlato diritto dell'opinione pubblica ad essere informata), da un lato, e la tutela della riservatezza, dall'altro, in una società, quella contemporanea, ove le possibilità di aprire veri e propri squarci sull'intimità delle persone sono enormemente superiori rispetto al passato a causa dello sfruttamento dei dati personali di ognuno di noi, il nuovo "petrolio" del XXI secolo, sul quale tutta l'info-sfera digitale è stata costruita e plasmata[34].

Keywords

diritto di cronaca - tutela della riservatezza - essenzialità dell'informazione - messaggistica telematica - dati personali.

[34] Per riprendere la felice espressione di L. Floridi, *La quarta rivoluzione. Come l'info-sfera sta cambiando il mondo*, Milano, 2017, 5 ss.

Un ulteriore tassello nella ricostruzione interpretativa del GDPR: la Corte di giustizia amplia oltremisura il potere discrezionale delle autorità di controllo?*

Giovanna De Carne

Corte di giustizia, 26 settembre 2024, C-768/21, *TR c. Land Hessen*

La violazione dei dati personali delle persone fisiche non esige automaticamente l'intervento correttivo delle autorità di controllo di cui all'art. 58, par. 2, del GDPR, se la correttezza del trattamento è stata efficacemente ripristinata grazie, ad esempio, alle idonee misure adottate dal titolare del trattamento. Muovendo da queste considerazioni, la Corte di giustizia dell'Unione europea, nella sentenza del 26 settembre 2024 resa nella causa C-768/21, ha affermato la natura facoltativa dei poteri correttivi, il cui esercizio è subordinato ad una preventiva valutazione delle autorità di controllo. A tal fine, la Corte individua tre parametri utili a orientare la decisione: considerate le circostanze del caso concreto, l'intervento correttivo deve rivelarsi appropriato, necessario o proporzionato a garantire un'adeguata tutela dei dati personali.

Sommario

1. Premessa. - 2. La ricostruzione dei fatti all'origine del rinvio pregiudiziale. - 3. La configurabilità delle misure correttive come poteri facoltativi. - 4. Ulteriori osservazioni sulla natura facoltativa di un particolare potere correttivo: le sanzioni amministrative pecuniarie. - 5. Considerazioni conclusive.

1. Premessa

La protezione dei dati personali, oggi tutelata a livello internazionale, europeo e interno, può essere garantita solo in presenza di adeguati sistemi di controllo e di un apparato sanzionatorio che abbia anche un effetto

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

deterrente su possibili future violazioni.
Proprio nell'ottica di assicurare un idoneo standard di tutela al corpo elettronico delle persone fisiche[1], gli strumenti internazionali ed europei esistenti in materia hanno conferito alle c.d. autorità di controllo[2] poteri ampi ed eterogeni, tra i quali il potere di ripristinare la correttezza del trattamento dei dati personali a seguito di una loro violazione.
Si tratta di un'esigenza essenziale per assicurare l'effettività del diritto alla protezione dei dati personali come risulta sia dall'aggiornata Convenzione 108+[3] del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, sia dal Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, in prosieguo "GDPR" o "Regolamento").
Con riguardo alla Convenzione, l'aggiornamento, tra gli altri elementi, ha avuto al centro, proprio ai fini di garantire maggiore effettività agli obblighi convenzionali, l'individuazione delle autorità di controllo competenti nell'adozione delle sanzioni[4]: l'art. 15, par. 2, lett. c), infatti, richiede agli Stati di individuare dette autorità che hanno il potere di emettere decisioni e di ricorrere a sanzioni amministrative [5]. Questa norma è senza dubbio ispirata dall'art. 58, par. 2, del Regolamento il quale attribuisce all'autorità di controllo il potere di adottare numerose misure correttive elencate nelle

[1] S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, conia per la prima volta l'espressione corpo elettronico per indicare che l'identificazione e la conoscenza di una persona umana al giorno d'oggi passa anche, e talvolta esclusivamente, attraverso i suoi dati; di qui l'esigenza di garantire un adeguato standard di tutela ai dati che incarnano la persona umana.
In questo senso, si segnala altresì l'intervento al convegno "Uomini e Macchine" di G. Bianchi Clerici dal titolo *Corpo elettronico e tecnologie informatiche*, in *garanteprivacy.it*, 30 gennaio 2018.

[2] Sul ruolo centrale delle autorità di controllo si veda E. Guardigli, *Le Autorità di controllo*, in G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 489 ss.; L. Califano, *La protezione dei dati personali e il ruolo del Garante in ambito pubblico*, in questa *Rivista*, 1, 2018, 134 ss.; F. Pizzetti, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, ivi, 104 ss.; R. D'Orazio, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. Cuffaro – R. D'Orazio – V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 81 ss.

[3] La Convenzione 108+, anche nota come Protocollo di modifica, del 18 maggio 2018 ha aggiornato la precedente Convenzione 108 adottata a Strasburgo il 28 gennaio 1981. Essa è stata ratificata in Italia con legge n. 60 del 22 aprile 2021.

[4] Nella Convenzione n. 108, con riguardo alle sanzioni, l'art. 10 si limitava a stabilire che ciascuna parte contraente si impegnava a stabilire sanzioni e ricorsi appropriati per le violazioni delle regole di diritto interno che davano attuazione alle norme convenzionali.

[5] La Convenzione 108+ del Consiglio d'Europa conferisce alle autorità di controllo poteri di indagine e di intervento, il potere di emettere decisioni in merito alle violazioni delle disposizioni della Convenzione e di imporre sanzioni amministrative, il potere di avviare procedimenti giudiziari o di portare all'attenzione delle autorità giudiziarie competenti le violazioni delle disposizioni della Convenzione.

lett. a)-j)[6], ricomprendenti anch'esse le sanzioni amministrative pecuniarie[7]
Dunque, entrambi gli strumenti investono le autorità di controllo del compito di porre rimedio ad un illecito trattamento dei dati attraverso le sanzioni amministrative e presentano una certa affinità in ragione del fatto che la portata innovativa del Regolamento ha condotto a una simultanea revisione della precedente Convenzione 108 del 1981.
Alla somiglianza circa il potere sanzionatorio non corrisponde, tuttavia, una eguale chiarezza in ordine alla natura dello stesso: infatti, dal raffronto tra le due disposizioni emerge *ictu oculi* una rilevante differenza tra la formulazione dell'art. 15 del Trattato internazionale e quella dell'art. 58 del Regolamento.
La Convenzione 108+ adotta un approccio più cauto in relazione alle sanzioni amministrative, stabilendo all'art. 15, par. 2, lett. c) che le autorità di controllo «*shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions*».
Nel testo spicca l'impiego del verbo "*may*", atto ad esprimere inequivocabilmente la mera potenzialità di infliggere dette sanzioni.
Diversamente, l'art. 58, par. 2, del GDPR presenta, sul punto, qualche ambiguità perché, pur indicando un elenco di misure[8], con ciò facendo presumere una libertà di scelta nell'individuazione delle stesse da parte dell'autorità di controllo[9], non precisa se le indicate autorità abbiano un

[6] Il regolamento (UE) 2016/679, temporalmente antecedente alla Convenzione 108+, attribuisce alle autorità poteri di indagine, correttivi, consultivi e autorizzativi, ciascuno dei quali è sviluppato nel dettaglio dal legislatore europeo attraverso una fitta elencazione. Inoltre, ogni autorità ha il potere di intentare un'azione o di agire in sede giudiziale o stragiudiziale in caso di violazione del Regolamento, previa disposizione dello Stato membro, il quale può altresì riconoscere alla propria autorità ulteriori poteri oltre quelli espressamente disciplinati.

[7] Circa il potere sanzionatorio delle autorità di controllo si veda A. G. Parisi, *Responsabilità e sanzioni*, in S. Sica - V. D'Antonio - G. M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 306 ss.; M. Ratti, *Il regime sanzionatorio previsto dal regolamento per l'illecito trattamento dei dati personali*, in G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 595 ss.; S. Antoniazzi, *Le sanzioni amministrative*, in V. Cuffaro – R. D'Orazio – V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1093 ss.; E. Grosso, *L'incerto statuto delle sanzioni tra Corti europee e giurisprudenze nazionali. Un'introduzione*, in *Diritto pubblico comparato ed europeo*, 4, 2019, 1010 ss.; M. Orofino, *Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR*, in *Diritto pubblico comparato ed europeo*, 4, 2019, 1144 ss.; L. Califano, *Il ruolo di vigilanza del Garante per la protezione dei dati personali*, in *federalismi.it*, 2 dicembre 2020, 17 ss..; M. Bassini, *Commento all'art. 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie*, in R. D'Orazio - G. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, 896 ss.; O. Pollicino – M. Bassini – G. De Gregorio, *The General Data Protection Regulation*, in *Internet law and protection of fundamental rights*, Milano, 2022, 213-215.

[8] Giova sottolineare che il par. 1 e il par. 3 dell'art. 58 del GDPR, dedicati rispettivamente ai poteri di indagine e ai poteri autorizzativi e consultivi, presentano analoga struttura.

[9] CGUE, C-311/18, *Facebook Ireland e Schrems* (2020). In questa sentenza la Corte afferma la discrezionalità delle autorità di controllo nell'individuazione dei poteri correttivi. In particolare, al § 112 si legge: «Benché la scelta del mezzo appropriato e necessario spetti all'autorità di controllo e questa debba fare tale scelta prendendo in considerazione tutte le circostanze del trasferimento di dati personali di cui trattasi, detta autorità è comunque tenuta ad assolvere al suo compito di vigilare sul pieno rispetto del RGPD con tutta la diligenza richiesta».

obbligo di intervento in ogni caso di violazione o se abbiano un margine di discrezionalità, facilitando così l'insorgere di dubbi interpretativi.
Taluni chiarimenti sul potere e sugli obblighi delle autorità di controllo sono arrivati dalla sentenza del 26 settembre 2024 della Corte di Giustizia dell'UE (Prima Sezione), la quale - adita in via pregiudiziale dal Tribunale amministrativo di (Wiesbaden) - è stata chiamata a pronunciarsi, per la prima volta, sulla possibilità di considerare o meno come obbligatorio il ricorso da parte delle autorità di controllo, nei casi in cui sia accertato un trattamento illecito dei dati, ai poteri correttivi di cui all'art. 58 e, specialmente, alle sanzioni amministrative pecuniarie.
Premesso che l'interpretazione di una disposizione non può limitarsi al solo dato letterale, ma deve avere riguardo altresì al contesto complessivo dell'atto di cui fa parte nonché dell'obiettivo perseguito e delle finalità[10], nella sentenza in commento sono ricostruiti alcuni passaggi con cui si giunge ad escludere un "automatismo" dei poteri correttivi a seguito di violazioni accertate dei diritti e delle libertà delle persone fisiche.
Nello specifico, come vedremo, i giudici di Lussemburgo escludono l'obbligo di adottare una misura correttiva qualora «un siffatto intervento non sia appropriato, necessario o proporzionato al fine di porre rimedio all'inadeguatezza constatata e garantire il pieno rispetto di tale regolamento»[11].
Il dispositivo della sentenza potrebbe, dal canto suo, suscitare qualche perplessità circa il riconoscimento di un eccessivo potere discrezionale in capo alle autorità di controllo.
Pertanto, ripercorrendo i ragionamenti sottesi alla decisione della Corte, si tenterà di verificare se tale discrezionalità sia solo "apparentemente eccessiva" o, al contrario, "effettiva", con il potenziale rischio, in quest'ultimo caso, di pregiudicare il perseguimento dell'obiettivo, sancito dal Regolamento, di un livello di protezione uniforme in tutti gli Stati membri dei diritti e delle libertà delle persone fisiche e finanche di intaccare il ruolo centrale delle autorità di controllo, riconosciuto altresì dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea che, affermato il diritto di ogni persona alla protezione dei dati personali che la riguardano, attribuisce alle autorità indipendenti il compito di controllare sul rispetto delle regole in materia[12].

---

[10] § 30 della sentenza.

[11] Si veda il dispositivo della sentenza.

[12] Mentre la Carta dei diritti fondamentali dell'Unione europea ha conferito alla protezione dei dati personali il rango di diritto fondamentale, riservando a tale diritto un autonomo riconoscimento nell'art. 8 e scorporandolo dal più ampio *genus* del diritto al rispetto della vita privata di cui all'art. 7, sul piano internazionale la protezione dei dati personali è stata assicurata per via giurisprudenziale grazie all'interpretazione estensiva dell'art. 8 della Convenzione europera dei diritti dell'uomo ad opera della Corte di Strasburgo.
In merito, si veda V. Colomba - G. Zanetti, *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in *Teoria e critica della regolazione sociale*, 1, 2017, 31-33; A. Fabbricotti - L. Raponi, *La struttura multilivello della protezione dei dati personali in Europa,* in *Rivista italiana per le scienze giuridiche*, 8, 2017, 397 ss.; A. Pisapia, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in *federalismi.it*, 31 gennaio 2018, 4 ss.; O. Pollicino - M. Bassini, *Social network e tutela dei dati personali*, in L. Scaffardi (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, spec. 65-75; O. Pollicino, *Judicial*

2. La ricostruzione dei fatti all'origine del rinvio pregiudiziale

La controversia da cui ha avuto origine la domanda pregiudiziale ha riguardato la consultazione ripetuta, effettuata in diverse occasioni e non autorizzata dei dati personali di TR da parte di una dipendente della Sparkasse, una Cassa di Risparmio tedesca di carattere pubblico che svolge anche operazioni bancarie e creditizie.
Presa contezza dell'infrazione, la Sparkasse, in conformità a quanto previsto dall'art. 33 del Regolamento, ha prontamente informato l'HBDI (il commissario per la protezione dei dati e la libertà di informazione del Land Hessen), ma non anche il diretto interessato.
Questi, venuto a conoscenza dell'accaduto, ha presentato reclamo all'HBDI, lamentando, tra l'altro, la presunta inosservanza dell'art. 34 del GDPR, che prevede la notifica della violazione all'interessato ogniqualvolta essa possa tradursi in un rischio elevato per i suoi diritti e per le sue libertà.
Tanto considerato, l'HBDI ha provveduto all'ascolto della Cassa di risparmio, la quale ha giustificato l'omissione in virtù della considerazione che il proprio responsabile per la protezione dei dati personali non aveva riscontrato la sussistenza di un siffatto rischio e che, comunque, nei confronti della dipendente erano state adottate delle opportune misure disciplinari.
Pertanto, l'HBDI ha respinto la doglianza di TR e, soprattutto, ha ritenuto di non infliggere una sanzione amministrativa pecuniaria.
In disaccordo con le conclusioni dell'autorità di controllo, il cliente leso ha presentato ricorso al Tribunale amministrativo di Wiesbaden, argomentando a sostegno delle proprie ragioni l'errata valutazione delle circostanze di fatto da parte dell'HBDI, che avrebbe dovuto infliggere la sanzione di cui all'art. 83 del GDPR per le plurime violazioni dello stesso Regolamento, e chiedendo che il giudice nazionale ingiungesse all'autorità di intervenire nei confronti della Sparkasse.
Più specificamente, la parte ricorrente ha affermato che la violazione delle disposizioni del GDPR giustificherebbe di per sé l'adozione delle misure correttive di cui all'art. 58, essendo libera l'autorità di controllo solo di decidere non già se, ma come intervenire.
Pur essendo di diverso avviso, il Tribunale amministrativo di Wiesbaden, con decisione del 10 dicembre 2021, ha ritenuto di sottoporre la questione alla Corte di giustizia al fine di chiarire se l'interpretazione dell'art. 57, par. 1, lett. a) ed f) e dell'art. 58, par. 2, lett. a)- j), letti in combinato disposto con l'art. 77, par. 1, del GDPR, induca a ritenere sussistente un incondizionato obbligo di intervento da parte dell'autorità di controllo in presenza di una violazione constatata.

Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?, Oxford, 2021, spec. 110-115; O. Pollicino, *Costituzionalismo, privacy e neurodiritti*, in questa *Rivista,* 2, 2021, 12 ss.. Inoltre, per un maggiore approndimento circa l'art. 8 della CEDU e gli artt. 7 e 8 della CDFUE si vedano rispettivamente i commenti di M. Castellaneta; G. Martinico; O. Pollicino - M. Bassini, in R. D'Orazio - G. Finocchiaro - O. Pollicino - G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, 3-64.

3. La configurabilità delle misure correttive come poteri facoltativi

La questione sollevata non è certamente di pronta soluzione, come potrebbe sembrare da una lettura *prima facie* dell'art. 58 del Regolamento. Tuttavia, a nostro avviso, la Corte è riuscita a fornire un preciso percorso interpretativo della norma che, al par. 2, illustra un ampio ventaglio di poteri correttivi graduati in ordine alla gravità e all'intensità della violazione. In particolare, si comincia con il primo potere che assolve ad una "funzione preventiva", giacché contempla l'avvertimento rivolto al titolare o al responsabile del trattamento circa la verosimile violazione delle disposizioni del Regolamento, per poi terminare con le due previsioni sulle sanzioni amministrative pecuniare e sulla sospensione dei flussi di dati verso il destinatario di un paese terzo o verso un'organizzazione internazionale[13].
Proprio questa vasta gamma di poteri di cui dispongono le autorità di controllo, finanche nell'ipotesi di presumibile - e quindi non ancora accertata - violazione del GDPR, potrebbe indurre a sostenere che l'unica discrezionalità riconoscibile a tali istituzioni sia quella concernente la scelta delle misure più adeguate al caso di specie.
In realtà, la Corte, dopo aver affermato la discrezionalità di cui sono investite le autorità di controllo quanto alla determinazione delle misure correttive, sottolinea che sussiste comunque la possibilità di escludere il ricorso a dette misure seppure "in via eccezionale" [14]. La Corte, infatti, riconosce l'esigenza che venga assicurata una reazione nei casi di inosservanza del Regolamento proprio per garantire effettività ai diritti indicati nel testo, ma non esclude che eccezionalmente il ripristino della situazione violata non necessiti di un intervento dell'autorità di controllo. Questo principio è espressamente enunciato dalla Corte laddove sottolinea che una misura correttiva può «in via eccezionale e tenuto conto delle circostanze particolari del caso concreto, non imporsi, a condizione che la situazione di violazione del RGPD sia già stata ripristinata e che sia garantita la conformità dei trattamenti di dati personali a tale regolamento da parte del loro titolare, e che una siffatta omissione dell'autorità di controllo non sia tale da pregiudicare il requisito di un'applicazione rigorosa delle norme, come ricordato al punto 38 della presente sentenza»[15].
Le motivazioni addotte per sostenere la facoltà di un ricorso alle misure correttive sono tratte da una lettura in combinato disposto del considerando 129[16] e dell'art. 58 del Regolamento, nonché dalla finalità a cui è

[13] Circa la suddivisione tra misure *ex ante* ed *ex post* violazione si veda M. Orofino, *Ne bis in idem e sistema sanzionatorio nella disciplina della protezione dei dati personali dopo l'adozione del GDPR*, cit., 1146.

[14] §§ 43 e 46 della sentenza.

[15] § 46 della sentenza.

[16] Il considerando 129 richiama l'esigenza di garantire un'applicazione coerente e uniforme del Regolamento in tutta l'Unione e, a tal fine, afferma che le autorità di controllo nazionali devono avere gli stessi poteri di cui lo stesso considerando indica le caratteristiche essenziali: ogni misura, in base alle circostanze del caso di specie, deve essere appropriata, necessaria e proporzionata, deve garantire il diritto della persona nei cui confronti possa essere adottato un provvedimento pregiudizievole a essere ascoltata

preordinato l'intervento dell'autorità, consistente nel porre rimedio alla violazione dei dati personali: perché questo risultato sia raggiunto, la Corte precisa che l'autorità, analizzate le circostanze di ogni singolo caso concreto posto al suo esame, individui misure che siano appropriate, necessarie e proporzionate. La Corte si allinea così alla posizione dell'Avvocato generale Priit Pikamäe che nelle sue conclusioni dell'11 aprile 2024 ha osservato che il Regolamento prevede un obbligo di intervento da parte delle autorità di controllo, le quali, però, restano libere nella scelta della misura più confacente al caso concreto[17]. Ci sembra, d'altra parte, che questa conclusione sia in linea con la necessaria discrezionalità che deve sussistere in capo alle autorità di controllo chiamate a decidere in relazione ai singoli casi, valutando l'esito delle indagini, che potrebbe anche condurre ad escludere l'intervento correttivo laddove la situazione di difformità al Regolamento non lo richieda, perché, ad esempio, «il problema è stato nel frattempo risolto o superato e la violazione ha cessato di esistere»[18].

Quale logico corollario di tale discorso ne deriva che, se il titolare del trattamento pone rimedio tempestivamente ed efficacemente alla violazione dei dati personali ancora prima di un possibile intervento dell'autorità (in merito l'Avvocato generale parla di «misure autonome» adoperabili dai titolari del trattamento[19]), il ricorso ai poteri correttivi da parte di quest'ultima risulta privo di utilità proprio perché verrebbe meno una o più delle caratteristiche sancite dal considerando 129, ovvero il carattere appropriato, necessario e proporzionato di tali misure.

In relazione a questi requisiti, l'Avvocato generale ha individuato un ulteriore argomento a favore della natura facoltativa dei poteri correttivi e ha sostenuto che il riconoscimento di un obbligo di intervento ai sensi dell'art. 58 del Regolamento in ogni caso di violazione comporterebbe un dispendio di risorse che l'autorità può destinare, invece, alla soluzione di casi più complessi[20].

In realtà, la Corte, pur avendo aderito ai ragionamenti dell'Avvocato generale, non ha avallato espressamente tale osservazione, che, a nostro avviso, appare un po' più debole delle altre per escludere l'obbligatorietà delle misure in esame: le autorità di controllo, infatti, sono sempre e comunque tenute a svolgere una meticolosa analisi a fronte di una denunciata difformità al Regolamento indipendentemente dalla gravità della violazione, con la conseguenza che è la stessa attività di indagine[21] in ordine alla

---

e deve evitare costi e disagi eccessivi per gli interessati.

17 Al riguardo si veda il § 40 delle conclusioni dell'Avvocato generale in cui viene utilizzata l'espressione «in termini generali» per indicare che in linea di massima ad una violazione dei dati personali segue l'applicazione delle misure correttive più idonee a ripristinare la correttezza del trattamento.

18 § 48 delle conclusioni dell'Avvocato generale.

19 § 52 e 53 delle conclusioni dell'Avvocato generale.

20 § 52 delle conclusioni dell'Avvocato generale.

21 L'esigenza di una indagine approfondita da parte dell'autorità di controllo è del resto confermata dallo stesso Avvocato generale, il quale, al § 53 delle sue conclusioni sostiene espressamente che dette autorità debbano procedere ad un «esame rigoroso» del caso sottoposto alla loro attenzione prima di considerare sufficienti e adeguate le misure adottate dal titolare del trattamento.

valutazione delle singole circostanze del caso concreto e all'idoneità delle misure autonome dei titolari del trattamento a comportare un dispendio di tempo e risorse piuttosto che il ricorso alle misure correttive, le quali, come il termine stesso suggerisce, rispondono all'esigenza di ripristinare la situazione violata e rappresentano, dunque, il risultato finale (ed eventuale) del giudizio delle autorità.
In definitiva, per la Corte, quanto ai poteri correttivi, la regola generale è quella secondo cui, di fronte a violazioni del GDPR, le autorità sono tenute ad effettuare le opportune indagini e ad adottare una o più delle misure di cui all'art. 58, ad eccezione dei casi in cui la difformità al Regolamento sia stata ripristinata. In questi ipotesi, infatti, l'intervento correttivo dell'autorità sarebbe superfluo e ciò comporta, per la Corte, la necessità di escludere l'obbligo del ricorso a siffatti poteri.

4. Ulteriori osservazioni sulla natura facoltativa di un particolare potere correttivo: le sanzioni amministrative pecuniarie

Ricostruite le ragioni escludenti l'automatica applicazione delle misure correttive, la Corte non ha mancato di pronunciarsi sulle sanzioni amministrative pecuniarie al fine di verificare se anche l'applicazione di tali sanzioni sia rimessa ad una libera scelta delle autorità di controllo, seguendo l'*iter* tracciato in via generale per le misure previste dall'art. 58, par. 2, del Regolamento.
In particolare, la Corte ha espresso tre ragioni a sostegno della trasponibilità alle sanzioni amministrative del ragionamento sostenuto per le misure correttive. La prima, di agevole comprensione, è data dalla circostanza che le sanzioni amministrative pecuniarie rientrano nei poteri correttivi di cui all'art. 58 e, per i motivi esposti in precedenza, anch'esse rappresentano uno dei mezzi assoggettati all'apprezzamento delle autorità di controllo.
Non a caso, nelle loro ricostruzioni interpretative, tanto i giudici di Lussemburgo quanto l'Avvocato generale analizzano previamente i motivi escludenti l'obbligatorietà delle misure correttive, per poi considerare quelli alla stregua delle sanzioni di cui trattasi.
La seconda ragione è invece desumibile da un dato prettamente letterale dell'art. 83, par. 2, del Regolamento, messo in luce principalmente dall'Avvocato generale nelle sue conclusioni al § 67, ma che trova altresì riscontro al § 39 della sentenza.
Si intende fare riferimento a quella parte del succitato articolo in cui si statuisce: «Al momento di decidere se infliggere una sanzione amministrativa pecuniaria...».
L'impiego della congiunzione ipotetica "se" da parte del legislatore europeo chiarisce inequivocabilmente che le sanzioni amministrative pecuniarie sono inflitte sulla base di un libero giudizio dell'autorità di controllo.
È importante precisare che il giudizio è libero nel senso che l'autorità di controllo, all'esito di un attento esame, può (e non deve) infliggere le misure in questione.
Tuttavia, nel condurre una siffatta analisi, essa è vincolata a tenere in debi-

to conto una lunga serie di parametri indicati dalla lettera a) alla lettera k) dell'art. 83, par. 2, che guidano la decisione finale e che, quindi, restringono l'ambito di discrezionalità di tali istituzioni.

La terza ed ultima ragione attiene ad una lettura in combinato disposto del considerando 148[22]e dell'art. 83 del GDPR.

Come per i poteri correttivi, così per le sanzioni amministrative pecuniarie l'Avvocato generale e la Corte guardano al risultato a cui le stesse sono preordinate, ovvero quello di rafforzare l'osservanza del Regolamento, nel rispetto del principio del livello di protezione equivalente in tutti gli Stati membri. Non si perde, però, l'occasione di ricordare che lo stesso considerando 148 sancisce la preferenza dell'ammonimento rispetto alle sanzioni in due fattispecie specifiche, ovvero quando:

- la violazione è minore;
- la sanzione pecuniaria da irrogare è eccessivamente onerosa per una persona fisica.

L'insieme di queste considerazioni ha indotto la Corte a respingere la sussistenza di un diritto soggettivo del reclamante ad ottenere, a seguito della sua richiesta, l'inflizione di una sanzione amministrativa pecuniaria da parte dell'autorità di controllo, precisando, ancora una volta, che l'obbligo di quest'ultima consiste nel risolvere la violazione con le misure appropriate, sempre che di tale misure se ne ravvisi la necessità.

Questa conclusione ci sembra in linea con la volontà di graduare le misure correttive e sanzionatorie in relazione alle specifiche situazioni e ci sembra sia anche in continuità con la sentenza del 4 maggio 2023 resa nella causa C-300/21[23] nella quale la Corte, al fine di chiarire se la violazione dei dati personali giustificasse di per sé la richiesta di risarcimento del danno ai sensi dell'art. 82 del GDPR o se fosse necessario dimostrare anche l'esistenza di un danno subito dal ricorrente, ha escluso che il danno comporti *ipso facto* il diritto al risarcimento dello stesso e ha individuato tre condizioni che devono sussistere ai fini del suo esercizio: l'inosservanza del Regolamento, la prova del danno subito e il nesso di causalità tra quest'ultimo e la condotta illecita del titolare del trattamento.

Laddove le suddette condizioni non dovessero coesistere, la violazione dei dati personali non rimarrebbe comunque impunita, ben potendo essere contrastata con altre misure di *public enforcement*, ivi comprese le sanzioni amministrative pecuniarie[24].

---

[22] Il considerando 148, nel riconoscere le sanzioni, incluse le sanzioni amministrative pecuniarie, come un valido strumento per assicurare l'osservanza del Regolamento, ha cura di delineare i criteri a cui dette autorità devono attenersi nella scelta sanzionatoria, ovvero: la natura, la gravità e la durata della violazione, il suo carattere doloso, le misure adottate per mitigare il danno subito, il grado di responsabilità, le precedenti violazioni e le precedenti sanzioni, le modalità con cui l'autorità di controllo ha avuto contezza della violazione, l'adesione a codici di condotta nonché l'eventuale sussistenza di elementi aggravanti o attenuanti.

I criteri poc'anzi elencati sono specularmente riprodotti, seppure con maggiore dettaglio, nell'art. 83, par. 2, del Regolamento al fine di orientare la decisione delle autorità di controllo in ordine alle sanzioni amministrative pecuniarie.

[23] CGUE, C-300/21, *UI c. Österreichische Post AG* (2023).

[24] Cfr. A. Palmieri - R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, in *Il foro italiano*, 6, 2023, 278 ss.; M. Federico, *«La tempesta perfetta»: ultime*

Analogamente, la scelta di non applicare misure correttive nonché le sanzioni amministrative pecuniarie in modo automatico all'esito di un accertamento effettuato dall'autorità di controllo non implica un'impunità laddove sia stato già posto rimedio alla violazione.

5. Considerazioni conclusive

Dalla pronuncia della Corte risulta un rafforzamento del potere discrezionale delle autorià di controllo in virtù dell'applicazione del principio dell'equo bilanciamento tra l'esigenza di proteggere i dati personali e la necessità di evitare forme di automatismo che porterebbero a punire in modo non necessario l'autore della violazione che ha già proceduto a rimediare alla violazione[25]. Grazie al riconoscimento di un margine di discrezionalità in capo alle autorità di controllo si evita una difesa eccessiva a favore delle persone fisiche, che certo hanno il diritto a un accertamento sulla sussistenza di una possibile violazione ma non un automatismo nel risultato sanzionatorio in quanto non esiste un diritto soggettivo all'imposizione di una sanzione amministrativa.
In questo senso, la Corte riconosce che la tutela in materia di trattamento dei dati personali non esige l'intervento rimediale e/o sanzionatorio delle autorità indipendenti in ogni caso di violazione.
L'interrogativo che può porsi è se con questa pronuncia la Corte abbia ampliato ulteriormente ed oltremisura il perimetro di discrezionalità in cui operano le autorità di controllo, con la conseguente compromissione di un'applicazione uniforme del Regolamento in tutta l'Unione europea.
In altri termini, è lecito domandarsi se, nell'effettuare un tale bilanciamento, le autorità di controllo nazionali possano giungere a risultati diversi in relazioni a casi simili.
A nosro avviso, un simile rischio può essere evitato proprio alla luce delle indicazioni fornite dalla Corte la quale ritiene che la discrezionalità delle autorità di controllo in caso di inosservanza del Regolamento ha come confine invalicabile l'obiettivo di garantire un livello coerente ed elevato di protezione dei dati personali.
L'esplicito richiamo da parte dei giudici di Lussemburgo ai considerando 7[26] e 10[27] del GDPR evidenzia la necessità che il *modus operandi* delle auto-

dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva, in *Il foro italiano*, 6, 2023, 293 ss.; G. M. Riccio, *Dati personali e rimedi: diritti degli interessati e profili risarcitori,* in *La nuova giurisprudenza civile commentata*, 5, 2023, 1125 ss.

[25] Così M. D'onofrio, *L'illecito trattamento dei dati come difetto di conformità del contenuto digitale*, in *Giurisprudenza italiana*, 10, 2023, 2256.

[26] In base al considerando 7, le sfide poste dallo sviluppo tecnologico e dalla globalizzazione possono essere affrontate solo attraverso un sistema normativo più coerente e solido, sorretto da significative misure di attuazione, che possa garantire il controllo sui dati e sulla loro circolazione - sempre più facile, rapida e spesso transfrontaliera - nonché una maggiore certezza giuridica e operativa a favore delle persone fisiche e degli attori pubblici e privati.

[27] Il considerando 10 riconosce nell'equivalenza del trattamento dei dati in tutti gli Stati membri il presupposto necessario per «assicurare un livello coerente ed elevato di

rità di controllo nazionali sia sostanzialmente simile e uniforme, al fine di scongiurare le incertezze applicative della normativa europea che la direttiva 95/46/CE non era stata in grado di evitare.

L'indicazione specifica di questo limite, a nostro avviso, non è pleonastica, ma potrebbe essere letta come una sorta di "invito" rivolto alle autorità a rafforzare la loro cooperazione[28], così da sottrarsi al rischio di generare delle disparità di trattamento a parità di condizioni, tenendo conto altresì degli obblighi derivanti dal diritto primario e, in particolare, dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Tale aspetto ci sembra emerga anche dalle conclusioni dell'Avvocato generale, il quale riconosce nell'esistenza di un grave rischio per la lesione dei diritti fondamentali dell'interessato e nell'impatto persistente di una violazione dei dati personali due esempi di circostanze che richiedono il ricorso ad una specifica misura correttiva da parte dell'autorità di controllo[29], con ciò assicurando una mitigazione del loro potere discrezionale.

Come noto, peraltro, l'obiettivo contemplato dal considerando 10 di garantire un applicazione coerente ed uniforme del Regolamento in tutto il territorio europeo è affidato altresì al Comitato europeo per la protezione dei dati personali (o secondo l'acronimo inglese EDPB - European Data Protection Board)[30], il quale, tra i vari strumenti a disposizione, può adottare linee guida per chiarire l'interpretazione del GDPR e armonizzare le decisioni delle autorità di controllo. Queste ultime, infatti, pur operando nei contesti nazionali in piena indipendenza[31], sono tenute a collaborare onde evitare una diversificazione di tutela dei dati personali. In questa pro-

protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione», ma, al tempo stesso, riserva agli Stati la facoltà di disciplinare nel dettaglio specifiche situazioni di trattamento.

[28] In merito alla cooperazione tra le autorità di controllo, si veda M. Macchia – C. Figliolia, *Autorità per la privacy e Comitato europeo nel quadro del general data protection regulation*, in *Giornale di Diritto Amministrativo*, 4, 2018, 429 ss.; F. Parodo, *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali*, in *federalismi.it*, 3 novembre 2021, 126 ss.

[29] § 58 e § 76 delle conclusioni dell'Avvocato generale.

[30] Il Comitato europeo per la protezione dei dati personali, disciplinato nella sezione 3 del GDPR, è il successore del «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali», comunemente conosciuto come "Gruppo art. 29" o WP29, previsto dall'art. 29 della direttiva 95/46/CE. A differenza di quest'ultimo, l'EDPB non è un semplice gruppo consultivo, ma assume la veste di organismo indipendente dell'Unione dotato di personalità giuridica e ha il compito di garantire un'applicazione uniforme del Regolamento in tutti gli Stati membri mediante un ampio ventaglio di poteri, di cui alcuni a carattere vincolante. Esso si compone dei vertici delle autorità di controllo e del Garante europeo per la protezione dei dati, che controlla il rispetto al trattamento dei dati personali dei cittadini da parte delle istituzioni e degli organi dell'Unione e assolve altresì ad una funzione consultiva in materia nei confronti della Commissione, del Consiglio e del Parlamento europeo.

Per un maggiore approfondimento si veda V. Zambrano, *Il Comitato europeo per la protezione dei dati*, in V. Cuffaro – R. D'Orazio – V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 985 ss.

[31] All'indipendenza delle autorità di controllo il Regolamento dedica l'art. 52, il quale presenta una struttura "tripartita".

Il primo paragrafo stabilisce in modo laconico che: «Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri

spettiva, la pubblicazione di linee guida funge da ausilio per la definizione di un comune orientamento a cui le autorità si informano nel rispetto del dovere di collaborazione[32].

Con specifico riguardo ai poteri correttivi, ai sensi dell' art. 70[33], par. 1, lett. k), del Regolamento, l'EDPB «elabora per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, paragrafi 1, 2 e 3, e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83».

Per le sanzioni amministrative pecuniarie, il Comitato europeo per la protezione dei dati personali è già intervenuto in due differenti occasioni stabilendo i casi in cui dette sanzioni sono applicabili[34] e le loro modalità di calcolo[35]. In modo analogo, l'elaborazione di linee guida volte a delimitare le circostanze "residuali" in cui non vi è la necessità di ricorrere a misure correttive potrebbe rappresentare, a nostro avviso, uno strumento idoneo a fronteggiare i rischi di un illimitato potere discrezionale dei garanti.

In ultimo, un ulteriore argomento a favore di una discrezionalità circoscritta delle autorità di controllo può essere tratto dal fatto che, talvolta, sono proprio le circostanze del caso concreto ad esigere il ricorso ad una

---

conformemente al presente regolamento».

Il secondo e il terzo paragrafo specificano in cosa consiste tale indipendenza e si rivolgono ai membri che compongono l'autorità, chiamati a non subire interferenze da soggetti esterni nell'adempimento delle loro funzioni e a non svolgere incarichi incompatibili con il loro mandato.

Gli ultimi tre paragrafi, invece, esplicano le modalità con cui si realizza l'indipendenza. Significativamente, i destinari di queste disposizioni sono gli Stati membri ai quali sono richieste tre differenti garanzie: essi forniscono alle autorità di controllo le risorse e gli spazi necessari per l'espletamento delle loro funzioni, provvedono affinché dette autorità scelgano il proprio personale sottoposto alla loro esclusiva direzione e assicurano che il controllo finanziario a cui le stesse sono assoggettate non comprometta la loro indipendenza.

Per un maggiore approfondimento si veda A. Patroni Griffi, *L'indipendenza del Garante*, in *federalismi.it*, 14 febbrario 2018, 2 ss.

[32] L'esigenza che le autorità di controllo cooperino tra loro per un'applicazione uniforme del GDPR è enunciata nell'art. 57, par. 1, lett. g) come compito dei garanti e nell'art. 63 concernente il meccanismo di coerenza.

[33] L'art. 70 del Regolamento contiene un elenco dettagliato dei compiti affidati al Comitato europeo per la protezione dei dati personali, il quale è tenuto a sorvegliare il Regolamento e la sua corretta applicazione, fornire consulenza alla Commissione, esaminare qualsiasi questione concernente l'applicazione del Regolamento, procedendo o di propria iniziativa oppure su impulso di uno dei suoi membri o della Commissione, elaborare e pubblicare linee guida, raccomandazioni e migliori prassi sia genericamente su qualsiasi questione concernente l'applicazione del Regolamento sia in merito a specifiche situazioni individuate dallo stesso art. 70, verificare e valutare la corretta applicazione delle linee guida, delle raccomandazioni e delle migliori prassi, promuovere l'elaborazione dei codici di condotta, nonché l'istituzione dei meccanismi di certificazione, accreditare gli organismi di certificazione ai sensi dell'art. 43 del Regolamento, i quali sono inseriti in un registro pubblico di cui si occupa lo stesso Comitato, curare un registro elettronico liberamente accesssibile e contenente le decisioni delle autorità di controllo e delle autorità giurisdizionali sulle questioni affrontate nell'ambito del meccanismo di coerenza.

[34] Cfr. Guidelines on the application and setting of administrative fines (wp253), *ec.europa.eu*, 3 ottobre 2017.

[35] Cfr. Guidelines 04/2022 on the calculation of administrative fines under the GDPR, *edph.europa.eu*, 24 maggio 2023.

determinata misura correttiva, giacché l'adozione di altri strumenti non consentirebbe di porre rimedio alla violazione e di garantire la tutela dei dati personali che è il risultato da conseguire. In questo contesto, la stessa Corte ha sottolineato la necessità di apprezzare il comportamento del titolare del trattamento, il cui pronto e immediato intervento nella risoluzione della violazione constatata, nonché l'esatto adempimento di quanto richiesto dal Regolamento *ex ante* ed *ex post* violazione rappresenterebbero dei criteri utili e validi per escludere l'adozione delle misure di cui all'art. 58 del Regolamento e per restringere la discrezionalità dei garanti in ordine alla scelta del "se" ricorrere ai medesimi[36].

Keywords

dati personali – misure correttive – sanzioni amministrative pecuniarie – autorità di controllo – titolare del trattamento

[36] In questo senso la Corte, al § 48 della sentenza, richiama le iniziative intraprese dalla Cassa di risparmio a seguito dell'illecito trattamento dei dati da parte della sua dipendente, lasciando intendere che proprio l'intervento tempestivo ed adeguato della Sparkasse abbia ragionevolmente condotto l'HBDI ad escludere la necessità di una misura correttiva a sostegno dell'interessato.

Il segreto professionale del giornalista alla prova del sequestro: la Cassazione tra libertà di informazione e funzione del processo penale*

Amalia Mariana Buzura

Corte di cassazione, sez. VI penale, 22 gennaio 2025, n. 11498

Il sequestro dei dispositivi informatici del giornalista diretto a identificare la fonte riservata costituisce una forma di compressione del segreto professionale e può essere disposto solo previa verifica giudiziale dei requisiti indicati dall'art. 200, co. 3, c.p.p.

Sommario

1. La Cassazione e il sequestro informatico a carico del giornalista: contesto, motivi, decisione. - 2. Tutela dell'anonimato della fonte informativa del giornalista e libertà di informazione: un presidio della democrazia costituzionale. - 2.1. La tutela del segreto sulla fonte nell'elaborazione della Giurisprudenza Europea. - 3. La portata dell'art. 200, c. 3, c.p.p. alla luce della giurisprudenza costituzionale e del diritto convenzionale. - 4. La segretezza sulla fonte informativa del giornalista ostacola la funzione cognitiva del processo penale? - 5. Conclusioni: i limiti prescritti dall'art. 200, c. 3, c.p.p. si estendono ai mezzi di ricerca della prova.

1. La Cassazione e il sequestro informatico a carico del giornalista: contesto, motivi, decisione

Con la sentenza n. 11498 del 2025, la Corte di cassazione ha escluso la legittimità del sequestro dei dispositivi digitali di un giornalista, disposto dal pubblico ministero al fine di risalire all'identità della persona da cui il giornalista aveva ricevuto notizie di carattere fiduciario, in assenza dei presupposti indicati dall'art. 200, c. 3, c.p.p.
Il provvedimento ablativo era stato adottato a seguito della pubblicazione,

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

su un quotidiano, di atti coperti da segreto istruttorio, relativi al suicidio di un'allieva della Scuola Marescialli dell'Arma dei carabinieri, iscritto a modello 45 (registro dei fatti non costituenti reato).
Aperta un'indagine per il reato di rivelazione illecita di segreti d'ufficio, la Procura disponeva la perquisizione e il contestuale sequestro dei dispositivi informatici in uso al giornalista. L'operazione si concludeva con la duplicazione integrale di tutti i dati ivi contenuti.
Avverso il decreto di perquisizione e sequestro, la difesa proponeva istanza di riesame, rigettata dal Tribunale competente. La decisione veniva successivamente impugnata mediante ricorso per Cassazione, articolato su tre motivi, ricondotti dalla stessa Corte a due profili distinti: il primo, di diritto penale sostanziale, relativo alla configurabilità del concorso dell'*extraneus* nel reato previsto dall'art. 326 c.p., in assenza dell'individuazione del pubblico ufficiale autore della rivelazione; il secondo, di ordine processuale, riguardante la legittimità del sequestro probatorio dei dispositivi informatici in uso al giornalista, con riferimento ai limiti imposti dagli artt. 256, 200 e 191 c.p.p., nonché dagli artt. 1, 8 e 10 CEDU.
Ritenuta infondata la questione di diritto penale sostanziale, la Corte ha spostato l'analisi sul versante processuale, rilevando, anzitutto, che il sequestro dei dispositivi informatici era finalizzato esclusivamente all'identificazione della fonte riservata da cui il giornalista aveva ricevuto gli atti coperti da segreto.
Accertata tale finalità, la Corte ha verificato se ricorressero i presupposti indicati dall'art. 200, c. 3, c.p.p., che consentono, in via eccezionale, di imporre al giornalista la rivelazione della fonte: *i)* l'indispensabilità della notizia ai fini della prova del reato per cui si procede, *ii)* la possibilità di accertare la veridicità della notizia solo attraverso l'identificazione della fonte, *iii)* la previa autorizzazione del giudice.
Nel caso di specie, secondo quanto ricostruito dalla Corte, l'identificazione della fonte non avrebbe apportato alcun contributo rilevante all'accertamento di fatti illeciti. Il mezzo di ricerca della prova si presentava, pertanto, come un'iniziativa investigativa priva di adeguata giustificazione probatoria, finalizzata unicamente ad aggirare il vincolo di riservatezza che tutela il rapporto fiduciario tra giornalista e fonte.

2. Tutela dell'anonimato della fonte informativa del giornalista e libertà di informazione: un presidio della democrazia costituzionale

La pronuncia in epigrafe impone una riflessione sul bilanciamento tra due diritti di rango costituzionale che, in circostanze come quella esaminata, si trovano in fisiologica tensione: da un lato, la libertà di stampa di cui all'art. 21 Cost.[1]; dall'altro, l'interesse pubblico all'accertamento dei fatti

[1] La dottrina sull'art. 21 Cost. è sterminata. Cfr., *ex multis*: A. Ambrosi, *sub art. 21 Cost.*, in V. Crisafulli – L. Paladin (a cura di), *Commentario breve alla Costituzione*, Padova, 1990, 129 ss.; P. Barile, *Libertà (aspetti etici)*, in *Enciclopedia del diritto*, vol. XXIV, Milano, 1974, spec. 424 ss.; G. Corrias Lucente, *Internet e libertà di manifestazione del pensiero*, in *Diritto dell'informazione e dell'informatica*, 2000, 597 ss.; P. Costanzo, *Informazione nel diritto costituzionale*, in *Digesto*

penalmente rilevanti, che costituisce la finalità propria del processo penale, rinvenibile, come è noto, dall'art. 27 Cost. [2].

Tradizionalmente, il rapporto tra giustizia penale e stampa viene considerato nella prospettiva del rischio che l'informazione comprometta l'ac-

delle discipline pubblicistiche, vol. VIII, 1993, 319 ss.; V. Crisafulli, *Problematica della «libertà di informazione»*, in *Il Politico*, 2, 1964, 285; F. Donati, *L'art. 21 della Costituzione settanta anni dopo*, in *medialaws.eu*, 1, 2018, 92 ss.; C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958; S. Fois, *Principi costituzionali e libera manifestazione del pensiero*, Milano, 1957; M. Luciani, *La libertà di informazione nella giurisprudenza costituzionale italiana*, in *Politica del diritto*, 4, 1989, 605 ss.; M. Manetti, *La libertà di manifestazione del pensiero*, in R. Nania – P. Ridola (a cura di), *I diritti costituzionali*, vol. II, 2ª ed. aggiornata, Torino, 2006, 767 ss.; A. Pace, *Informazione: valori e situazioni soggettive*, in Aa.Vv., *Studi in onore di Maurizio Pedrazza Gorlero. La libertà di informazione e la democrazia costituzionale*, vol. II, Napoli, 2014, 441 ss.; A. Pace – M. Manetti, *Art. 21. Rapporti civili. La libertà di manifestazione del proprio pensiero*, in G. Branca – A. Pizzorusso (a cura di), *Commentario della Costituzione*, Bologna–Roma, 2006; A. Valastro, *sub art. 21 Cost.*, in R. Bifulco – A. Celotto – M. Olivetti (a cura di), *Commentario alla Costituzione*, vol. I, Torino, 2006, 451 ss.; G.E. Vigevani, *sub art. 21*, in *La Costituzione italiana. Commento articolo per articolo*, vol. I, *Principi fondamentali. Parte I – Diritti e doveri dei cittadini (artt. 1–54)*, 2018, 156 ss.; Id., *Informazione e potere*, in *Enciclopedia del diritto. I Tematici*, vol. V, 2023, 223 ss.; Id., *La protezione del segreto del giornalista al tempo di internet*, in *Costituzionalismo.it*, 3, 5 dicembre 2011.

V. anche Aa.Vv., *Processo penale e informazione. Proposte di riforma e materiali di studio*, coordinato da G. Giostra,, Macerata, 2001, che raccoglie il dibattito interno al gruppo di ricerca dedicatosi al tema «Processo penale e informazione» e il progetto di riforma elaborato in tale sede. V. spec. E. Zappalà, *Il segreto giornalistico*, ivi, 84 ss.

[2] Cfr. O. Mazza, *Il processo che verrà: dal cognitivismo garantista al decisionismo efficientista*, in *Archivio penale*, 2022, 2, 3: «il processo penale ha un'unica finalità, che è quella cognitiva da conseguire attraverso il rispetto delle garanzie che la Costituzione pone a tutela dell'imputato»; Id., *La verità giudiziale nel sistema delle fonti tecnologiche*, in Id., *Tradimenti di un codice*, Torino, 2020, 3: «a nessun livello, né teorico né pratico, potrebbe infatti predicarsi la celebrazione di un processo che non avesse finalità cognitive, pena lo scadimento della giustizia penale verso un modello puramente decisionista connotato da arbitrarietà e irrazionalità». Per un'analisi puntuale della "cognizione" perseguita nel processo penale – vale a dire della verità cui tende il giudizio e dell'evoluzione registrata nel passaggio dal sistema misto del 1930 al modello tendenzialmente accusatorio introdotto con il codice del 1989 – si veda, Id., *Verità reale e verità processuale*, in *Digesto delle discipline penalistiche.*, Aggiornamento, Torino, 2014, 713 ss.

Inoltre, *ex multis*: A. Bassi, *Principio dispositivo e principio di ricerca della verità materiale: due realtà di fondo del nuovo processo penale*, in *Cassazione penale*, 1993, 1371 ss.; F. Callari, *Verità processo prova certezza: il circuito euristico della giustizia penale*, in *Rivista di diritto processuale*, 2013, 1346 ss.; G. Canzio, *Prova scientifica, ricerca della "verità" e decisione giudiziaria nel processo penale*, in Aa.Vv., *Decisione giudiziaria e verità scientifica*, Milano, 2005, 71 ss.; F. Caprioli, *Verità e giustificazione nel processo penale*, in *Rivista italiana di diritto e procedura penale*, 2013, 610; F. Carnelutti, *A proposito di ricerca della verità*, in *Rivista di diritto processuale*, 1960, 675 ss.; E. Carnevale, *Carattere della verità nel processo penale*, in *Diritto criminale*, III, Roma, 1932; F. D'Agostini, *L'uso scettico della verità*, in Aa.Vv., *"Verità" del precetto e della sanzione penale alla prova del processo*, a cura di G. Forti – G. Varraso – M. Caputo, Napoli, 2014, 25 ss.; U. Ferrari, *La verità penale e la sua ricerca nel diritto processuale italiano*, Milano, 1927; A. Garofoli, *Funzione dimostrativa della prova (verità del fatto nel processo e sistema probatorio)*, in *Rivista di diritto processuale*, 2001, 77 ss.; M. Nobili, *Verità e dibattimento*, in Id., *Scenari e trasformazioni del processo penale*, Padova, 1998, 50 ss.; P.P. Rivello, *"Verità" e processo*, in *Rivista italiana di diritto processuale penale*, 2010, 1230 ss.; F. Stella, *Verità, scienza e giustizia. Le frequenze medio-basse nella successione di eventi*, in *Rivista italiana di diritto processuale penale*, 2002, 1215 ss.; G. Ubertis, *La ricerca della verità giudiziale*, in Aa.Vv., *La conoscenza del fatto nel processo penale*, a cura di G. Ubertis, Milano, 1992, 1 ss.

certamento: si teme, con ragione, che la rappresentazione mediatica[3] del processo condizioni lo svolgimento del giudizio e alteri le dinamiche del giusto processo[4]. La sentenza in commento sposta l'asse del discorso, soffermandosi su una questione diversa ma altrettanto cruciale: fino a che punto le esigenze investigative e cognitive possono legittimamente comprimere la libertà di informare e, con essa, il diritto del giornalista a tutelare le proprie fonti?

Il rischio considerato, in questa prospettiva, non è più quello di un processo inquinato dall'informazione, ma di un'informazione disinnescata dal processo.

Per affrontare tale delicata questione è necessario chiarire, in via preliminare, il significato profondo che l'ordinamento costituzionale attribuisce alla libertà di informazione e il ruolo che essa riveste nel sistema democratico. Per questo, il punto di partenza non può che essere l'art. 21 Cost., che garantisce a «tutti» il «diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione» e assicura la libertà di stampa prevedendo che «non può essere soggetta ad autorizzazioni o censure».

Sebbene la norma esprima formalmente una libertà individuale, è ormai opinione consolidata che essa tuteli anche un interesse collettivo: quello della cittadinanza a ricevere l'informazione libera, pluralistica e affidabile[5]. Come chiarito dalla Corte costituzionale, la libertà di stampa svolge una funzione «insostituibile ai fini dell'informazione dei cittadini e quindi della formazione di una pubblica opinione avvertita e consapevole»[6]. L'informazione non è solo uno strumento di espressione, ma una condizione strutturale per l'esercizio effettivo dei diritti politici[7]: solo cittadini informati possono partecipare consapevolmente alla vita pubblica, valutare l'operato delle istituzioni e contribuire al controllo democratico del potere.

---

[3] O. Mazza, nella recente intervista *La giustizia non è un rito di espiazione: stiamo regredendo alla barbarie*, 15 aprile 2025, in *IlDubbio.it*, sottolinea l'ulteriore amplificarsi di questo fenomeno posto che al processo "mediatico" tradizionale si aggiunge quello ancora più pericoloso «social-mediatico».

[4] Cfr., *ex multis*, G. Caneschi, *Processo penale mediatico e presunzione di innocenza: verso un'estensione della garanzia?*, in *Archivio penale*, 2021, 3; C. Conti, *Processo mediatico e processo penale: per un'analisi critica dei casi più discussi da Cogne a Garlasco*, Milano, 2016; M. Chiavario, *I rapporti giustizia-«media» nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Foro italiano*, V, 2000, 209 ss.; G. Giostra, *Processo penale e informazione*, Bologna, 1989; Id., *Processo penale mediatico*, in *Enciclopedia del diritto. Annali*, X, 2017, 646 ss.; Id., *La giustizia penale nello specchio deformante della cronaca giudiziaria*, in *medialaws.eu*, 2018, 3, 23 ss.; G. Mantovani, *Informazione, giustizia penale e diritti della persona*, Torino, 2011; N. Triggiani, *Giustizia penale e informazione: la pubblicazione di notizie, atti e immagini*, Bari, 2012; F. Petrelli, *Comunicare il processo*, in *Questionegiustizia.it*, 2018, 4, 275 ss.; P. Rivezzo, *L'ingiusto processo mediatico*, in *medialaws.eu*, 2018, 3, 62 ss.

[5] Per tutti, v. G.E. Vigevani, *Informazione e potere*, cit., 223.

[6] Corte cost., 9 giugno 1972, n. 105, in *giurcost.org*, *considerato in diritto* n. 3.

[7] G.E. Vigevani, *Informazione e potere*, cit., 225: «come è evidente, la libera informazione è essenziale per assicurare l'universalità dei diritti politici, posto che per partecipare in modo effettivo e consapevole all'organizzazione della vita pubblica i singoli devono essere compiutamente informati; il diritto di informare ha dunque un ruolo decisivo nel rapporto fra cittadini e potere (pubblico o privato che sia), consentendo ai primi di conoscere, controllare ed eventualmente sanzionare il secondo».

Limitare l'accesso all'informazione significa quindi compromettere non solo l'autonomia del giornalista, ma la qualità del dibattito pubblico e la capacità del sistema informativo di esercitare la propria funzione di vigilanza.
In questo quadro, emerge la *ratio* della tutela della fonte giornalistica che non rappresenta un privilegio corporativo della categoria dei giornalisti, ma un presidio funzionale alla libertà di informazione della collettività. La protezione della riservatezza della fonte è infatti il presupposto che consente alla fonte stessa di parlare senza timore. E, se la fonte parla, il giornalista può ottenere informazioni; se le ottiene, può diffonderle; se le diffonde, la collettività è informata.
È in questa sequenza, tanto semplice quanto essenziale, che si radica l'effettività del diritto a essere informati[8].

2.1. La tutela del segreto sulla fonte nell'elaborazione della giurisprudenza europea

L'importanza della tutela della fonte giornalistica riceve autorevole conferma anche nella giurisprudenza della Corte europea dei diritti dell'uomo[9].

[8] Sul rapporto tra processo penale e segreto del giornalista v., in particolare, S. Erbani, *Processo penale e obblighi del giornalista*, in *Questione giustizia*, 2001, 791 ss.; G. Lattanzi – E. Lupo, *sub art. 200 c.p.p.*, in P. Bronzo – E. Gallucci (a cura di), *Codice di procedura penale*, Milano, Giuffrè, 2020, 189 ss.; P. Mutti, *Segreto professionale*, in *Digesto delle discipline penalistiche*, vol. XIII, Torino, Utet, 1997, 133 ss.; T. Rafaraci, *Segreto del giornalista e processo penale,* in *Cassazione penale*, 1991, 919 ss.; P. Spagnolo, *Il segreto giornalistico nel processo penale*, Milano, Giuffrè, 2014, 69 ss.; V. Vasta, *Libertà di informazione e segreto giornalistico sulla fonte delle notizie*, in *Rivista italiana di diritto e procedura penale*, 2021, 324 ss.; G. E., Vigevani*, La protezione del segreto del giornalista al tempo di internet*, cit.
Il tema è stato oggetto di ampio dibattito ancora prima dell'entrata in vigore del nuovo codice del 1989 che, per la prima volta, riconosce in termini espressi la tutela del segreto del giornalista. Cfr. Aa.Vv., *Il segreto professionale del giornalista. Atti della Tavola rotonda del 15 marzo 1977 promossa dalla Direzione della Rivista Giurisprudenza di merito di concerto con l'Ordine Interregionale dei Giornalisti del Lazio*, in *Giurisprudenza di merito*, 1977, IV, 963 ss.; A. Pace, *Sulla rilevanza processuale del segreto professionale dei giornalisti in Italia e negli Stati Uniti d'America*, in *Giurisprudenza costituzionale*, 1978, I, 1261 ss.; E. Pennacchini, *Il segreto professionale dei giornalisti in relazione al segreto di Stato*, in Aa. Vv., *Segreti e prova penale. Atti del Convegno*, Milano, 1979, 217 ss.; C. Piacentini, *Spunti critici sulla riconoscibilità del segreto giornalistico nel processo penale*, in *Giustizia penale*, 1979, III, 285 ss.; P. Pisa, *Il "segreto giornalistico" nel processo penale*, cit., 296. Nella giurisprudenza, la titolarità dello *ius tacendi* in capo al giornalista risultava esclusa da Cass., Sez. VI, 16 ottobre 1981, Fallaci, in *Cassazione penale*, 1983, 143; Pret. Roma, 18 giugno 1977, Fallaci, in *Giustizia penale*, 1977, III, 519; contra, Trib. Min. Roma, 26 aprile 1976, Pelosi, in *Rivista di diritto processuale*, 1976, 398, con nota di A. Crespi, *La vigente procedura "ridotta alla moderna pratica": il c.d. segreto del giornalista nel processo penale.*

[9] Analizzano la giurisprudenza convenzionale M. Castellaneta, *La libertà di stampa nel diritto internazionale ed europeo*, Bari, Cacucci, 2012; A. Cardone – M. Oetheimer, *sub art. 10*, in S. Bartole – P. De Sena – V. Zagrebelsky (a cura di), *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2011, 397 ss.; A. Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti*, cit., 45 ss.; G.E. Vigevani, *Libertà di espressione e discorso politico tra Corte europea dei diritti e Corte costituzionale*, in N. Zanon (a cura di), *Le corti dell'integrazione europea e la Corte costituzionale italiana*, Napoli, 2006, 469 ss.; Id., *La protezione del segreto del giornalista al tempo di internet*, cit., 2 il quale afferma che è fondamentale analizzare tale giurisprudenza

A partire dal caso *Goodwin c. Regno Unito* (1996), i giudici di Strasburgo hanno qualificato la riservatezza della fonte come componente strutturale e corollario della libertà di informazione tutelata dall'art. 10 CEDU, funzionale al ruolo della stampa come public watchdog[10].

In particolare, è stato evidenziato come la mancata protezione dell'anonimato comprometterebbe la stessa disponibilità futura di fonti informative, generando un effetto dissuasivo sistemico (c.d. *chilling effect*): chi è in possesso di informazioni scomode o sensibili sarebbe disincentivato a rivelarle, se non potesse confidare in una garanzia di anonimato[11].

Sulla base di questa consapevolezza, la Corte europea ha evidenziato con estrema circospezione i presupposti che possono legittimare un'ingerenza nella riservatezza delle fonti giornalistiche ai sensi dell'art. 10 CEDU.

Più precisamente, si ritiene che affinché l'autorità giudiziaria possa legittimamente imporre la rivelazione della fonte, devono sussistere cumulativamente alcune condizioni: (*i*) l'ingerenza deve essere prevista dalla legge; (*ii*) deve perseguire una preminente esigenza di interesse pubblico, quale, per esempio, la tutela della sicurezza nazionale, la prevenzione dei reati o la protezione dei diritti altrui; (*iii*) deve risultare «necessaria in una società democratica»[12].

Quest'ultimo requisito impone un esame concreto e stringente di proporzionalità e sussidiarietà: la compressione del segreto può dirsi ammissibile solo se risponde a un bisogno sociale urgente e se non sussistano alternative investigative equivalenti. Non è sufficiente dimostrare un'utilità generica ai fini dell'indagine: data la valenza sistemica della riservatezza delle fonti, la rivelazione della loro identità può essere imposta solo in presenza

---

proprio perché «nella prospettiva di Strasburgo forse si coglie meglio quel legame tra trasparenza del potere e libertà dell'informazione».

[10] CEDU, *Goodwin c. Regno Unito*, ric. 28957/95 (1996), in *Rivista internazionale dei diritti dell'uomo*, 1996, 441 ss., con nota di M. Castellaneta, *Il caso Goodwin e la protezione delle fonti giornalistiche nella convenzione europea e nell'ordinamento italiano*. I principi ivi affermati sono stati ribaditi e rafforzati da successive pronunce. Cfr. CEDU, *Tillack c. Belgio*, ric. 20477/05 (2007). Anche il Communiqué du Greffier che accompagna tale sentenza e ne sintetizza i contenuti essenziali evidenzia che la Corte ha inteso ribadire «l'importanza essenziale della stampa in una società democratica e il ruolo cardine svolto dalla protezione delle fonti giornalistiche, considerata una pietra angolare della libertà di stampa» (*La Cour rappelle le rôle essentiel que joue la presse dans une société démocratique et la protection des sources journalistiques, pierre angulaire de la liberté de la presse*). E, ancora, CEDU, *Sanoma Uitgevers B.V. c. Paesi Bassi,* ric. 38224/03 (2010), in *Cassazione penale*, 2011, 397; CEDU, *Ressiot e altri c. Francia,* ric. 15054/07 (2012), in *Processo penale e giustizia*, 1, 2013, 51 ss., con nota di F. Trapella, *Esigenze d'indagine e tutela delle fonti giornalistiche secondo la Corte e.d.u.*; CEDU, *Jecker c. Svizzera,* ric. 35449/14 (2020), in *giustiziainsieme.it*, con nota di M. Castellana, *Segretezza delle fonti giornalistiche nel quadro della CEDU. Una nuova pronunzia della Corte di Strasburgo.*

[11] Cfr. CEDU, *Goodwin c. Regno Unito*, cit., § 39: «*Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest*»; CEDU, *Sanoma Uitgevers B.V. c. Paesi Bassi*, cit., § 71: «*chilling effect will arise wherever journalists are seen to assist in the identification of anonymous sources*».

In dottrina, approfondisce il tema, anche attraverso puntuali richiami alla giurisprudenza sovranazionale, V. Faggiani, *Il* chilling effect *sulla libertà di informazione dei giornalisti nel quadro della crisi dello Stato di diritto*, *in lceonline.eu,* 2, 2023, 271 ss.

[12] CEDU, *Tillack c. Belgio*, cit., § 60.

di un apporto probatorio determinante e altrimenti irraggiungibile[13].

3. La portata dell'art. 200, c. 3, c.p.p. alla luce della giurisprudenza costituzionale e del diritto convenzionale

La giurisprudenza costituzionale e convenzionale, qui pure solo rapidamente richiamate, forniscono preziose coordinate per comprendere la portata dell'art. 200, c. 3, c.p.p.[14]

[13] Cfr. CEDU, *Jecker c. Svizzera*, cit., che ripropone testualmente quanto affermato già nel 1996, CEDU, *Goodwin c. Regno Unito*, cit.: «In generale, la "necessità" di qualsiasi restrizione all'esercizio della libertà di espressione deve essere stabilita in modo convincente. [...] Certo, spetta in primo luogo alle autorità nazionali valutare se esiste una "pressante necessità sociale" in grado di giustificare tale restrizione, esercizio per il quale godono di un certo margine di discrezionalità. Tuttavia, la discrezione nazionale si scontra con l'interesse della società democratica a garantire e mantenere la libertà di stampa. Analogamente, a tale interesse deve essere dato grande peso nel determinare, come richiesto dall'articolo 10, comma 2, se la restrizione sia proporzionata allo scopo legittimo perseguito. In breve, le limitazioni alla riservatezza delle fonti giornalistiche richiedono l'esame più scrupoloso da parte della Corte. Nell'esercizio della sua funzione di controllo, la Corte non ha il compito di sostituirsi ai giudici nazionali, ma di riesaminare, ai sensi dell'articolo 10, le decisioni da essi adottate secondo il loro potere discrezionale. A tal fine, la Corte deve considerare l'"ingerenza" di cui trattasi alla luce della causa nel suo complesso, al fine di determinare se le ragioni addotte dalle autorità nazionali per giustificarla appaiano "pertinenti e sufficienti"».

[14] L'art. 200, c. 3, c.p.p., non è l'unica disposizione dedicata al segreto della fonte informativa del giornalista. Infatti, ai sensi dell'art. 2 della L. 3 febbraio 1963, n. 69, *Ordinamento della professione di giornalista*, pubblicato in *Gazz. Uff. n.49 del 20 febbraio 1963,* statuisce che «è diritto insopprimibile dei giornalisti la libertà di informazione e di critica, limitata dall'osservanza delle norme di legge dettate a tutela della personalità altrui ed è loro obbligo inderogabile il rispetto della verità sostanziale dei fatti, osservati sempre i doveri imposti dalla lealtà e dalla buona fede.
Devono essere rettificate le notizie che risultino inesatte, e riparati gli eventuali errori.
Giornalisti e editori sono tenuti a rispettare il segreto professionale sulla fonte delle notizie, quando ciò sia richiesto dal carattere fiduciario di esse, e a promuovere lo spirito di collaborazione tra colleghi, la cooperazione fra giornalisti e editori, e la fiducia tra la stampa e i lettori».
A queste disposizioni si aggiungono anche previsioni di atti sovranazionali. È il caso, per esempio, della Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information; rileva inoltre anche la Premessa della Carta dei doveri del giornalista, Documento CNOG-FNSI dell'8 luglio 1993, in www.odg.it. Fra i Principi della Carta si precisa che «Il giornalista è tenuto ad osservare il segreto professionale, quando ciò sia richiesto dal carattere fiduciario delle sue fonti. In qualsiasi altro caso il giornalista deve dare la massima trasparenza alle fonti». Nel paragrafo dedicato alle fonti, infine, si prevede che «Nel caso in cui le fonti chiedano di rimanere riservate, il giornalista deve rispettare il segreto professionale e avrà cura di informare il lettore di tale circostanza. In qualunque altro caso il giornalista deve sempre rispettare il principio della massima trasparenza delle fonti d'informazione, indicandole ai lettori o agli spettatori con la massima precisione possibile. L'obbligo alla citazione della fonte vale anche quando si usino materiali delle agenzie o di altri mezzi di informazione, a meno che la notizia non venga corretta o ampliata con mezzi propri, o non se ne modifichi il senso e il contenuto. In nessun caso il giornalista accetta condizionamenti dalle fonti per la pubblicazione o la soppressione di una informazione».

La disposizione prevede che il giornalista iscritto all'albo non possa essere obbligato a rivelare l'identità delle persone dalle quali ha ricevuto notizie fiduciariamente, salvo che siano soddisfatti congiuntamente tre requisiti: (*i*) l'indispensabilità della rivelazione ai fini della prova del reato; (*ii*) l'impossibilità di accertare altrimenti la veridicità della notizia; (*iii*) la presenza di un provvedimento giudiziario autorizzativo.
Ebbene, questa formulazione deve essere intesa con particolare serietà e rigore: la tutela della fonte è la regola, mentre la deroga del segreto deve essere rara eccezione, circoscritta e motivata.
Il caso specifico da cui origina la sentenza in epigrafe, impone un'ulteriore considerazione: le garanzie previste dall'art. 200, c. 3, c.p.p. non possono ritenersi circoscritte alla sola ipotesi -espressamente contemplata dal testo della norma- dell'ordine giudiziale impartito in sede di deposizione testimoniale. Al contrario, devono trovare applicazione anche, e forse con ancor maggiore intensità, anche in sede di indagini quando venga attivato un mezzo di ricerca della prova avente come finalità l'identificazione della fonte informativa[15].
In questo secondo scenario, infatti, l'interferenza con il diritto all'informazione risulta ancor più incisiva e ad essa si aggiungono ulteriori potenziali lesioni di diritti fondamentali: si determina un'ingerenza generalizzata in uno spazio riservato che, oltre al nome della fonte, può contenere, e di solito contiene, dati personali del giornalista e persino dati di soggetti terzi, del tutto estranei alla vicenda oggetto di indagine.
Da ciò discende la necessità di un vaglio particolarmente attento circa la proporzionalità della misura rispetto all'interesse investigativo perseguito, che non sussiste ove non siano pienamente rispettate le condizioni previste dall'art. 200, c. 3, c.p.p.
In tale prospettiva, l'onere motivazionale si fa particolarmente stringente: non è sufficiente richiamare l'interesse all'accertamento, né è ammissibile un rinvio a valutazioni legislative generali in ordine, per esempio, alla gravità del reato. Occorre, al contrario, individuare in concreto le ragioni per cui, nel caso specifico, la protezione della fonte dovrebbe cedere ed entro quali limiti il sequestro può essere attuato.

4. La segretezza sulla fonte informativa del giornalista ostacola la funzione cognitiva del processo penale?

Tutto ciò chiarito, è ora necessario interrogarsi sull'impatto di una simile disposizione sull'altro pilastro costituzionale coinvolto, cui si è già accennato: la funzione cognitiva del processo penale.

[15] Sul rapporto tra segreto del giornalista e sequestro probatorio v. L. Bacchini, *Il sequestro probatorio nei confronti del giornalista non indagato: il problema del bilanciamento di interessi costituzionalmente garantiti ed il rischio di elusione delle tutele*, in *Diritto dell'informazione e dell'informatica,* 6, 2008, 743 ss.; F. Porcu*, Sequestro probatorio e segreto giornalistico: crocevia fra processo penale e informazione*, in *Diritto Penale e Processo*, 5, 2015, 555 ss.; V. Sisto, *Mezzi di ricerca della prova "intrusivi" e diritto alla riservatezza del giornalista: il ruolo guida del principio di proporzionalità¸* in *Processo penale e giustizia*, 5, 2021, 1218 ss.

Ebbene, l'art. 200, c. 3, c.p.p. costituisce, stando alle categorie teoriche della procedura penale, un "limite probatorio", la cui violazione comporta -o almeno dovrebbe comportare- l'inutilizzabilità della prova ai sensi dell'art. 191 c.p.p., con la conseguente esclusione definitiva di quel dato cognitivo dal patrimonio probatorio del giudice[16].

È importante però chiarire che, al pari di tutti i c.d. "limiti" imposti dal "diritto probatorio", anche il segreto sulla fonte non nega il valore dell'accertamento, bensì ne definisce il metodo, subordinando la ricerca della verità al rispetto di principi.

Si tratta del riflesso di un passaggio culturale essenziale segnato dal codice del 1989[17]: il processo non mira più alla verità storica assoluta, utopistica[18], perseguibile anche a scapito dei diritti fondamentali, ma alla ricostruzione di una verità giudiziale, che può essere raggiunta solo attraverso un percorso ispirato a valori costituzionali.

Pur non potendo approfondire in questa sede il tema della verità nel processo penale[19], è necessario e sufficiente considerare che limiti probatori e le forme processuali selezionano le modalità attraverso cui la prova può entrare nel processo, costituendo barriere a tecniche lesive di beni fondamentali[20], come è la libertà di manifestazione del pensiero e i suoi corollari.

---

[16] Sul tema dell'inutilizzabilità e dei limiti che possono innescare tale sanzione processuale la produzione scientifica è particolarmente estesa. Senza pretesa di completezza, si segnalano, tra gli altri: N. Galantini, *Inutilizzabilità della prova e diritto vivente*, in *Rivista italiana di diritto e procedura penale*, 2012, 64 ss. Id., *L'inutilizzabilità della prova nel processo penale*, Padova, 1992; Id., *Vizi degli atti processuali penali*, in *Digesto delle discipline penalistiche,* Aggiornamento, 1999, 340 ss.; Id, *voce Inutilizzabilità*, in *Enciclopedia del diritto*, Aggiornamento I, 1997, 690 ss.; E. Gironi, *Linee sistematiche ed orientamenti giurisprudenziali sull'inutilizzabilità della prova nel processo penale*, in *Foro. it*., II, 2000, 218 ss.; F. Grifantini, *Inutilizzabilità*, in *Digesto delle discipline penalistiche*, vol. VII, Torino, 1993, 241 ss.; G. Illuminati, *L'inutilizzabilità della prova nel processo penale italiano*, in *Rivista italiana di diritto e procedura penale*, 2010, 521 ss.; G. Pierro, *Una nuova specie di invalidità: l'inutilizzabilità degli atti processuali penali,* Salerno, 1992; A. Scella, *L'inutilizzabilità della prova nel sistema del processo penale*, in *Rivista di diritto processuale penale*, 1992, 203 ss.; Id., *Prove penali e inutilizzabilità. Uno studio introduttivo*, Torino, 2000.

[17] In generale, sulla scelta del nuovo codice di abbandonare il riferimento, anche terminologico, al concetto di verità v. E. Amodio, *Verso una storia della giustizia penale in età moderna e contemporanea*, in *Criminalia*, 2010, 13, secondo il quale «si è voluto esorcizzare un passato inquisitorio in cui il principio di 'ricerca della verità materiale', in tutto il continente europeo, [era stato] il pilastro di un sistema probatorio che [aveva] consentito di scavalcare qualsiasi ordine o limite nell'iter di accertamento del reato». V. anche F. Caprioli, *Verità e giustificazione nel processo penale*, in *Revista Brasileira de Direito Processual Penal*, 3(1), 2017, 3, spec. nt. 4.

[18] In proposito v. L. Ferrajoli, *Diritto e ragione. Teoria del garantismo penale*, Milano-Bari, 1989, 23, ove chiarisce che «l'idea contraria che si possa raggiungere ed asserire una verità oggettivamente e assolutamente certa è infatti un'ingenuità epistemologica». L'idea della verità materiale è rigettata anche da D. Negri, *Fumus commissi delicti. La prova per le fattispecie cautelari*, 2004, 255, in quanto frutto di una «concezione epistemologica ormai superata». Ripudia la verità materiale anche R. Kostoris, *Giudizio*, in *Enciclopedia giuridica Treccani*, vol. XV, Aggiornamento, Roma, 1997, 8 ss., in quanto «chimerica», «ingenua», «fuorviante».

[19] *Cfr. supra*, nt. 2.

[20] Come evidenziato anche da F. R. Dinacci, *Regole di giudizio (dir. proc. pen.),* in *Archivio penale*, 5, 2013: «la procedura ed il sistema probatorio non costituiscono un mero strumento tecnico e come tale neutro, indipendente dai valori; al contrario, la disciplina della prova è diretta espressione dei principi costituzionali in quanto riflette in modo immediato le scelte ideologiche del legislatore». In proposito v. anche A. Bargi, *Procedimento probatorio*

Peraltro, a ben vedere, il limite posto dal segreto sulla fonte si configura come relativo e non assoluto: in via eccezionale, qualora ogni altro mezzo si riveli inadeguato, la legge consente una deroga.
Infine, considerato nella sua proiezione generale e non in relazione al singolo caso, il vincolo imposto dall'art. 200, c. 3, c.p.p. non rappresenta affatto un ostacolo alla verità. Al contrario, proprio la protezione della fonte giornalistica garantisce l'emersione di informazioni di rilevanza pubblica, alimentando forme di controllo democratico e stimolando indagini su fatti altrimenti destinati a rimanere nell'ombra. Tutto ciò non sorprende: i limiti spesso agevolano la ricostruzione della verità. La storia del processo inquisitorio e del codice del 1930 insegna, infatti, come l'assenza di limiti e garanzie conduca non a una maggiore verità, ma a un accertamento fragile, distorto e spesso disancorato dalla realtà.

5. Conclusioni: i limiti prescritti dall'art. 200, c. 3, c.p.p. si estendono ai mezzi di ricerca della prova

Alla luce delle considerazioni svolte, la pronuncia della Corte di cassazione appare, nel suo impianto generale, condivisibile: «il pubblico ministero non può sequestrare a strascico telefoni e pc del giornalista per scoprirne la fonte informativa»[21]. «Dalla Suprema Corte giunge un chiaro segnale contro prassi investigative (…) disinvolte per eludere la tutela delle libertà fondamentali della persona»[22].
Non mancano, tuttavia, profili che avrebbero forse meritato un approfondimento più analitico.
In primo luogo, il decreto di sequestro ha interessato l'intero sistema informatico in uso al giornalista, senza che risultino adottati accorgimenti volti a circoscrivere l'acquisizione ai soli dati pertinenti all'indagine. Ancorché il pubblico ministero avesse fornito indicazioni operative per la perquisizione, non vi è traccia di un effettivo utilizzo di chiavi selettive da parte della polizia giudiziaria. Il risultato è stato un sequestro integrale e indiscriminato del contenuto digitale, comprensivo, con ogni probabilità, di informazioni personali dello stesso giornalista e magari anche di dati relativi a terzi, del tutto estranei alla vicenda.
A fronte di tale situazione, la Corte avrebbe potuto esplicitare che simile operato si pone in tensione con i principi di proporzionalità e adeguatezza della misura cautelare, che divengono ancor più stringenti quando il mez-

e giusto processo, Napoli, 1990, 108; N. Galantini, *Inutilizzabilità della prova e diritto vivente*, in *Rivista italiana di diritto processuale penale*, 2012, 64; O. Mazza, *Il crepuscolo della legalità processuale*, in Id., *Tradimenti di un codice. La Procedura penale a trent'anni dalla grande riforma*, Torino, 2020, 98, ove puntualizza che le regole di procedura sono «scandite da una scala di valori da rispettare, in cima alla quale vi sono le garanzie dell'imputato». Già M. Nobili, *Forme e valori duecento anni dopo*, in Id., *Scenari e trasformazioni del processo penale,* Padova, 1998, sottolineava come ciascuna forma «incarna delle scelte di valore».

[21] Si è riassunto così il fulcro della sentenza, riprendendo il titolo di una recente nota alla medesima pronuncia. V. L. Filippi, *Iuspenale-portale DeJure*, 2 aprile 2025.

[22] *Ibidem*.

zo di ricerca della prova sia destinato a incidere sul segreto giornalistico.
In secondo luogo, una ulteriore criticità concerne il profilo dell'autorità competente a disporre il sequestro.
L'art. 200, c. 3, c.p.p. prevede che la rivelazione della fonte possa essere imposta al giornalista solo dal giudice, previa verifica della ricorrenza delle condizioni eccezionali stabilite dalla norma. Il legislatore ha dunque inteso riservare a un soggetto terzo e imparziale – e non all'organo requirente – il potere di autorizzare una deroga così incisiva alla tutela del segreto professionale. In tale prospettiva, anche il sequestro probatorio che sia finalizzato all'identificazione della fonte deve ritenersi soggetto al medesimo filtro giurisdizionale perché si tratta di un intervento che incide in via sostanziale sul rapporto fiduciario tra giornalista e fonte. Nel caso di specie, tuttavia, la misura risulta disposta dal pubblico ministero, in assenza di autorizzazione giudiziale, con ciò eludendo la procedura di garanzia prevista dall'ordinamento.

Keywords
tutela fonti informative del giornalista – anonimato - interesse all'informazione – funzione del processo penale – sequestro probatorio

Cronache

The Cybersecurity and AI Nexus in the EU Digital Acquis*

Irene Kamara, Marco Bassini

Table of contents

1. Introduction. – 2. AI for cybersecurity in cybersecurity law. – 3. The tripartite dimension of cybersecurity in the AI Act. – 4. Cybersecurity as a fundamental right? Insights from the AI Act. – 5. Conclusion.

1. Introduction

Cybersecurity has been at the core of numerous legislative initiatives of the European Union in the past years. Growing concerns have more recently emerged regarding its specific role within the broader global context shaped by escalating international conflicts. Increasingly, hybrid warfare - where cyber operations are used alongside conventional military tactics - dominates the international security landscape. Calls to develop risk-measured responses that adequately take these risks into account have increasingly emerged[1], including from institutional actors[2]. However, cybersecurity is not merely a key concept in interstate relations, and thus in the international public law domain; rather, it has gained significant momentum from a regulatory perspective in the context of EU digital law through a variety of legal norms applicable to the private sector, as well as to public authorities.

AI systems process large amounts of information, both during inference and model training, which renders them vulnerable to cybersecurity threats and risks. In addition, AI systems rely on software and hardware, which may be open to software vulnerabilities, as well as input manipulation and poisoning attacks[3]. At the same time, AI can be used to generate malware

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

The authors would like to thank Lorenzo Dalla Corte for the feedback to an earlier version of this comment. This work was supported by the European Commission [grant number 101070670 (ENCRYPT)].

1 See for example the discussion on a principle of due diligence in terms of cybersecurity among states: K. Bannelier, *Due diligence as a cardinal principle in the fight against malicious cyber activities*, in A. Segura Serrano (ed.), *Global Cybersecurity and International Law*, London, 2024; A. Coco- T. de Souza Dias, *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law,* in *European Journal of International Law*, 32(3), 2021, 771 ss.

2 B. Buchanan, *The hacker and the state: Cyber attacks and the new normal of geopolitics*, Cambridge (MA), 2020.

3 CEPS, *Artificial Intelligence and Cybersecurity. Technology, Governance, and Policy Challenges*, Final Report, CEPS Task Force, 2021, 55f.

or automate cyberattacks[4]. Yet, AI does not pose a threat to cybersecurity[5]; it may also serve as part of the solution, by improving system robustness, response, and resilience[6]. Machine learning, for example, can detect cybersecurity vulnerabilities[7]. The interaction between the concepts, applications, and uses of AI and cybersecurity is reflected in the recent EU legal instruments, adopted in the area of cybersecurity and artificial intelligence[8]. Therefore, cybersecurity has clearly emerged as a distinct issue, closely linked to - but separate from - data protection, even though the two aspects remain - in the words of the European Data Protection Supervisor Wojciech Wiewiórowski - «two sides of the same coin»[9].

It is not by coincidence that cybersecurity stands out as a key principle in the context of the EU AI regulation, in the AI Act[10] (along with data protection). As well-known, building upon its well-established risk-based approach blueprint, the EU wishes to leverage its role as first-mover compared to other jurisdictions in governing the implementation of AI systems in many respects. As AI systems become increasingly popular, adopted by private and public actors in the performance of business activities but also public services, a key question arises: what is the role of cybersecurity in this domain? While data protection is a well-established fundamental right in the EU legal order and has played a pivotal role in shaping of the EU digital acquis[11] over the past decade, even gaining the status of ethical key requirement for trustworthy AI systems[12], does the Union legislator regard

---

[4] T. Wischmeyer-M. Strecker, *Generative AI and Cybersecurity*, in P. Hacker-A. Engel-S. Hammer-B. Mittelstadt (eds.), *The Oxford Handbook of the Foundations and Regulation of Generative AI,* Oxford, 2025.

[5] T.F. Blauth-O.J. Gstrein-A. Zwitter, *Artificial intelligence crime: An overview of malicious use and abuse of AI*, *IEEE Access*, 10, 2022, 77110 ss.

[6] CEPS, *Artificial Intelligence and Cybersecurity. Technology, Governance, and Policy Challenges*, cit.

[7] A. Calderaro-S. Blumfelde, *Artificial intelligence and EU security: the false promise of digital sovereignty*, in *European Security*, 31(3), 2022, 415 ss.; K. Munonye-M. Péter, *Machine learning approach to vulnerability detection in OAuth 2.0 authentication and authorization flow*, in *International Journal of Information Security*, 21(2), 2022, 223 ss.

[8] H. Junklewitz-R. Hamon-A. André-T. Evas-J. Soler Garrido-J.I. Sanchez Martin, *Cybersecurity of Artificial Intelligence in the AI Act*, Luxembourg, 2023.

[9] W. Wiewiórowski, *Cybersecurity and Data Protection: a necessary and powerful duo*, in *European Data Protection Supervisor*, 28 September 2023

[10] 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).

[11] See the use of art. 16 TFEU as the legal basis for the adoption of a number of EU law acts, such as the AI Act (along with art. 114 TFEU), the Law Enforcement Directive(Directive (UE) 680/2016), the EUDPR Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98.

[12] European Commission, *Ethics guidelines for trustworthy AI*, in *digital-strategy.ec.europa.eu,* 8 April 2019.

cybersecurity to a comparable status? To answer the question above, we take the AI Act as a litmus test for the growing, yet still underdeveloped role of cybersecurity. We do not ask whether cybersecurity is or should be a fundamental right; rather, we ask if the consideration that cybersecurity receives in the AI Act is conducive to an emerging role - or at least an aspiration - of cybersecurity to have a function similar to that of other fundamental rights in shaping EU policy and law making. We discuss, for example, the similarities that can be observed with the overall impact of data protection in EU digital law.

In the end, we aim to determine if the AI Act promotes a trajectory towards recognising cybersecurity as a fundamental right, evaluating this possibility in light of its various possible interpretations and recent developments in EU law.

The analysis is based on doctrinal legal method, with the aim to offer an understanding of the rationales, design, and main role related to cybersecurity in the AI Act and reflect on the main research question of this work. This paper does not aim to draw an exhaustive analysis of the understanding of cybersecurity in the European Union legal order; rather, its goal is to test the growing legal ambitions of this requirement against the most important of the recent developments in the EU digital acquis, namely the AI Act.

The paper begins by analysing the relationship between AI and cybersecurity in the EU cybersecurity law, taking the Network and Information Security Directive 2 ("NIS2 Directive" or "NIS2") and the Cyber Resilience Act ("CRA") as examples, then it will tackle a tripartite dimension of this concept in the AI Act, to assess the extent to which cybersecurity is moving closer to being recognised as a fundamental right that may contribute to shaping future developments in EU law.

2. AI for cybersecurity in cybersecurity law

2.1 Cybersecurity as a regulatory priority in the Union

The 2020 EU's Cybersecurity Strategy for the Digital Decade stressed, among other concerns, that the EU lacks collective situational awareness of cyber threats while many of the critical sectors such as transport, energy, health, and telecommunications depend on network and information security. The Strategy also highlighted that the investigation of almost all crimes involves a digital component and that cybersecurity incidents such as WannaCry ransomware attack have a major impact on the global economy[13]. In the same line, the Europol Internet Organised Crime Assessment 2021 reported an increase in cybercrime-as-a-service, an improvement in the modus-operandi of malware operators, and an overall increase in op-

[13] Joint Communication to the European Parliament and the Council, *The EU's Cybersecurity Strategy for the Digital Decade*, JOIN (2020) 18 final, 16.12.2020.

portunities and sophistication[14]. The sophistication extends beyond technical tools and methods of the attackers, to include other aspects, such as the sentimental value owners bear for their organisations[15], especially in the case of Smaller and Medium Enterprises.

The 2024 Threat Landscape, published by European Cybersecurity Agency ('ENISA') highlights the use of artificial intelligence as an assistant to threat actors, for example for phishing and scripting assistance[16]. Since the adoption of the Network and Information Security Directive (NIS), which was the first EU-wide horizontal cybersecurity law[17], and the 2022 NIS2 Directive[18], the European co-legislators have made cybersecurity a clear priority in policy and law-making. The Cybersecurity Act was published in 2019[19], a regulation for a high level of cybersecurity in EU institutions and agencies was published in 2023[20] and the Cyber Resilience Act was also adopted one year later[21]. Earlier in 2025, the Cyber Solidarity Act was adopted as a Regulation, aiming at strengthening the capacity in the Union to detect, prepare and respond to cyber threats and incidents[22]. These are few of the developments in the field, which further underscore the growing commitment of the EU to develop a comprehensive cyberse-

[14] European Union Agency for Law Enforcement Cooperation, *Internet Organised Crime Threat Assessment (IOCTA) 2021*, Luxembourg, 2021.

[15] L.Y. Connolly-D.S. Wall-M. Lang-B. Oddson, *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability,* in *Journal of Cybersecurity*, 6(1) 2020, tyaa023.

[16] ENISA, *ENISA Threat Landscape 2024,* September 2024.

[17] Markopoulou et al. explain that the EU's interest in cybersecurity was already manifested in 2009 with the Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection *Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security, and resilience* (COM (2009)149). See D. Markopoulou- V. Papakonstantinou-P. De Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, in *Computer Law & Security Review,* 35(6), 2019, 105336 ss.

[18] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.202.

[19] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019.

[20] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, OJ L, 2023/2841, 18.12.2023.

[21] 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) OJ L, 2024/2847, 20.11.2024.

[22] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) OJ L, 2025/38, 15.1.2025.

curity policy and legal framework[23].

ENISA had defined cybersecurity as the «security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace»[24]. Later, the Cyber Security Act provided a definition of cybersecurity as «the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threat»[25]. There are plenty of other definitions on what constitutes cybersecurity[26], the existence of which, demonstrates the complexity of cybersecurity as a research area. The taxonomy proposed by the Joint Research Centre shows for example the different aspects that comprise cybersecurity ranging from sectors such as energy, digital services, platforms to telecoms, banks, and others, to domains such as networked and distributed systems, cryptology, assurance, and to use cases and technologies such as AI, disaster resilience, Internet of Things (IoT), fight against crime, and many others[27].

Independently of the approach one may choose to adopt as regards the concept and regulation of cybersecurity, it is clear that cybersecurity plays a dual role; it is both an accessory regulatory tool, aimed to protect rights, principles, goods, and values, but also constitutes a regulatory target on its own. For example, cybersecurity is an essential means to protect one's online privacy. At the same time, cybersecurity warrants autonomous protection, since cybersecurity breaches may inflict damages on computer systems and data, and in turn result in financial losses or other operational harms. In ransomware cases, where offenders exploit security vulnerabilities and prevent rightsholders such as hospitals or universities from accessing their systems and data, one understands the individual value of cybersecure environments[21].

Before delving into the role of cybersecurity in the AI Act, this work examines how EU cybersecurity law regards AI. The focus is on the Network and Information Security Directive 2 and the Cyber Resilience Act, two of the most impactful cybersecurity legal instruments in EU cybersecurity.

---

[23] At the same time, the EU regulator has acknowledged the complexity of the cybersecurity regulatory environment and the EU digital acquis more generally (including the General Data Protection Regulation and other instruments) and has announced the proposal of amendments aiming at the simplification of obligations and requirements. See European Commission, *A simpler and Portfolio faster Europe: Communication on implementation and simplification*, European Commission 2024-2029.

[24] ENISA *Definition of Cybersecurity Gaps and overlaps in standardisation*, v. 1, 2015, 7, available at *enisa.europa.eu.*

[25] Art. 2(1) Cyber Security Act.

[26] See overview in V. Papakonstantinou, *Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?*, in *Computer Law & Security Review,* 44, 2022, 105653 ss. and in M. Veale-I. Brown, *Cybersecurity*, in *Internet Policy Review,* 9(4), 2020; 1 ss.

[27] I. Nai Fovino-R. Neisse-J. Hernandez Ramos- N. Polemi-G. Ruzzante-M. Figwer- A. Lazari, *A Proposal for a European Cybersecurity Taxonomy,* EUR 29868 EN, Luxembourg, 2019.

2.2 AI as a cybersecurity enhancing technology in NIS2

EU cybersecurity law maintains a technology-neutral approach, but in parallel, acknowledges the possible impact of different AI applications on cybersecurity. Two prominent examples are found in the NIS2 Directive and the Cyber Resilience Act[28]

The NIS2 Directive, which provides cybersecurity risk-management measures and reporting obligations for its regulated entities (essential and important entities) across different sectors[29], invites these entities to evaluate their capabilities and pursue "cybersecurity enhancing technologies", such as AI. Specifically, AI is seen as capable of enhancing the cybersecurity capabilities of essential and important entities, and the security of network and information systems[30].

Further, NIS2 invites Member States to encourage the use of AI for the «detection and prevention of cyberattacks»[31]. Another more nuanced use of AI in the framework of NIS2 concerns the power of Computer Security Incident Response Teams (CSIRTs)[32] to provide «proactive scanning of the network and information systems [...] to detect vulnerabilities with a potential significant impact»[33], which may rely on AI, but not necessarily[34].

2.3 Cybersecurity requirements for high-risk AI systems in the Cyber Resilience Act

The Cyber Resilience Act, which was adopted in parallel with the AI Act, provides, inter alia, «essential cybersecurity requirements for the design, development and production of products with digital elements», as well as «obligations for economic operators in relation to those products with respect to cybersecurity»[35]. The products with digital elements, regulated in the CRA, may sometimes include AI applications (e.g. a smart home appliance, which uses a remote biometric identification system), or be classified

[28] See more in S. Schmitz-Berndt-M.D. Cole, *Towards an efficient and coherent regulatory framework on cybersecurity in the EU: the proposals for a NIS 2.0 directive and a cyber resilience act*, in *Applied Cybersecurity & Internet Governance*, 1(1), 2022, 1 ss.; N. Vandezande, *Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor,* in *Computer Law & Security Review*, 52, 2024, 105890 ss.

[29] Art. 1(2)(b) NIS2 Directive.

[30] Recital 89 NIS2 Directive.

[31] Recital 51 NIS2 Directive.

[32] CSIRTs are designated by Member States and have a range of powers to support inter alia essential and important entities. See further art. 10 NIS2 and I. Kamara-J. van den Boom, *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: Good practices*, National Cybersecurity Centre, 2022.

[33] Art. 11(3)(e) NIS2 Directive.

[34] See ENISA, *Proactive Detection Measures and Information Sources,* 2020, available at *enisa.europea.eu.*

[35] Art. 1(b) CRA.

themselves as AI systems[36].
For those specific systems, to which both the CRA and the AI Act apply, the CRA provides a dedicated provision, clarifying the applicability of the different requirements and aims at harmonising and cutting red tape, where possible. Art. 12 CRA introduces therefore a presumption of compliance with the requirement for cybersecure high-risk AI systems[37]. Products with digital elements, which are also high-risk AI systems, are deemed to comply with art. 15 AI Act, when three cumulative conditions are met: First, the products must fulfil the essential cybersecurity requirements of the CRA. Second, the manufacturer of such products has implemented processes that also comply with the essential cybersecurity requirements of the CRA. And third, the product has successfully passed a conformity assessment procedure and is accompanied by a declaration of conformity[38].
Overall, the analysed cybersecurity legislation identifies the relevance and interdependence of cybersecurity and the diverse uses of artificial intelligence, and a need for harmonisation and alignment of the legal frameworks. At a conceptual level, while EU secondary cybersecurity law elevates the significance of cybersecurity for the digital market, citizens and society -and may support claims that cybersecurity is a collective good[39], serving at times public interests - it does not establish cybersecurity as an individual fundamental right, at least not within the scope of the examined legal instruments[40].

3. The tripartite dimension of cybersecurity in the AI Act

While the AI Act is certainly not a cybersecurity law, the term "cybersecurity" is mentioned more than fifty times. The significance of a cybersecure AI system is stressed throughout the text of the Act.
Recital 76 provides: «Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. [...] To ensure a level of cybersecurity appropriate to the risks, suitable measures, such as security controls, should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure».
As explained in the following sections, the AI Act addresses cybersecuri-

[36] See art. 6(2) and Annex III AI Act. Read further: J. Schuett, *Risk management in the artificial intelligence act*, in *European Journal of Risk Regulation*, 15(2), 2024, 367 ss.

[37] See further analysis of art. 15 AI Act in section 3 of this paper.

[38] Art. 12(1) and art. 43 CRA. An exception to this presumption is established in art. 12(3) CRA for important products with digital elements. See further Annex III CRA.

[39] See similar point made in from M. Kianpour-S.J. Kowalski-H. Øverby, *Advancing the concept of cybersecurity as a public good,* in *Simulation Modelling Practice and Theory,* 116, 2022, 102493 ss.

[40] A.J. Menéndez, *Some elements of a theory of European fundamental rights*, in A.J. Menéndez-E. O. Eriksen (eds.), *Arguing Fundamental Rights,* Dordrecht, 2006, 155 ss.

ty in three dimensions: as a non-functional requirement, as a conformity assessment criterion, and as an organisational measure. These three dimensions are interconnected, as omitting anyone of them would create a gap in the cybersecurity value chain of the AI ecosystem, which includes providers designing and offering AI systems, deployers using the systems, but also entities tasked with monitoring and supervising compliance.

First, cybersecurity is a *non-functional requirement* for high-risk AI systems and general-purpose AI models with a systemic risk. High-risk AI systems must in general fulfil a range of requirements to mitigate risks to health, safety, and fundamental rights[41]. In line with art. 15(1) high-risk AI systems must achieve an «appropriate level of accuracy, robustness, and cybersecurity»[42]. Those essential requirements must be fulfilled during the lifecycle of a high-risk AI system, and thus abide by the principle of security-by-design[43]. To assess whether an AI system meets the appropriate level of cybersecurity, a security risk assessment is necessary, as mandated in art. 9 AI Act. The AI Act also establishes a transparency requirement, according to which the provider of a high-risk AI system must inform the deployer about the level of cybersecurity of the system and any «known and foreseeable circumstances» that may impact this level of cybersecurity[44]. This transparency obligation essentially forces providers to conduct cybersecurity due diligence.

Despite these safeguards, cybersecurity of AI systems and AI-specific technologies face several challenges, both in terms of operational processes (e.g., adapting existing measures for AI software) and research and development challenges (e.g., defining metrics for AI cybersecurity or AI threat modelling)[45]. To assist providers of AI systems with compliance to the cybersecurity requirement for AI systems and address those challenges, the European Commission issued a standardisation request towards CEN and CENELEC to develop European technical standards, inter alia providing good practices and state-of-the-art solutions in the area of AI cybersecurity[46]. Currently, a European harmonised standard is being devel-

41 Recital 66 AI Act.

42 Art. 15(1) AI Act.

43 During the legislative process, the European Parliament had proposed the insertion of the principles of security-by-design and by-default in the text of art. 15(1), which however was not accepted in the negotiations with the Council. The wording in the final text nevertheless still essentially refers to the very meaning of security-by-design, by requiring high-risk AI systems to «be designed» and implement cybersecurity «[...] throughout their lifecycle».
See proposed amendment 321, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

44 Art. 13(3)(b)(ii) AI Act.

45 H. Junklewitz-R. Hamon-A. André-T. Evas-J. Soler Garrido-J.I. Sanchez Martin, *Cybersecurity of Artificial Intelligence in the AI Act*, Luxembourg, 2023, 6.

46 Commission Implementing Decision of 22.5.2023 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence,

oped in response to this request, focusing on organisational and technical solutions aimed at ensuring the cybersecurity of high-risk AI systems over their lifecycle[47]. Additionally, the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) are developing an international standard providing guidance for organisations to address privacy and information security risks in AI systems and machine learning (ML) models[48].

In the case of general-purpose AI models, cybersecurity is a non-functional requirement only for those AI models that present a systemic risk. Providers of such models are obliged to ensure an adequate level of cybersecurity protection for both the model and the physical infrastructure[49]. As noted by Nolte et al., there is a discrepancy between the required level of cybersecurity for high-risk AI systems and general-purpose models in the AI Act[50]; while for the former an *appropriate* level of cybersecurity is required, for the latter only an *adequate* level is sufficient.

The second dimension of cybersecurity in the AI Act concerns *cybersecurity as a criterion in conformity assessment*. Before entering the internal market, high-risk AI systems are required to undergo a conformity assessment procedure, either in the form of internal control or via a specific competent body (notified body)[51]. This *ex-ante* evaluation of high-risk AI systems, inspired by the product safety legislation and the New Legislative Framework ("NLF"), is mandatory for providers of high-risk AI system[52].

While the essential cybersecurity requirement of art. 15(1) for high-risk AI systems, discussed above, concerns a non-functional requirement of the system, cybersecurity as a conformity assessment criterion concerns whether the system meets the pre-determined appropriate level of cybersecurity. The threshold of acceptable cybersecurity level should be determined based on a range of factors, including the intended use of the system, the associated risks, and the state-of-the-art in cybersecurity controls and measures[53].

Third, cybersecurity constitutes a technical and organisational measure for surveillance and other authorities involved in the enforcement of the AI Act[54]. In particular, conformity assessment bodies themselves must adopt

Annex 1, point 8.

47 See *Artificial intelligence - Cybersecurity specifications for AI Systems*, at *cenelec.eu.*

48 ISO/IEC CD 27091 Cybersecurity and Privacy - Artificial Intelligence - Privacy protection.

49 Art. 55(1)(d) AI Act.

50 H. Nolte-M. Rateike-M. Finck, *Robustness and Cybersecurity in the EU Artificial Intelligence Act*, Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25), 2025.

51 Art. 16(f) AI Act. A notified body is defined as «a conformity assessment body notified in accordance with this Regulation and other relevant Union harmonisation legislation» in art. 3(22) AI Act.

52 Read further at *single-market.economy.ec.europea.eu*;. T. de Graaf-G. Veldt, *The AI Act and its impact on product safety, contracts and liability*, in *European Review of Private Law,* 30(5), 2022, 803 ss.

53 See Recital 78 AI Act.

54 Art. 78(2) AI Act.

suitable cybersecurity measures to qualify for notification to the European Commission[55]. Cybersecurity as a technical and organisational measure is not a novel requirement, but a necessary one, for both protecting the models and systems under scrutiny, and establishing trust between regulators and the entities they oversee.

The tripartite framing of cybersecurity in the AI Act certainly shapes it as both a condition of a system and a status, which organisational and technical measures must achieve. The fulfilment of the condition requires normative decisions, from the provider of the system, or standardisation bodies and similar entities, tasked to guide compliance through technical standards and other mechanisms. Those normative decisions largely depend on assessments made by those entities, and have therefore been characterised as value-laden,[56] as they involve choosing which technical solutions better address cybersecurity risks.

4. Cybersecurity as a fundamental right? Insights from the AI Act

To make sense of how cybersecurity is considered in the AI Act, it is worth recalling the ongoing debate on whether cybersecurity constitutes or should constitute a fundamental right[57]. First of all, given the variety of nuances surrounding this concept, we need to determine in which sense we can speak of cybersecurity as a fundamental right.

Cybersecurity has been conceptualised by Papakonstantinou as a *praxis* and as a *state,* whereby the former represents actions and measures and the latter the protected sphere for natural and legal persons[58]. Other scholars frame cybersecurity as a cluster of values, protecting privacy, security, fairness, and accountability[59], or approach cybersecurity by association to the threats against it[60].

Any discussion on the possible role of cybersecurity as a fundamental right could perhaps end with a very old-fashioned and frequently claimed argument in the context of digital policy and regulation: can't we consider cybersecurity as a component of the "general" right to security individuals

[55] Art. 31 AI Act.

[56] M. Veale-F. Zuiderveen Borgesius, *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*, 22(4), 2021, 97 ss.; A. Tartaro, *Value-laden challenges for technical standards supporting regulation in the field of AI,* in *Ethics and Information Technology*, 26(4), 2024, 72; M. Cantero Gamito-C.T. Marsden, *Artificial intelligence co-regulation? The role of standards in the EU AI Act*, in *International Journal of Law and Information Technology*, 32, 2024, eaae011.

[57] Among others, see P.G. Chiara, *Towards a right to cybersecurity in EU law? The challenges ahead,* in *Computer Law & Security Review,* 53 (2024) 105961.

[58] V. Papakonstantinou, *Cybersecurity as praxis and as a state*, cit.

[59] I. van de Poel, *Core values and value conflicts in cybersecurity: beyond privacy versus security,* in *The ethics of cybersecurity*, 2020, 45 ss.

[60] D. Craigen-N. Diakun-Thibault-R. Purse, *Defining cybersecurity,* in *Technology Innovation Management Review*, 4(10), 2014. See also K. Bannelier-T. Christakis, *Cyber-Attacks–Prevention-Reactions: The Role of States and Private Actors,* Paris, 2017, 86.

already enjoy under the existing constitutions and bills of rights? In other terms, wouldn't it simply work as a "cyber" version of the right to security? As far as the EU legal order is concerned, it is already well known that the Court of Justice has provided a negative answer regarding the coverage afforded by art. 6 of the Charter of Fundamental Rights of the European Union. Following the Advocate General's opinion in *La Quadrature du Net I*[61], the Court made it clear that this provision reflects the content of art. 5 of the European Convention of Human Rights, which protects the right to liberty and the right to security; however, the provision aims «to ensure that individuals are protected from arbitrary or unjustified deprivations of liberty» by a public authority[62]; accordingly, art. 6 of the Charter cannot be interpreted «as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offences»[63]. As noted by the Advocate General, the security in question[64] is «personal security, concerned with the conditions under which individuals may have their physical freedom restricted, not the public security inherent in the existence of the State, which is an essential prerequisite in a developed society for reconciling the exercise of public powers with the enjoyment of individual rights»[65]. This interpretation already presents a significant obstacle to deriving a concept of cybersecurity as a fundamental right from the existing provisions, given the variety of nuances by which cybersecurity can be characterised.

At the same time, the fact that cybersecurity may come into play as a requirement playing different roles – as noted above – makes it difficult to effectively capture its nature and circumscribe it to a specific constitutional concept: it equally constitutes a condition for individuals to enjoy their privacy but also other fundamental rights. Therefore, the variety of ways in which cybersecurity operates as a requirement, including in the AI domain, suggests why building cybersecurity upon the existing concept of security would only partially reflect the reach and significance of such notion. This does not mean that constitutions or international (or EU) treaties should necessarily incorporate a new formulation of this requirement for it to be substantively recognized as a fundamental right. In other terms, any discussion focused on the need to revisit the wording of existing provisions to modernize their content would be pointless; rather, the key point lies in whether we can speak of cybersecurity using the same fundamental rights "language" in which concepts such as privacy and data protection are used. Therefore, discussing the fundamental right nature of cybersecurity goes far beyond debating whether existing provisions, given their current wording, suffice to protect it. To understand if such

[61] Opinion of Advocate General Sánchez-Bordona, Joined Cases C-511/18, C-512/18, *La Quadrature du Net et al.* (2020), § 95.

[62] ECJ, Joined Cases C 511/18 Case C 512/18 Case C 520/18, *La Quadrature du Net et al.* (2023), § 125.

[63] *Ibidem*.

[64] More recently, see also the opinion of Advocate General Pikamäe, Case C-118/22 (2023), § 51

[65] Opinion of Advocate General Sánchez-Bordona, Joined Cases C-511/18, C-512/18, cit., § 99.

nature actually emerges in the EU digital law-making, the AI Act constitutes a litmus test to test the ambitions and aspirations of the concept of cybersecurity

As well-known, scholars have defined the AI Act a «medley of product safety legislation and fundamental rights» protection[66]. Concerns for fundamental rights protection received a far from consistent consideration in the legislative process of the AI Act[67], which brought to light the possible varying understanding of AI as a product but also as a source of risks and opportunities alike. While protection of fundamental rights emerged as a pivotal concern before European Parliament, the text eventually voted as result of the Trilogue has commonly been seen as a compromise, and sometimes criticized as an ineffective paradigm[68] which ultimately risk undermining fundamental rights protection. Against these discussions regarding the actual degree of protection that the AI Act offers for fundamental rights, the role of cybersecurity within its broader architecture has to be discussed in light of its tripartite nature as described above. Is it merely a component, albeit important, of product safety legislation or can it aspire to a broader consideration as part of a fundamental right requirement? We conduct this analysis by observing some analogies in the language of a key piece of legislation with a clear fundamental rights-driven nature, like the General Data Protection Regulation ("GDPR")[69].

On one hand, the current wording of art. 15 AI Act resembles to a certain extent that of art. 5 GDPR, by setting forth some basic principles such as accuracy, robustness and cybersecurity. Para. 1 requires high-risk AI systems to be designed and developed in order to meet an appropriate level of these requirements and so that they perform consistently throughout their lifecycle. The wording of this provision also recalls the language of the data protection by design principle as shaped by art. 25 GDPR and, albeit indirectly, that of art. 32 of the GPDR, which requires the adoption of adequate organisational and technical measures in light of the inherent level of risk of the processing activities. However, while the data protection by design seems to lay down a near-universal principle applicable regardless of the level of risk posed by processing activities, art. 15 AI Act is framed as a requirement binding on high-risk AI systems only. This means that the requirement does not apply to AI systems other than high-risk ones, which indirectly reveals that accuracy, robustness and cybersecurity are not mandatory outside the high-risk specific domain,

---

[66] N. Petit-M. Almada, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, Robert Schuman Centre for Advanced Studies Research Paper No. 2023_59; see also see P.G. Chiara, *Understanding the regulatory approach of the Cyber Resilience Act: protection of fundamental rights in disguise?*, in *European Journal of Risk Regulation,* 2025, 1 ss.

[67] F. Palmiotto, *The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation,* in *European Journal of Risk Regulation,* 2025, 1 ss.

[68] M. Almada-A. Radu, *The Brussels side-effect: how the AI Act can reduce the global reach of EU policy*, in *German Law Journal,* 25(4), 2024.

[69] Regulation (UE) 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.

when one considers solely the AI Act. The limited scope of application of these requirements weakens cybersecurity consideration in a fundamental rights fashion. Para. 2 also establishes that the Commission shall define the relevant performance metrics to measure, among other things, the appropriate levels of accuracy and robustness. The remaining provisions set forth in art. 15 are not conducive of a different evaluation. Indeed, they specify the requirement of resilience and impose the adoption of technical and organisational measures for this purpose. In this respect, some convergences can be observed comparing once again the AI Act to the GDPR, most notably to the extent the latter, pursuant to art. 32, requires controllers and processors to «implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk» in light of a variety of factors, namely «the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons». This is not necessarily connected to a fundamental right-based understanding of cybersecurity (which, strictly speaking according to the language of the AI Act, is only one of the three requirements laid down for high-risk AI systems by art. 15); rather, it highlights that, for the purposes of the AI Act, cybersecurity does not merely reflect (nor does it correspond to) the need to ensure an adequate level of data protection. If the principle of data protection by design were enough, the AI Act would not specify the requirements under art. 15, which go beyond compliance with the GDPR principles. This is a more complex and encompassing requirement, which applies regardless of the existence of data processing activities and implies the need of additional safeguards than the ones implemented pursuant to the GDPR. However, while defining such requirement the AI Act seems to employ more the language of product safety legislation rather than that of fundamental rights-driven legislation. So, the language of the AI Act does not support any findings on a supposed nature of cybersecurity as a fundamental right; at the same time, its specific shaping of the risk-based approach leads to considering cybersecurity, together with accuracy and robustness, as a binding set of requirements only when it comes to high-risk AI systems, therefore implicitly downgrading its value as fundamental right. If cybersecurity were to be treated as a requirement stemming from the existence of such a fundamental right, it would be difficult to reconcile this understanding with the limited scope of art. 15 AI Act, which applies only to high-risk AI systems. While the AI Act acknowledges the importance of cybersecurity and incorporates it in the regulation of AI, the regulation does not significantly enhance its value - at least not to the extent that would reflect its recognition as a fundamental right. This should not come as surprise, in the end, given that the AI Act does not posit itself as a piece of legislation that is genuinely driven by the protection of fundamental right.

5. Conclusion

The trajectory drawn in this article illustrates how cybersecurity has evolved into a regulatory priority, becoming a sine qua non requirement for a variety of actors and domains, namely for data-driven systems, critical infrastructures as well as for providers of essential and vital services. The specific developments in EU cybersecurity legislation and the cybersecurity requirement established under the AI Act for high-risk AI systems support this point. With specific regard to art. 15(1) AI Act, one may perhaps claim that this provision inherently incorporates a value-laden requirement[70]. The very same background of the AI Act, which is mostly framed as product safety legislation but with a view to pursuing fundamental rights protection, may pave the way for such construction. However, this provision does not operationalise nor substantiate such a thing as a fundamental right to cybersecurity. This does not prevent scholars from reflecting upon an augmented consideration of cybersecurity in digital policymaking, which will likely remain a pivotal issue in the coming years. But if the AI Act serves as a litmus test to measure the expansion of this concept beyond its well-established consideration, then it ultimately misses the opportunity to elevate cybersecurity to a fundamental rights concern.

[70] See among others A. Tartaro, *Value-laden challenges for technical standards supporting regulation in the field of AI,* cit.; M. Veale, *Value-Laden Areas for Standardisation in the AI Act*, 5 September 2022, at *michae.lv*; M. Cantero Gamito-C.T. Marsden, *Artificial intelligence co-regulation?,* cit.

Abstract

This paper explores the interplay between cybersecurity and artificial intelligence within the European Union's digital legislation. While cybersecurity has been seen as a tool to safeguard data protection, its emerging role suggests a broader regulatory ambition. The analysis investigates whether cybersecurity, as framed in the AI Act, may be transitioning toward a more autonomous legal status, possibly akin to a fundamental right. Through a doctrinal and normative assessment, the paper examines the tripartite role cybersecurity plays in the AI Act—as a non-functional requirement, a criterion for conformity assessment, and an organisational measure. Despite frequent references to cybersecurity and its conceptual proximity to data protection, the AI Act ultimately treats it within the confines of product safety legislation. The findings suggest that although cybersecurity is essential for AI system governance, its recognition as a fundamental right remains aspirational within the current EU legal landscape.

Keywords

artificial intelligence – AI Act – cybersecurity – Cyber Resilience Act – NIS2 Directive

The Legal Challenges of AI Literacy Between Enforcement and Compliance*

Ludovica Paseri, Massimo Durante, Ugo Pagallo

Table of contents

1. Introduction. - 2. The il/literate lawmaker. - 2.1 The US Executive Orders. 2.2 - The EU AI Act. - 3. Soft and hard legal literacy. - 4. Four kinds of legal problem. - 4.1 The development of new standards. - 4.2 Forms of accountability for AI literacy. - 4.3 The effectiveness of soft law policies. - 4.4 The pace of technological innovation. - 4.5 A vicious circle. - 5. Conclusions.

1. Introduction

The normative challenges of Artificial Intelligence (AI), in particular, of what EU lawmakers call "general purpose" AI (GPAI), are increasingly drawing the attention of scholars and institutions[1]. This paper reflects on that part of the legal challenges that concern AI literacy. The notion refers to the ability of individuals and institutions to understand, assess, and interact with AI and GPAI technologies. AI literacy entails multiple cognitive competences of institutions and individuals, taking into account different social roles, such as those of developers and lawmakers, retailers and end-users of the technology. From a normative perspective, AI literacy spans from tracing duties of humans dealing with a meaningful control of AI models and systems to the interpretative skills and capabilities of people interacting with the latest version of Chat GPT. The challenges may concern different problems such as the explainability and transparency of AI, further issues of equity and inclusion, bias and fairness, public education and awareness, people's privacy and data protection, international cooperation and development of standards.

---

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

The research described in this paper is part of the following projects: Project PRIN 2022 EquAI CUP D53D23007280006; and Project PRIN 2022 "Smart Legal Order in DigiTal Society" SLOTS CUP D53D23008070006. Ludovica Paseri authored sections 1, 2, 3, 4, 5; Massimo Durante authored sections 1 and 5; Ugo Pagallo authored sections 1 and 5.

[1] J. Bertomeu – Y. Lin – Y. Liu – Z. Ni, *Capital market consequences of generative ai: Early evidence from the ban of ChatGPT in Italy*, in *SSRN*, 2023, 1 ss.; U. Pagallo, *LLMs meet the law: Who is the sorcerer's apprentice?*, in *Cambridge forum on AI: Law and governance*, 2025, 1 ss.

A robust amount of work has stressed the novelty of the challenges posed in particular by GPAI: an entire chapter of the EU AI Act[2], i.e. Chapter V of Reg. (EU) 2024/1689 aims to tackle such challenges. Further efforts regard China's interim measures for Generative AI in 2023[3], and the sectorial provisions of the White House's Executive Order from October of that year[4], although overruled in January 2025[5]. This normative activism is not by chance. The uniqueness of GPAI entails several legal challenges in addition to issues of bias and fairness, explainability and transparency, cooperation and standards. The use of GPAI models and systems can trigger for example misinformation hazards that affect trust, or that lead to less well-informed users, or to human-computer interaction harms that depend on users overvaluing the capabilities of GPAI, thus using the technology in unsafe ways[6]. In addition, the attention should be drawn to the environmental harms that hinge on the energy power that is necessary to train and operate the technology[7]. GPAI models and systems can also exacerbate traditional normative problems, such as information hazards that impinge on people's privacy by leaking personal information and inferring sensitive data; or discrimination issues that perpetuate social stereotypes and biases, triggering representational and allocational harms; down to GPAI-generated fake news, which are more credible to human raters than human-written disinformation: texts, images, audios, and videos generated by GPAI can be impossible to distinguish from human creation[8].

Against this set of normative challenges, the paper intends to restrict the focus of the lawmakers' response to the challenges of AI literacy. An increasing amount of work deals with the challenges of AI literacy[9]; and yet,

[2] 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, 12.7.2024.

[3] M. Zou – L. Zhang, *Navigating China's regulatory approach to generative artificial intelligence and large language models*, in *Cambridge forum on AI: Law and governance*, 1, 2025, 1 ss.

[4] EO (2023) Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, The White House, October 30, 2023, Washington D.C., USA.

[5] The White House, *Initial rescissions of harmful executive orders and actions*, January 20, 2025, Washington D.C., USA.

[6] L. Weidinger et al., *Ethical and social risks of harm from language models*, in *2021 ACM Conference on fairness, accountability, and transparency*, 2021, 214 ss.; K. Lekadir – G. Quaglio – A. Tselioudis Garmendia – C. Gallin, *Artificial intelligence in healthcare. Applications, risks, and ethical and social impacts*, in *European parliamentary research service,* PE 729.512, 2022.

[7] U. Pagallo – J. Ciani Sciolla – M. Durante, *The environmental challenges of AI in EU law: Lessons learned from the Artificial Intelligence Act (AIA) with its drawbacks*, in *Transforming government: People, process and policy*, 16(3), 2022, 359 ss.

[8] S. J. Nightingale – H. Farid, *AI-synthesized faces are indistinguishable from real faces and more trustworthy*, in *Proceedings of the national academy of sciences*, 119(8), e2120481119, 2022, 1 ss.

[9] There is a wide variety of studies on this point, involving several fields of research, from computer science to the social sciences, such as education and philosophy.

there is still limited research on how current legal systems intend to tackle such challenges with some crucial issues of legal theory[10]. This paper aims to fill this gap, highlighting the challenges of AI literacy by comparing the different US and EU approaches with the analysis of the US Executive Order on AI from 2023, how Trump's White House overruled it in January 2025, down to EU law with the exam of the AI Act, or Reg. (EU) 2024/1689 from July 2024. This perspective sheds light on how the notion of AI literacy is intended in the legal domain to dissect its relevance for practical purposes in both the private and public sectors.

The overall assumption of the paper is that four issues of law enforcement and compliance with legal regulations follow as a result of this inquiry. To substantiate the claim, the paper is divided into three parts that regard: (i) The lawmakers' response to the challenges of AI literacy (Section 2); (ii) The assessment of such a response (Section 3); and, (iii) The open problems of the field with the corresponding issues of legal theory (Section 4). Against the plethora of definitions and issues of AI literacy from an ethical, technological, or political viewpoints, the first step of the analysis is to elucidate the ways in which lawmakers have intended to address the problems of AI literacy, in particular, those posed by uses of GPAI.

2. The il/literate lawmaker

Forms of AI, such as Generative AI, Foundation Models, and Large Language Models (LLMs), broke the news by the end of 2022 and throughout 2023. Benefits and threats of technology ignited people's imagination and drew the regulatory attention of lawmakers and institutions, including the Group of Seven (G7) countries under the Japanese Presidency in May 2023. In addition to the declarations of the G7, the "AI Principles" of the G20, and the initiatives of the Council of Europe[11], national and regional lawmakers soon followed suit, in particular, with the White House's 2023 Executive Order on AI, and the 2024 EU AI Act. A comparative law perspective is fruitful to stress commonalities and divergences of the US and the EU approaches. Both jurisdictions aim to govern the challenges of technology vis-à-vis issues of AI literacy; and however, the Executive Order and the AI Act mirror traditional differences between US and EU law. Although recently overruled, the US 2023 EO is still particularly instructive to grasp crucial differences with the EU approach. The fact

Among the many see J.E. Aoun, *ROBOT-PROOF: Higher education in the age of artificial intelligence*, Cambridge, MA, 2017; D. Long – B. Magerko, *What is AI literacy? Competencies and design considerations*, in *Proceedings of the 2020 CHI conference on human factors in computing systems*, 2020, 1 ss.; Y. Yi, *Establishing the concept of AI literacy*, in *Jahr–European Journal of Bioethics*, 12(2), 2021, 353 ss.; L. Wilton et al., *Where is the AI? AI literacy for educators*, in *International conference on artificial intelligence in education*, Cham, 2022, 180 ss.

[10] K.T. Kotsis, *The scientific literacy enables policymakers to legislate on artificial intelligence*, in *European Journal of Political Science Studies*, 7(1), 2024, 69 ss.

[11] Council of Europe, *Human rights by design future. Proofing human rights protection in the era of AI*, 2023; H. Habuka, *Japan's approach to AI regulation and its impact on the 2023 G7 Presidency*, in *Center for Strategic & International Studies*, 2023, 1 ss.

that the US 2023 EO was rejected since the first week of the new Trump administration makes such differences more crystal clear.

2.1 From Biden to Trump

The differences between EU and US law start with different definitions of technology. The US 2023 EO, for example, defines generative AI (Gen AI) as follows:

> «The class of AI models that emulate the structure and the characteristics of input data in order to generate derived synthetic content» (US 2023 EO's Section 3).

After a three year-long institutional debate, on the other hand, it is worth mentioning that art. 3(1) of the AI Act intends AI as a «machine-based system» that can operate with «varying levels of autonomy» and eventually adapt itself after deployment. Drawing on this basis, the EU definition of GPAI is general enough to include the notion of Gen AI. It goes as follows:

> «An AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market» (art. 3(1)(63) of the AI Act).

Against this framework of technological definitions, we can appreciate the differences of legal approaches. In particular, Biden's 2023 Executive Order unpacked a number of vertical regulations on biosecurity risks and child sexual abuse, patent law and development of standards, consumer law and American civil rights. The AI Act, on the contrary, is a horizontal regulation in the jargon of EU lawyers: the AI Act is in fact an all-encompassing legislation that aims to govern the life cycle of the technology from the first phase of design to the last updates in the market. Whilst Biden's Executive Order mostly regarded public authorities and only indirectly private companies — lest doing business with the federal government — the AI Act affects public and private sectors with a few exceptions for military uses of technology and public order, among others. Although dealing with the same problems of AI literacy and the use of next generation GPAI models, crucial differences between Biden's EO and the AI Act should be emphasized.

In the US, the provisions of Biden's Executive Order that had to do with AI literacy can be divided into three sets. They are related to:

- Human capabilities to assess risks;
- The aim to attain informed oversight; and,

- Recruitment of talent.

Concerning the requirements of AI literacy to assess risks, they can be illustrated with the 2023 EO's Section 2 on policy and principles: letter (d) referred to the AI Risk Management Framework, «in seeking to ensure that AI complies with all Federal laws and to promote robust technical evaluations, careful oversight, engagement with affected communities, and rigorous regulation… Only then can Americans trust AI to advance civil rights, civil liberties, equity, and justice for all».

As regards informed oversight of public actors deploying AI, the EO set up measures to «advance the responsible and secure use of generative AI in the Federal Government» (10.1(d) and (f)). In particular, «agencies are discouraged from imposing broad general bans or blocks on agency use of generative AI». Instead, agencies should have adopted guidelines and limitations on the proper use of GPAI — Generative AI, in the EO jargon — so that they personnel could have had access to secure and reliable GPAI capabilities, «at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans' rights» (lett. (f)(i)).

The third set of provisions related to AI literacy in the 2023 EO concerned «increasing AI talent in Government» (Section 10.2). We should not forget that the US government is by far the largest single buyer of AI technologies in the US economy with over $750 billion in annual spend. According to lett. (d) of Section 10.2, the intent was «to meet the critical hiring need for qualified personnel to execute the initiatives in this order, and to improve Federal hiring practices for AI talent». To attain this goal, on the one hand, it was established the review of the «existing Executive Core Qualifications (ECQs) for Senior Executive Service (SES) positions informed by data and AI literacy competencies» (vii of "d"); on the other hand, a «review of competencies» of civil engineers and related occupations was set up (viii of "d").

All these provisions simply disappeared on 23 January 2025 with the new White House's Executive Order. Its title speaks volumes: *Removing Barriers to American Leadership in Artificial Intelligence*. Section 5 implements the revocation of the previous EO no. 14110 in accordance with the policy of the AI Act. In the phrasing of its Section 2, «the policy of the United States [is] to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security». It will come as no surprise that the US 2025 EO on AI dominance does not refer any longer to risk assessment issues, informed oversight, recruitment of talent, and last but not least, AI literacy. The Assistant to the President for Science and Technology (APST), the Special Advisor for AI and Crypto, and the Assistant to the President for National Security Affairs (APNSA), will determine all actions under Biden's 2023 EO «that are or may be inconsistent with, or present obstacles to, the policy set forth in section 2 of this order» (Section 5 of Trump's 2025 EO on AI).

2.2 The EU approach

The EU AI Act law tackles issues of AI literacy according to four "horizontal" sets of legal provisions. They regard:

- Legal duties of providers and deployers;
- Compliance and enforcement of the Regulation;
- General awareness; and,
- Education.

Art. 3(56) on definitions of the AI Act intends AI literacy as «skills, knowledge and understanding that allow providers, deployers and affected persons… to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI». Art. 4 of the AI Act establishes the measures that providers and deployers of AI systems shall take to «ensure to their best extent a sufficient level of AI literacy» of both their staff and individuals. Providers and deployers should use their AI systems in accordance with such parameters as sound technical knowledge, experience and training, and taking into account the context in which the technology is employed.

As regards compliance and correct enforcement of the AI Act, recital 20 establishes that «AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems» and moreover, that «AI literacy should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement». Informed decisions refer to proper understanding of the technology and interpretation of its outputs as well as the measures to be applied during the use of the technology and, in case of affected persons, the understanding of how AI decisions may impact them.

Further provisions of soft law in the AI Act complement the aim of the EU lawmakers to tackle the challenges of AI literacy. Concerning general awareness in the use of AI, recital 20 of the Regulation refers to «the wide implementation of AI literacy measures and the introduction of appropriate follow-up actions», in particular, the initiatives of the European AI Board under art. 66 of the AI Act. In addition, the Codes of conduct set up in art. 95 should play a key role in promoting AI literacy, «in particular that of persons dealing with the development, operation and use of AI» (art. 95(2)(c)). Recital 165 encourages providers and even deployers of AI systems, in particular of GPAI, to apply additional requirements on literacy «on a voluntary basis».

Specific provisions are finally devoted to the deployment of AI systems in education. In the wording of recital 56, it is «important to promote high-quality digital education and training and to allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes».

Divergences between US and EU law shed light on the multiple ways in which the law can tackle the challenges of AI literacy. From the viewpoint of legal theory, the approach may regard either the soft tools or the hard means of the law, together with different forms of legal governance. Hard

law refers to the rules that aim to directly govern social and individual behaviour hinging on the threat of physical or pecuniary sanctions. Soft law regards guidelines, opinions, and recommendations that, although not legally binding, provide authoritative instructions as to how to interpret or implement the law. Governance concerns the establishment and implementation of policies, procedures, and standards for the proper development, use, and management of AI systems. Variables of legal governance include forms of self-regulation, co-regulation, and strict top-down enforcement of the provisions of hard law[12]. How jurisdictions intend to strike a balance between soft law and hard law with legal variables of technological governance help to further understand differences between legal systems in comparison and competition. The aim of the next section is to explore such differences.

3. Soft and hard legal literacy

We noted above in the previous section that several provisions of the AI Act intend to tackle the challenges of AI literacy through the means of hard law. The attention should be drawn, first of all, to art. 4 of the AI Act on the measures that providers and deployers of AI systems shall take for the AI literacy of their staff and potential parties to a lawsuit. On the one hand, as regards their own staff or team, AI providers should ensure they are capable to perform their tasks and fulfil their obligations; on the other hand, dealing with end-users, or deployers of the technology, the standard is set by that which is necessary to make informed decisions concerning AI and, in particular, the «systemic risk» of GPAI under art. 3(65) of the AI Act. Such informational duties add to what the General Data Protection Regulation, or GDPR (EU) 2016/679[13], establishes for cases of personal data processing. Both provisions converge and may reinforce each other. EU law clarifies that the duty of AI providers, deployers, and data controllers, is to abide by the sets of principles in data protection, such as fairness and transparency under the "accountability principle" of art. 5(1) of the GDPR[14]. Whereas recital 85 of the GDPR refers to accountability

[12] U. Pagallo – P. Casanovas – R. Madelin, *The middle-out approach: Assessing models of legal governance in data protection, artificial intelligence, and the web of data*, in *The theory and practice of legislation*, 7, 2019, 1 ss.

[13] 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), OJ L 119, 4.5.2016.

[14] This aspect is also underlined in EDPS, *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*, 2024, 1 ss., spec. 20, according to which it «is essential that the datasets used to create and train models ensure an adequate and fair representation of the real world - without bias that can increase the potential harm for individuals or collectives not well represented in the training datasets - while also implementing accountability and oversight mechanisms that allow for continuous monitoring to prevent the occurrence of biases that have an effect on individuals, as well as to correct those behaviours». Similarly, see EDPB, *Opinion 28/2024 on certain data protection aspects related*

in connection with responsibility for data breaches and risks for the data subjects' rights and freedoms, art. 5(2) mentions the principle as the way in which data controllers shall be able to demonstrate compliance with the «principles relating to processing of personal data» under art. 5(1)[15]. Such co-regulatory approach fits like hand into glove with the duty of AI providers and deployers of the technology to guarantee appropriate compliance and enforcement of the AI Act through the means of AI literacy (recital 20 of the AI Act).

Mind, this hard approach of EU law does not mean that no US hard law exists for informational duties and tortious claims for AI damage that can be related to issues of literacy[16]. What we mean is that, contrary to the AI Act, even Biden's Executive Order mostly focused on the regulation of administrative agencies and vertical provisions that hinge on the soft tools of the law. Since AI literacy refers to multiple cognitive competences that entail the ability of individuals (and institutions) to understand, assess, and interact with GPAI technologies, this soft approach makes sense because lawmakers can hardly defeat any AI ignorance by decree. The soft law approach to the normative challenges of AI — that we also noted in certain provisions and recitals of the EU regulation, such as art. 66 or art. 95 of the AI Act — materialize through guidelines, opinions, recommendations, and even incentives in both the EU and the US.

However, strict top-down legal governance of AI and GPAI is supplemented through forms of self-regulation or co-regulation with a key difference: whilst a «market-driven approach» prevails or even triumphs in US law[17]; in EU law, the self-regulatory measures that may complement the provisions of hard law often concern forms of supervised (but not enforceable) self-regulation[18]. Consider the voluntary application of specific requirements of the AI Act under the codes of conduct of art. 95. Among the clear objectives and performance indicators that such codes must possess under the encouragement and facilitation of the AI Office and the EU Member States, the attention is drawn to the effectiveness and inclusiveness of the codes (recital 165); the 2019 guidelines of the High-Level Expert Group on the ethical principles of AI (recital 27); and AI literacy (recital 20). Against every form of pure self-regulation, it is up to the European AI Board to take care of the development, application and evaluation of the Codes of conduct (art. 66(e)(i)).

The distinction between soft law and hard law, between variables of self-regulation, co-regulation, or top-down legislation, does not entail any tight separation. Soft law and hard law can supplement each other as much

to the processing of personal data in the context of AI models, 2024, par. 129.

[15] M. Kaminski, *Binary governance: Lessons from the GDPR's approach to algorithmic accountability*, in *Southern California Law Review*, 92, 2019, 1529 ss.; U. Pagallo – P. Casanovas – R. Madelin, *The middle-out approach*, cit., 1 ss., spec. 9-10.

[16] W. Barfield – U. Pagallo, *Advanced introduction to the law and artificial intelligence*, Cheltenham, 2020, 108-121.

[17] A. Bradford, *The Brussels effect: How the European Union rules the world*, Oxford, 2020; Federal Trade Commission, Using artificial intelligence and algorithms, 2020.

[18] C.T. Marsden, *Internet co-regulation and constitutionalism: Towards a more nuanced view*, in *SSRN*, 2020, 1 ss.

as occurs with the primary rules of the law that aim to directly govern individual and social behaviour on AI literacy, and the secondary rules of the law that provide for the organization and functioning of the legal system. This interplay between hard law and soft law, between primary and secondary rules of the law, holds for the notion of appropriate compliance and correct enforcement of top-down regulations, such as those of the AI Act. For example, according to art. 112(7) and recital 174 of the AI Act, the ultimate goal of the voluntary application of specific requirements for other than high-risk AI systems through the formation of the codes of conduct under art. 95 of AI Act is to expand the safeguards of certain high-risk uses of AI with the corresponding set of hard law regulations to the governance and regulation of all AI systems[19]. Despite crucial differences between EU and US law, a similar approach is at work, for example, with the powers and soft law of the Federal Drugs Administration (FDA) in releasing authorizations for the use of AI systems as medical tools in the health sector in US law[20].

Regardless of differences between US and EU law, however, dealing with the challenges of AI literacy, it seems fair to admit that there are some problems open. They concern:

Issues of hard law, such as the enforcement of the top-down provisions of EU lawmakers on AI literacy;

Issues of soft law that regard the alternative of compliance or non-compliance with guidelines and recommendations of institutional authorities; and,

How the interplay between law enforcement and compliance with soft law provisions has to be grasped through governance mechanisms that shall properly tackle the pace of technological innovation.

Such legal drawbacks can be illustrated with the problems of today's institutional efforts to tackle those challenges of AI literacy, such as problems of general awareness, public education or, in the jargon of the overruled US Executive Order, issues of AI compliance «with all Federal laws» as a condition for Americans' trust on AI (the 2023 EO's letter (d) of Section 2). In our view, the problem does not only regard whether strict top-down regulations are effective; whether self-regulatory approaches are good enough; or whether the mix of hard law and soft law through different

[19] This results to the extent that Article 112(7) AI Act specifically provides for the possibility for the European Commission to assess by 2 August 2028, «the impact and effectiveness of voluntary codes of conduct […] for AI systems other than high-risk AI systems and possibly other additional requirements for AI systems other than high-risk AI systems, including as regards environmental sustainability». Accordingly, Recital 174 AI Act underlines that «by 2 August 2028 and every three years thereafter, the Commission should evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements provided for high-risk AI systems in the case of AI systems other than high-risk AI systems and possibly other additional requirements for such AI systems». It seems fair to argue that Art. 112(7) and Recital 174 of the AI Act are an example of the European institutions' quest for a balance between various governance approaches.

[20] Federal Drug Administration, *Artificial Intelligence and Machine Learning (AI/ML)-enabled medical devices*, 2024; U. Pagallo et al., *The underuse of AI in the health sector: Opportunity costs, success stories, risks and recommendations*, in *Health and Technology*, 14, 2024, 1 ss.

forms of technological governance is up to the task. The claim of this paper is that the lawmakers' response to the challenges of AI literacy also entails problems of legal theory as regards, for example, the dichotomy between compliance and no compliance.
The aim of the next section is to elucidate this mix of practical and theoretical problems.

4. Four kinds of legal problem

The paper has discussed so far two forms of regulation (hard law and soft law), and three types of legal governance — i.e. top-down, bottom-up, and co-regulation with their variables — to assess some provisions of EU law on AI literacy with the challenges of GPAI systems and models. Against this framework on legal forms of regulation and types of legal governance, we reckon that four issues are crucially open. They regard: (i) The development of new standards; (ii) Forms of accountability for AI literacy; (iii) The effectiveness of soft law policies; and, (iv) The anticipatory capabilities of the law in tackling the pace of technological innovation.
In addition, a new digital divide could follow as a result of these legal problems with the challenges of AI literacy. Such new forms of digital divide could on the other hand exacerbate the challenges of AI literacy for law enforcement and compliance with legal regulations.
Each of these legal problems is examined separately in the next subsections.

4.1 The development of new standards

The development of new standards plays a crucial role in the AI Act (Section III, Chapter 5 of the Regulation)[21]. However, scholars have paid little attention to the development of new standards for AI literacy as regards the enforcement of the top-down rules of the law.
As thresholds of evaluation for the assessment of the design, functioning and use of technology[22], standards for AI literacy should complement general provisions of the law against damage arising out of strict product and malfunction liability, negligence and breach of warranty, or conformity to a certain standard of conduct. While there is a well-established interpretation and application of the information duties[23], incumbent on data controllers in the case of automated processing of personal data (meaningful information the logic involved must be provided on the basis of arts. 13(2)(f) and 14(2)(g) of the GDPR), it remains to be seen how the information duties imposed by EU law on developers and distributors of GPAI mod-

[21] Likewise for the overruled Executive Order (Section 4 of the EO).

[22] M. Durante, *Computational power: The impact of ICT on law, society, and knowledge*, New York-London, 2021, 23-42.

[23] See EDPB, *Article 29 Working Party - Guidelines on transparency under Regulation 2016/679*, 2018.

els and systems will address AI literacy issues. The uncertainty depends on the role that standards for AI literacy may play in the establishment of new individual rights, and private and public duties related to the development of new technological standards[24]. In addition, such standards are particularly critical as regards either third parties, or end-users of GPAI models that allow to innovate without any gatekeeping[25]. In addition, it will be crucial to examine whether and to what extent the AI governance standards being developed by the international standardisation bodies will impact this scenario[26]. Further problems of standardization are discussed below in the next subsections in connection with the assessment of the soft law initiatives of lawmakers and the pace of technological innovation. Yet, the myriad legal standards related to issues of AI literacy should not lead to overlooking a common threat. Whereas the development of standards should be understood as instrumental to the ability of individuals to grasp, assess, and interact with AI technologies, the opaqueness of the standardization process and the lack of civil society expertise in standard-setting pose serious risks for the rule of law and democracy[27].

4.2 Forms of accountability for AI literacy

A second issue with the lawmakers' response to the challenges of AI literacy has to do with the appropriate compliance and correct enforcement of top-down regulations. Whereas, in EU law, the AI Act has innovated the legal framework through new duties of information and compliance with the obligations that follow the high-risk status of certain uses of AI in Chapter III, and of GPAI in Chapter V of the AI Act, how AI literacy will determine such duties and obligations in addition to the definition of new standards remains an open issue.

In the public sector, the uncertainty depends on the kinds of duty and obligations, if any, that public agencies would have. In the field of contracts and tort law, it is unclear to what extent providers and deployers of AI systems may attempt to turn around some duties and obligations on risk management or data governance through contracts or terms of service, and how burdens of proof for negligence-based liability of private actors

[24] U. Pagallo – J. Ciani Sciolla, *Anatomy of web data scraping: Ethics, standards, and the troubles of the law*, in *European Journal Data Privacy Law & Technology*, 2, 2023, 1 ss.

[25] B. Dickson, *How Open-source LLMs Are Challenging OpenAI, Google, and Microsoft*, 2023.

[26] Consider, for instance, the role of ISO (International Organization for Standardization), IEEE (Institute of Electrical and Electronics Engineers), and BSI (British Standards Institution). Efforts by these standardisation bodies, such as ISO/IEC 42001, the IEEE P7000 series and BSI's PAS, aim to provide best practices for the design, development, deployment and use of AI and could also play a role about AI literacy.

[27] M. Cantero Gamito – C.T. Marsden, *Artificial intelligence co-regulation? The role of standards in the EU AI Act*, in *International Journal of Law and Information Technology*, 32.1, eaae011, 2024, 1 ss.

would work in case of AI illiteracy[28]. Such issues add to tortious liability claims among 27 legal systems in the EU and, except the state of Louisiana, 49 unified tortious legal regimes in the US[29]. Moreover, it remains to be seen whether individuals may claim a right to AI literacy against either private companies or the public administration. Should such a right be protected only indirectly through contracts, terms of service, or tortious liability claims in case of damage, the result could be a vicious circle. We would be bounced back to the issues of contractual responsibility, tortious liability claims, or public agencies' accountability[30] mentioned in this subsection.

4.3 The effectiveness of soft law policies

A third concern with AI literacy regards the notion of compliance. The notion has traditionally been understood as a sort of zero-sum game in the legal domain[31]. Yet, rather than 0s or 1s, either yes or no, focus should be on more subtle assessments that distinguish between ideal, sub-ideal and non-compliant statuses of legal agents[32]; or, between "good", "ok", or "bad" compliance[33]; down to more fine-grained views that distinguish average compliance, reasonably high compliance, very high compliance, and full compliance[34]. The binary alternative of compliance or non-compliance does not provide critical information for the assessment and improvement of those institutional initiatives, such as the codes of conduct of art. 95 in the AI Act, which add to similar provisions and policies of

[28] A thorough analysis of the coordination between the AI Act and the newly adopted Product Liability Directive, i.e. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, in P. Hacker, *The European AI liability directives. Critique of a half-hearted approach and lessons for the future*, in *Computer Law & Security Review* 51, 2023, 1 ss.; and T. Rodríguez de las Heras Ballell, *The revision of the product liability directive: a key piece in the artificial intelligence liability puzzle*, in *ERA Forum*, 24, 2023, 247 ss.

[29] W. Barfield – U. Pagallo, *Advanced introduction to the law and artificial intelligence*, cit., 108-121.

[30] See the recent European Commission, *AI Literacy - Questions & Answers*, 2025. Significantly, one of the frequent questions taken up by the European institutions is specifically related to the assessment of the level of AI literacy as a means of ensuring the accountability of actors. For instance, one of the questions refers to the «minimum content to consider for an AI literacy programme complying with article 4 of the AI Act».

[31] R.V. Stover – D.W. Brown, *Understanding compliance and noncompliance with law: The contributions of utility theory*, in *Social Science Quarterly*, 1975, 363 ss.

[32] R. Lu – S. Sadiq – G. Governatori, *Measurement of compliance distance in business processes*, in *Information Systems Management*, 25(4), 2008, 344 ss.

[33] E. Morrison – A. Ghose – G. Koliadis, *Dealing with imprecise compliance requirements*, in *Proceedings of the 2nd International Workshop on Dynamic and Declarative Business Processes (DDBP 2009)*, Los Alamitos, 2019, 6 ss.

[34] M. Hashmi – P. Casanovas – L. de Koker, *Legal compliance through design: Preliminary results of a literature survey*, in *TERECOM2018@ JURIX, Technologies for Regulatory Compliance*, 2018, 59 ss.

EU law[35], such as legal experimentation by open access in Chapter III of the Digital Governance Act (DGA), i.e. Regulation (EU) 2022/868[36].
We noted that illiteracy remains a problem that does not simply revolve around the top-down enforcement of the tools of hard law, but also, on the success of the promotional side of the law and the aim to foster AI for good[37]. Therefore, the "popularity" of the registration mechanisms for data altruism of the DGA, or the "efficacy" of current policies against the underuse of AI through methods of cooperation — for example, through the sandboxes of art. 57 of the AI Act — should be finetuned between 0 and 1, to determine how much these norms of soft law have been effective in tackling the opportunity costs of technology[38]. Since we stressed that many challenges of AI literacy cannot be tackled through the means of hard law, this lack of more subtle assessments on the effectiveness of soft law policies is critical to improve any legal policy on the drivers of AI illiteracy.

4.4 The pace of technological innovation

A fourth problem with the legal challenges of AI literacy concerns how effective current initiatives of lawmakers will be in coping with the pace of technological innovation. The problem is not only to find forms of accountability for AI literacy, or thresholds for legal enforcement and compliance with new standards. Also, what is at stake concerns how the law intends to intercept the trajectory of technological progress. The paper mentioned activism of US public agencies (although under the Biden administration), as well as future work of such new EU authorities, as the European AI Board, or the AI Office[39].
However, it remains to be seen how effective the soft side of the law can be in promoting AI literacy while catching up with the race of technological progress. We do not have to buy into any argument of those scholars who claim that the race of technology is so determined and powerful

[35] U. Pagallo, *The politics of data in EU Law: Will it succeed?*, in *Digital Society*, 1, 2022, 1 ss.

[36] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022. See L. Paseri, *Scienza aperta: Politiche europee per un nuovo paradigma della ricerca*, Milano-Udine, 2024, 166-170.

[37] M. Taddeo – L. Floridi, *How AI can be a force for good*, in *Science*, *361*.6404, 2018, 751 ss.

[38] U. Pagallo – M. Durante, *The good, the bad, and the invisible with its opportunity costs: Introduction to the 'J' Special Issue on "the Impact of Artificial Intelligence on Law"*, in *J*, 5(1), 2022, 139 ss.

[39] World Economic Forum, *Data Equity: Foundational Concepts for Generative AI: Briefing Paper*, 2023; World Economic Forum, *The Presidio Recommendations on Responsible Generative AI*, 2023; European Commission, *Successful and timely uptake of Artificial Intelligence in science in the EU*, Publication office of the EU, Luxembourg, 2024, 1 ss.; Council of Europe, Human rights by design future. Proofing human rights protection in the era of AI, cit.

that it cannot be deterred by legal means[40], to admit that it is a troubling question whether lawmakers and their normative acts will be good enough in this kind of "cat-and-mouse" game. The development of standards with the alignment of metrics and indexes, for example, does not occur overnight[41]. Today's problems of the law with new forms of accountability for AI literacy and with thresholds of evaluation for compliance with new standards can only make the anticipatory capabilities of every lawmakers' response worse. It is worth mentioning that only two years after the release of the first draft of the AI Act in 2021, the Brussels lawmakers discovered a new world of AI models to be disciplined in addition to the original material scope of the regulation, namely, the set of GPAI models and systems under the lens of this paper.

4.5 A vicious circle

A new digital divide, even harsher than the first wave in the early 2000s[42], could follow as a result of multiple cognitive competences of institutions and individuals affected, in the jargon of EU law, by the «systemic risk» of certain GPAI models and systems. A full array of cases shows users overvaluing the capabilities of GPAI, or using such technology in unsafe ways, or even with malicious purposes or criminal intent[43]. The impact is systemic and spans from developers to lawmakers, consumers and citizens, retailers and end-users. AI illiteracy may depend on previous drivers of social inequality and digital division, such as educational, generational, attitudinal, geographical, or socio-economic factors that add to problems of individuals with physical disabilities, lack of digital training, or infrastructure. However, the uniqueness of AI — and moreover, of GPAI technologies — can bring forth new problems of access, usage, and outcomes, such as data inequalities, algorithmic awareness, misinformation hazards which affect trust, or perpetuation of biases and stereotypes that trigger discrimination and thus, representational and allocational harms.
Lawmakers should be attentive to such new forms of digital divide[44], and how they may exacerbate today's challenges of AI literacy. The multiple cognitive competences involved in how to grasp, assess, and interact with AI technologies regard different epistemic and normative aspects of AI

[40] H. Moravec, *Robot: Mere machine to transcendent mind*, Oxford, 1999; R. Kurzweil, *The singularity is near*, New York, 2005; K. Kelly – J.J. Myers, *What technology wants*, New York, 2010.

[41] U. Pagallo – M. Durante, *The good, the bad, and the invisible with its opportunity costs*, cit.

[42] R. Cullen, *Addressing the digital divide*, in *Online information review*, 25(5), 2001, 311 ss.; J.A.G.M. Van Dijk, *Digital divide research, achievements and shortcomings*, in *Poetics*, 34(4-5), 2006, 221 ss.

[43] See A.M. Barrett et al., *AI risk-management standards profile for general-purpose AI (GPAI) and foundation models*, Centre for Long-Term Cybersecurity, UC Berkeley, 2025, 1 ss.

[44] S. Lythreatis – S. K. Singh – A.N. El-Kassar, *The digital divide: A review and future research agenda*, in *Technological Forecasting and Social Change*, 175, 121359, 2022, 1 ss.

literacy[45]. The epistemic challenges concern the delegation of cognitive tasks and decision-making processes to AI systems that may end up with unjustified actions, opacity, or biases that fall within the loopholes of the law, such as cognitive biases; institutional biases; learning biases; or use biases[46]. The normative challenges of AI literacy have to do with unfair outcomes that pose threats to both human autonomy and social cohesion[47]. We noted that GPAI-generated fake news is often more credible to human raters than human-written disinformation, and that videos generated by GPAI can be impossible to distinguish from human creation[48]. As a result, the problem is not only given by the hallucination of GPAI systems, i.e. the false information they provide about the states of the world. Also, the problem regards individuals who are not capable of understanding they are facing just hallucinations.

New forms of digital divide can only aggravate the four issues of law enforcement and compliance with legal regulation under scrutiny in this paper with the development of new standards; new forms of accountability for AI literacy; the effectiveness of soft law policies; and the anticipatory capabilities of the law in tackling the pace of technological innovation. A vicious circle may follow as a result. In fact, the more AI systems and GPAI models trigger issues of access, usage, and outcomes with a new digital divide[49], the less the law appears effective in addressing literacy problems; and yet, the more the law struggles to address issues of law enforcement and compliance with legal regulations — as suggested in this paper — the more a new digital divide is fated to increase. Although some scholars claim that AI systems can be understood as both the reason and solution of this new digital divide[50], the assumption cannot be reasonably extended to the governance and regulatory problems under scrutiny in this context. After all, it is up to lawmakers the responsibility of how to cope with the pressing problems of the present, and moreover, how to anticipate the challenges of the future.

One of the most relevant challenges of AI literacy has indeed to do with "meta-cognition", i.e. the ways in which the law may aim to anticipate the challenges of an uncertain future through the anticipation capabilities

[45] M. Durante – L. Paseri, *Examining epistemological challenges of Large Language Models in law*, in *Cambridge Forum on AI: Law and Governance*, 1, 2025, 1 ss.

[46] E. Loza de Siles, *AI, on the law of the elephant: Toward understanding artificial intelligence*, in *Buffalo Law Review*, 69, 2021, 1389 ss.

[47] M. Durante – L. Floridi, A *legal principles-based framework for AI liability regulation*, in J. Mökander – M. Ziosi (eds.), *The 2021 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook*, Cham, 2022, 93 ss; U. Pagallo, *Algo-rhythms and the beat of the legal drum*, in *Philosophy and Technology*, 31, 2018, 507 ss.

[48] S. J. Nightingale – H. Farid, *AI-synthesized Faces Are Indistinguishable from Real Faces and More Trustworthy*, cit.

[49] J. Bertomeu – Y. Lin – Y. Liu – Z. Ni, *Capital market consequences of generative AI*, cit.; I. Celik, *Exploring the determinants of artificial intelligence (AI) literacy: Digital divide, computational thinking, cognitive absorption*, in *Telematics and Informatics*, 83, 102026, 2023, 1 ss.

[50] V. Božić, *Artificial intelligence as the reason and the solution of digital divide*, in *Language Education and Technology*, 3.2, 2023, 96 ss.

of AI literacy[51]. This meta-cognitive approach was at work with certain provisions of the overruled US Executive Order, for example, regarding «purposes of experimentation» with Generative AI in Section 10.1 (f)(i). The same holds for the AI Act with «the necessary digital skills and competences, including media literacy, and critical thinking» in recital 56. How to attain these meta-cognitive goals of legislation, however, remains itself an open issue, which brings us back to the dilemmas of hard law, soft law, and governance dissected in this section.

5. Conclusions

An increasing amount of work has been devoted to the analysis of the challenges of AI literacy over the past years. However, there is still few research on the lawmakers' response to these challenges. The paper aimed to fill this gap by examining the ways in which the 2024 EU AI Act has intended to strengthen the ability of individuals and institutions to understand, assess, and interact with GPAI technologies. Focus was on the tools of soft law and hard law with different kinds of legal governance related to both public and private actors. The attention was drawn to the aims to be attained, such as individual autonomy, awareness, or proper understanding of the use of technology, as well as AI literacy as a means of regulation. Lack of AI literacy appears often crucial because it jeopardizes the development of all those sectors — from the digitalization of public administrations to the competitiveness of private companies — which need new skills, abilities, and expertise to deal with the pressing problems of the present and the uncertain challenges of the future.

Four open issues related to law enforcement and compliance with legal rules were under scrutiny. Such problems are related to the development of new standards, the enforcement of hard law rules on AI literacy, the effectiveness of soft law policies, and how to cope with the pace of technological innovation. We stressed that a new digital divide should be expected in case the law is not up to this task. Since legislations are still in their infancy — for example, the AI Act will be at full speed only on 2 August 2026 — it is unclear how provisions on the accountability of both public actors and private companies will be implemented. And yet, on the other hand, such legislations are also affected by conceptual problems, as occurs with traditional notions of legal compliance that do not provide useful information for the assessment of most soft law initiatives on AI literacy.

Issues of AI literacy will thus be increasingly relevant in the legal domain for four reasons:

The speed of technological innovation, in particular, with new GPAI models that may exacerbate the problems with such a time-consuming operation, such as the development of legal standards, their interaction

[51] S.R. Yussen, *The role of metacognition in contemporary theories of cognitive development*, in D. Forrest-Pressley – G. Waller (eds.), *Contemporary Research in Cognition and Metacognition*, Orlando, FL, 1985; R. Miller, *Futures Literacy: transforming the future*, in R. Miller (ed.), *Transforming the future. Anticipation in the 21st century*, London-New York, 2018, 1 ss.

with technical standards, and the overall ability of the law to address the novelties of technology;
The implementation of hard and soft law provisions on AI literacy that in EU law are open to divergent but legitimate interpretations;
The effects of such implementation of hard law and soft law on further regulatory systems in society, such as the AI industry and the market, which add to competitive issues among jurisdictions; and,
Threats of a new digital divide and its interplay with the challenges of AI literacy, which may trigger a vicious circle.
Admittedly, the focus of our analysis could and shall be expanded, for example, by considering further jurisdictions in addition to the response of lawmakers to the challenges of AI literacy in EU law[52]. The aim of this paper, however, was not to be exhaustive, but rather, to explore a *terra incognita* due to the lack of research in the field. We piled up the problems that are open in the legal domain, and suggested why such open problems will increasingly draw the attention of scholars and institutions. By insisting on the pace of AI innovation and the shortcomings of legislative efforts with new risks of digital divide, it seems fair to conclude the bell has rung for everyone.

[52] Council of Europe, *Human rights by design future*, cit.; UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021; World Economic Forum, *Data Equity: Foundational Concepts for Generative AI*, cit.

Abstract

An increasing amount of work is devoted to the challenges of AI literacy. However, there is still limited research on how the law intends to tackle such challenges. The paper aims to fill this gap with the analysis of the AI Act of EU law vis-à-vis the US Executive Orders on AI from 2023 and 2025. Four issues of law enforcement and compliance with legal regulations follow as a result of the analysis. Such issues regard the development of new standards, forms of accountability for AI literacy, the effectiveness of soft law policies, and the anticipatory capabilities of the law in tackling the pace of technological innovation. A new digital divide, even harsher than the first wave of the early 2000s, should be expected if the lawmakers' response to the challenges of AI literacy is not up to the task.

Keywords

AI Act – digital divide – Executive Order on AI – general purpose AI – law enforcement

Navigating the Twin Transition: Digital and Ecological Transformations in the European Union*

Tobia Eugenio Boaro

Table of contents

1. Introduction. – 2. A Theoretical Framework. – 3. Technology as an Enabler of the Ecological Transformation... - 4. … and as a Barrier. – 5. Is Data Literally the "New Oil"? – 6. Policy and Governance of the Twin Transition in the EU. – 7. Circular Economy for a Digital Sustainable Future. – 8. Conclusion and Future Perspectives.

The European Union (EU) is currently navigating a complex but potentially transformative period characterized on one side by the need of ecological sustainability and, on the other side, by the digital revolution's deep impact on society and the economic system as a whole[1].
This period has been named with the term "twin transition"[2] so to emphasize the convergence of the two aforementioned transformations, which present both unprecedented opportunities and significant challenges for EU economic, social, and environmental future, the so called "trilemma"[3].
This paper provides an analysis of the interplay between digital and eco-

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1 European Commission, *Towards a Green & Digital Future*, in *publications.jrc.ec.europa.eu*, 14 March 2025; European Commission, *Fair transition working papers, policy briefs and seminars*, in *employment-social-affairs.ec.europa.eu*, 14 March 2025; European Commission, *Fair green and digital transitions, research*, in *employment-social-affairs.ec.europa.eu*, 24 March 2025; EASSH, *R&I for a Fair Digital Transition, 2024*, in *op.europa.eu*, 14 March 2025; EASSH, *R&I for a Fair Green Transition, 2024*, in *eassh.eu*, 14 March 2024.

2 B. Vermeulen - A. Pyka, *The Twin Digital and green Transition: Paradigm Shift or Tech Fix?*, in *Journal of Innovation Economics & Management*, 3, 2024, 1 ss.; Z. Kovacic - C. Garcia Casanas - H. March, *The twin green and digital transition: High-level policy or science fiction?*, in *journals.sagepub.com*, 14 March 2025; D. Diodato - E. Huergo - P. Monicada Paternò-Castello - F. Rentocchini - B. Timmermans, *Introduction to the special issue on "the twin (digital and green) transition: handling the economic and social challenges"*, in *Industry and Innovation*, 7, 2023, 755 ss.

3 M. Mandelli - S. Sabato - M. Jessuola, *EU Economic Governance and the Socio-Ecological Transition: Towards a More Sustainable European Semester?*, in *Politiche Sociali*, 3, 2021, 619 ss.; S. Sabato - M. Mandelli - M. Jessuola, *Towards an EU eco-social agenda? From Europe 2020 to the European Green Deal*, in M. Schoyen - B. Hvinden - M. D. Leiren (eds.), *Towards Sustainable Welefare States in Europe*, Cheltenham, 2022, 199 ss.

logical transitions within the EU context, exploring the theoretical framework of the two transitions and the role of digital technologies as enablers of ecological sustainability but at the same time as tools with a profound yet often overlooked environmental impact. The further analysis of the EU's policy framework will be crucial to show its implications for economic competitiveness, social equity, and the realization of a just transition.

1. Introduction

The need to address ecological challenges, most notably climate change, carbon dioxide emissions and fossil fuels, is crucial nowadays and felt as an imperative by many people[4]. This need coexists with the digital revolution's deep impact on everyday life, society and the economic system in every part of the world, taking the shapes of a real global shift[5].
As regards the EU, these two transformative forces are increasingly recognized not as independent, but as deeply intertwined and mutually influential. This is why they are more and more frequently referred to as the "twin transition"[6].
The EU is playing a crucial role in this transition, setting ambitious goals for both ecological sustainability and digital fairness. The main example of this is the European Green Deal (EGD), an initiative aimed at achieving zero net emissions of greenhouse gases by 2050[7], but the Digital Decade is also important as it seeks to ensure EU digital leadership through citizens and businesses' empowerment[8].
The basic assumption of these initiatives is that digital technologies can act as key enablers for achieving sustainability and reducing the environmental impact of numerous economic sectors, helping them to transition towards a circular economy[9].
However, the synergy between digital and ecological transitions is not automatic since it can lead to trade-offs and negative externalities, as is the case with the environmental footprint of digital infrastructures, AI and data centres[10].
From all these facts, it can be easily deduced that careful and future-proofed policy considerations are fundamental, and delving into the theoretical

[4] S. Lange - L. Denick, *Digital Reset. Redirecting Technologies for the Deep Sustainability Transformation*, Berlin, 2022.

[5] *Ibid.*

[6] B. Vermeulen - A. Pyka, *The Twin Digital and green Transition*, cit., 1 ss.; Z. Kovacic - C. Garcia Casanas - H. March, *The twin green and digital transition*, cit.; D. Diodato - E. Huergo - P. Monicada Paternò-Castello - F. Rentocchini - B. Timmermans, *Introduction to the special issue on "the twin (digital and green) transition"*, cit., 755 ss.

[7] European Commission, *The European Green Deal*, in *commission.europa.eu*, 24 March 2025.

[8] European Commission, *Europe's Digital Decade*, in *digital-strategy.ec.europa.eu*, 24 March 2025.

[9] M. Draghi, *The Future of European competitiveness. Part A*, in *commission.europa.eu*, 24 March 2025.

[10] *Ibid.*

framework regarding the twin transition must be the starting point of this analysis.

2. A Theoretical Framework

Understanding the twin transition requires adopting various points of view. To this end, the so called "Multi-Level Perspective" (MLP) provides a valuable framework for analyzing how digital technologies can challenge and potentially transform the dominant fossil-based regime[11]. MLP is able to highlight the interplay between technological progress, established socio-economic regimes, and external pressures in driving systemic change.
In this context, the concept of digital sustainability has emerged to address the relationship between digital technologies and sustainability goals[12]. More specifically, digital sustainability encompasses two dimensions: on one side, Green Information Systems (Green IS), that is the design and implementation of technologies that contribute to sustainable business processes; on the other side, Green Information Technologies (Green IT), mainly focused on energy and equipment utilization, including data centres' energy consumption, electronic waste, and devices' manufacturing carbon footprint[13].
While some scholars have emphasized the potential for a mutually reinforcing process where digitalization and sustainability transformations accelerate each other[14], other scholars have battled against the so called "digital solutionism", regarded as an overly optimistic view of digital technologies as default solutions to sustainability challenges, calling for a critical assessment of their material impact and potential unintended consequences[15].
In particular, Adi Kuntsman and Imogen Rattle, researchers respectively at the University of Manchester and at the University of Leeds, have proposed a «paradigmatic shift in sustainability studies» aimed at de-biasing current literature and embracing a more pragmatic and policy-oriented approach towards the twin transition[16].

---

[11] K. Vestkioja - R-M. Soe - E. Kisel*, Implications of digitalization in facilitating socio-technical energy transitions in Europe*, in *Energy Research & Social Science*, 91, 2022, 2 ss.; D. Loorbach - N. Frantzeskaki - F. Avelino*, Sustainability Transitions Research: Transofrming Science and Practice for Societal Change*, in *Annual Review of Environment and Resources*, 42, 2017, 599 ss.

[12] F. De Felice - A. Petrillo, *Green Transition: The Frontier of the Digicircular Economy Evidenced from a Systematic Literature Review*, in *mdpi.com*, 14 March 2025; A. Travassos Rosario - J. Carmo Dias, *Sustainability and the Digital Transition: A Literature Review*, in *mdpi.com*, 14 March 2025.

[13] T. Lynn - P. Rosati - D. Kreps - K. Conboy, *Digital Sustainability: Key definitions and Concepts*, in T. Lynn - P. Rosati - D. Kreps - K. Conboy (eds.), *Digital Sustainability. Leveraging Digital technology to Combat climate Change*, London, 2024, 1 ss.

[14] *Ibid.*

[15] A. Kuntsman - I. Rattle, *Towards a Paradigmatic Shift in Sustainability Studies: A Systematic Review of Peer Reviewed Literature and Future Agenda Setting to Consider Environmental (Un) sustainability of Digital Communication*, in *Environmental Communication*, 5, 2019, 567 ss.

[16] *Ibid.*

Other contributions have focused on applying the so called "Deep Transitions" (DT) framework, proposed by Johan Shot and Laur Kanger from the University of Sussex[17], on twin transition's studies, advocating for a radical and systemic turn embracing not just new technologies, but individuals, institutions and society as a whole.
These contributions have helped showing, through a historical point of view, that technological transitions tend to be faster than energy ones, implying a potential imbalance in the twin transition that necessitates proactive policy interventions to ensure that the decarbonization agenda, as set out by the EGD, keeps pace with the ever-changing digital sector[18].
In this context, a fundamental role is played by Mario Draghi's recent Report on European competitiveness, which lays out clear and multifaceted recommendations on how Europe should boost its economic growth trough innovation, technology and AI[19]. The Report focuses on both technology as an enabler and as a barrier of the ecological transformation, and so does this paper in the following paragraphs.

3. Technology as an Enabler of the Ecological Transformation…

EU intervention on the twin transition crosses various sectors and policy domains. In general, digitalization is envisioned as a key enabler for enhancing resource efficiency and promoting economic circularity[20].
For instance, digital product passports are being explored as means to improve businesses' transparency and accountability by providing consumers with accessible and comprehensive information about product lifecycles, material composition, and repair possibilities[21].
In the energy sector, the application of smart technologies together with users' nudge towards responsible energy consumption are central to the reduction of fossil fuels' usage[22]. The digitalization of the Estonian electricity sector serves as a guiding example of this, highlighting the benefits for both businesses and consumers[23].
Undoubtedly, realizing interoperable, Europe-wide energy data access requires standardized data protection laws among Member States, robust

[17] J. Schot - L. Kanger, *Deep Transitions: Emergence, Acceleration, Stabilization and Directionality*, in *papers.ssrn.com*, 14 March 2025.

[18] R. Fouquet - R. Hippe, *Twin transitions of decarbonisation and digitalisation: A historical perspective on energy and information in European economies*, in *Energy Research & Social Science*, 91, 2022.

[19] M. Draghi, *The Future of European competitiveness. Part A*, cit.

[20] *Ibid.*

[21] European Data, *EU's Digital Product Passport: Advancing transparency and sustainability*, in *data.europa.eu*, 14 March 2025.

[22] K. Vestkioja - R-M. Soe - E. Kisel, *Implications of digitalization in facilitating socio-technical energy transitions in Europe*, cit., 8 ss.

[23] *Ibid.*

consent management, and adequate transparency[24]. These are all essential elements to foster users' environmental awareness and to make green energy services' uptake scalable.

Artificial Intelligence (AI) and big data analytics, on their part, play a crucial role in the twin transition, since they can improve Environmental, Social, and Governance (ESG) reporting quality by streamlining businesses' data collection, enhancing in this way the collection of large volumes of data[25].

Starting from AI, it is identified as a General Purpose Technology (GPT) with a potentially systemic impact on firms' eco-innovation[26]. AI has the potential to optimize the use of natural resources, improve energy efficiency in buildings and transport, support the management of smart energy grids, predict and mitigate the impacts of climate change, and promote the design of more sustainable products and processes[27]. It can also be employed for environmental monitoring and simulations, emissions' data analysis, and promoting the circular economy through optimization of material flows and waste reduction[28].

Beyond operational optimization, AI also addresses one of the core challenges in environmental decision-making, that is the limitations of the precautionary principle[29]. While traditionally used to justify regulatory caution in the face of uncertainty, this principle often leads to economically inefficient outcomes, prohibiting or heavily regulating specific activities. AI, through its ability to perform probabilistic modeling and scenario analysis, provides an alternative decision framework that balances environmental risks with innovation potential[30]. This helps regulators and businesses to move beyond risk-aversion and the classical one-size-fits-all approach, towards an adaptive, evidence-based environmental governance.

Big data analytics further enhances this landscape by enabling the identi-

---

[24] European Parliament, *The impact of EU legislation in the area off digital and green transition, particularly on SMEs*, in *europarl.europa.eu*, 14 March 2025; M. Baumgart - B. Espinosa Apáez, *On the implementation of smart meters in the European Union: Legal considerations regarding privacy and personal data protection in times of the Twin Transitions*, in R. Leal-Arcas (ed.), *Research Handbook on EU Energy Law and Policy*, Cheltenham, 2024, 500 ss.; B. Garske - W. Holz - F. Ekardt, *Digital twins in sustainable transition: exploring the role of EU data governance*, in *frontiersin.org*, 14 March 2025.

[25] KPMG, *ESG in the age of AI*, in *assets.kpmg.com*, 17 March 2025.

[26] OECD, *AI Compute & Climate Change*, in *oecd.ai*, 17 March 2025; R. Nishant - M. Kennedy - J. Corbett, *Artificial intelligence for sustainability: Challanges, opportunities, and research agenda*, in *International Journal of Information Management*, 53, 2020, 1 ss.

[27] K. Vieth-Ditlmann, *Sustainable AI: a contradiction in terms?*, in *algorithmwatch.org*, 24 March 2025; European Parliament, *AI for Sustainability – A Human-centric Approach to Global Challenges*, in *futurium.eu.europa.eu*, 17 march 2025.

[28] World Economic Forum, *9 ways AI is helping tackle climate change*, in *weforum.org*, 24 March 2025.

[29] G. Muto, *Is it possibile to go beyond the precautionary principle in climate change policy-making? AI as a tool for efficient decisions*, in *medialaws.eu*, 30 May 2025; R. B. Stewart, *Environmental regulatory decisions making under uncertainty*, in *Research in Law and Economics*, 20, 2002, 71 ss.; C. R. Sunstein, *Beyond the precautionary principle*, in *University of Pennsylvania Law Review*, 3, 2003, 1003 ss.

[30] G. Muto, *Is it possibile to go beyond the precautionary principle*, cit.

fication of patterns and inefficiencies across vast datasets. In the energy domain, for instance, this can provide valuable insights for understanding consumption patterns, identifying inefficiencies, optimizing production and distribution, and monitoring pollution[31].

When integrated with geospatial and climate data, big data analytics also supports more precise environmental planning, from urban mobility to natural disaster resilience[32]. It enables real-time analysis of urbanization, air quality, land use and population dynamics, supporting the design of low-emission cities[33]. In disaster risk management, it improves forecasting of extreme weather events like floods and heatwaves, informing early warning systems and emergency preparedness strategies[34]. Additionally, such data-driven insights can guide post-disaster reconstruction by identifying the most resilient design strategies and the most affected zones[35]. Big data also aids in biodiversity conservation and greenhouse gas emissions' tracking, ensuring better compliance with climate goals both at the local and national scale[36].

It is important to highlight that, in its decision-making, big data analytics can incorporate not only economic but also social dimensions, thus facilitating a more holistic approach to sustainability[37]. This is particularly valuable as environmental issues often show complex trade-offs, that span different areas and catalyze strong partisan divisions[38]. Higher levels of trust, transparency and public engagement can also be achieved thanks to a broader access to data, benefiting not just researchers but society as a whole[39]. Citizens, NGOs and local communities can use this information to hold authorities accountable, contribute to local knowledge, and collaborate on sustainable intervention with a multistakeholder approach.

Besides AI and big data analytics, other emerging technologies, like Internet of Things (IoT) and blockchain, must be assessed for the purpose of this paper. IoT enables the collection of real-time data from a wide range of devices and sensors, providing a key tool for environmental monitoring, energy management, optimization of industrial processes, and imple-

---

[31] OECD, *Understanding and Applying the Precautionary Principle in the Energy Transition*, in *oecd.org*, 30 May 2025.

[32] UN Environmental Programme, *Can big data help protect the planet?*, in *unep.org*, 30 May 2025.

[33] E. Aloitaibi - N. Nassif, *Artificial intelligence in environmental monitoring: in-depth analysis*, in *Discover Artificial Intelligence*, 4, 2024, 1 ss.

[34] A. McGovern - R. J. Chase - M. Flora - D. Gagne - R. Lagerquist - C. K. Potvin - N. Snook - E. Loken, *A Review of Machine Learning for Convective Weather*, in *Artificial Intelligence for the Earth Systems*, 2, 2023, 1 ss.

[35] M. Yu - C. Yang - Y. Li, *Big Data in Natural Disaster Management: A Review*, in *Geosciences*, 5, 2018, 1 ss.

[36] UN Environmental Programme, *Can big data help protect the planet?*, cit.

[37] R. Dubey - A. Gunasekaran - S. J. Childe - T. Papadopoulos - S. Z. Luo - S. F. Wamba - D. Roubaud, *Can Big Data and Predictive Analytics Improve Social and Environmental Sustainability?*, in *Technological Forecasting and Social Change*, 1, 2017, 1 ss.

[38] D. Caldwell - G. Cohen - N. Vivyan, *Long-run trends in partisan polarization of climate policy-relevant attitudes across countries*, in *tandfonline.com*, 30 May 2025.

[39] OECD, *We need to use AI to right climate change*, in *oecd.ai*, 30 May 2025.

mentation of sustainable mobility solutions inside the so called "smart cities"[40].
Blockchain technologies, thanks to their decentralization and distribution, can ensure transparency and traceability in sustainable supply chains, facilitate peer-to-peer renewable energy trading and eliminate the need for inefficient intermediaries[41].

4. … and as a Barrier

Despite these potential transformative forces, the EU must address significant challenges and critical issues regarding digital technologies. The environmental footprint of digitalization is, in fact, substantial and growing proportionally with the energy demands of data centers, AI, and cloud computing[42].
Some scholars have even shown that specific technologies, that are cloud computers, data centres and blockchain miners, are potentially more detrimental than beneficial to the twin transition since they need large amounts of energy and water to cool the infrastructures[43]. In addition, data centres' greenhouse gas emissions are very high and they occupy vast areas of land, potentially damaging the surrounding biodiversity and landscape[44].
This highlights the need for evidence-based policies and for a constant and close dialogue between academia and institutions, focusing on both the benefits and the potential negative effects of digitalization.
But the negative effects of digitalization are not limited to energy and water consumption, greenhouse gases, and land use. Digital devices' supply chain, in fact, is based on raw materials, some of which are scarce or extracted with significant environmental and social impacts[45]. Furthermore, electronic devices' rapid obsolescence generates a growing volume of waste, posing significant challenges for recycling and hazardous materials' management[46].
It is therefore evident, in the trilemma between fiscal stability, ecological transition and strategic autonomy, that the twin transition has profound implications for the labor market and for social equity, too. While digitalization can enhance productivity and create new opportunities, it also

[40] F. A. Almalki - S. H. Alsamhi - R. Sahal - J. Hassan - A. Hawbani - N. S. Rajput - A. Saif - J. Morgan - J. Breslin, *Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities*, in *Mobile Networks and Applications*, 28, 2021, 178 ss.

[41] G. B. Bhavana - R. Anand, *Applications of blockchain technology in peer-to-peer energy markets and green hydrogen supply chains: a topical review*, in *Scientific Reports*, 14, 2024, 1 ss.

[42] S. Garsia, *The environmental costs of AI: a shake-up of the EU's twin transition*, in *law.kuleuven.be*, 24 March 2025.

[43] M. O'Brien - H. Fingerhut, *Artificial intelligence technology behind ChatGPT was built in Iowa – with a lot of water*, in *apnews.com*, 24 March 2025; S. Gonzalez Monserrate, *The Staggering Ecological Impacts of Computation and the Cloud*, in *thereader.mitpress.mit.edu*, 24 March 2025.

[44] J. Roundy, *Assess the environmental impact of data centers*, in *techtarget.com*, 24 March 2025.

[45] *Ibid.*

[46] S. Gonzalez Monserrate, *The Staggering Ecological Impacts of Computation and the Cloud*, cit.

poses risks of automation and job displacement[47].
Ensuring a just transition necessitates proactive policies focused on education, digital skills' development, and social welfare systems to support workers in adapting to a changing labour market and reducing social inequalities.
Alongside these policies, policy-makers must obviously focus also on mitigating the environmental impact of digitalization, promoting digital infrastructures' energy efficiency, sustainable materials' use, durable and repairable products' design, and effective recycling and reuse systems, with a comprehensive and data-driven approach[48].

5. Is data *literally* the "new oil"?

Data represent a cornerstone for both the digital and ecological transitions[49]. The availability of high-quality, granular, and accessible data is crucial for the development of smart energy services, accurate environmental monitoring, and rigorous scientific research[50].
The granularity of energy data has been identified as a barrier for more detailed data-driven analysis, limiting models' precision and the ability to provide effective real-time services[51]. Various types of energy data, including energy source, price data, and contractual information, are essential for accurate calculations, behavioral suggestions, and optimized management of energy consumption and production.
The accessibility and interoperability of data are crucial to fully leverage the potential of digital technologies in support of sustainability. The creation of online platforms and sandboxes for sharing environmental and energy data can surely facilitate the cooperation among policy-makers and improve transparency[52].
In this regard, AI, data centres and blockchain' environmental impact must not be overlooked, so not to turn into reality the famous expression

[47] Eurofound, *Employment impact of digitalisation*, in *eurofund.europa.eu*, 24 March 2025; A. M. Santos - J. Barbero - S. Salotti - A. Conte, *Job creation and destruction in the digital age: Assessing heterogeneous effects across European Union countries*, in *Economic Modelling*, 126, 2023, 1 ss.

[48] B. Vermeulen - A. Pyka, *The Twin Digital and green Transition*, cit., 1 ss.; Z. Kovacic - C. Garcia Casanas - H. March, *The twin green and digital transition*, cit.; D. Diodato - E. Huergo - P. Monicada Paternò-Castello - F. Rentocchini - B. Timmermans, *Introduction to the special issue on "the twin (digital and green) transition"*, cit., 755 ss.

[49] European Parliament, *The impact of EU legislation in the area off digital and green transition*, cit.; M. Baumgart - B. Espinosa Apáez, *On the implementation of smart meters in the European Union*, cit., 500 ss.; B. Garske - W. Holz - F. Ekardt, *Digital twins in sustainable transition*, cit.

[50] Team, *The benefits of high-frequency granular data in sustainability reporting*, in *teamenergy.com*, 24 March 2025; A. Davé - P. Ball - K. Salonitis, *Factory Eco-Efficiency Modelling: Data Granularity and Performance Indicators*, in *Procedia Manufacturing*, 8, 2017, 479 ss.

[51] *Ibid.*

[52] W. Min Kwok, *Sandboxing and experimenting digital technologies for sustainable development*, in *researchgate.net*, 24 March 2025; A. Attrey - M. Lesher - C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, Paris, 2020.

«data is the new oil»[53] and to make data de facto comparable to fossil fuels' impact.

6. Policy and Governance of the Twin Transition in the EU

The EU has established a comprehensive set of policies and regulatory instruments to steer the twin transition and to ensure digital sustainability among all Member States.

The EGD provides the overarching framework for achieving climate neutrality and environmental sustainability, explicitly recognizing the driving role of digital technologies[54]. The National Energy and Climate Plans (NECPs), introduced by Regulation (EU) 2018/1999, outline how Member States intend to address the five dimensions of the energy union, among which are decarbonisation and energy efficiency[55]. Initiatives like the Digital Education Action Plan aim, for their part, to enhance digital literacy and to promote digital ecosystems' use in education[56].

Recent and more detailed regulations include the Digital Services Act (DSA) and the Digital Markets Act (DMA) that, while primarily focused on citizens' rights protection, digital fairness and competition, also have implications for sustainability. For instance, the emphasis on responsible design and online interfaces in art. 25 DSA can indirectly contribute to more sustainable consumption patterns among consumers[57]. The reference made by arts. 34-35 DSA to systemic risks' mitigation by Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), the so called gatekeepers, could, in addition, require platforms to reduce their environmental impact[58].

Another recent EU regulation, the AI Act, includes several provisions to address the potential risks associated with AI technologies, fostering transparency and accessibility. Researchers, notably Zuzanna Warso and Kris Shrishak, have described these measures as «limited and inadequate … to reduce the environmental impact of AI systems»[59]. The adoption of codes of conduct and standards could, however, fill these loopholes thanks to a co-regulatory approach, involving all the stakeholders and con-

[53] European Parliament, *Is data the new oil? Competition issues in the digital economy*, in *europarl.europa.eu*, 24 March 2025.

[54] European Commission, *The European Green Deal*, in *commission.europa.eu*, 24 March 2025.

[55] European Commission, *National energy and climate plans*, in *commission.europa.eu*, 24 March 2025.

[56] European Commission, *Digital Education Action Plan (2021-2027)*, in *education.ec.europa.eu*, 24 March 2025.

[57] European Commission, *The Digital Services Act package*, in *digital-strategy.ec.europa.eu*, 26 March 2025.

[58] R. Griffin, *Climate Breakdown as a Systemic Risk in the Digital Services Act*, in *hertie-school.org*, 24 March 2025.

[59] Z. Warso - K. Shrishak, *Hope: The AI Act's Approach to Address the Environmental Impact of AI*, in *techpolicy.press*, 26 March 2025.

sumer organisations[60].

Data governance, standardization, interoperability, and cybersecurity are critical enablers of the ecological transformation[61]. This is why, in addition to the DSA, DMA and AI Act, the EU has developed a strong framework for data governance by introducing the Data Act, whose aim is to foster data ecosystems' environmental monitoring, resource management, and the development of circular economy solutions[62]. Challenges still remain in ensuring secure and ethical data access and sharing, while complying with privacy obligations.

Another important initiative in the EU context is the European Semester, EU's framework for economic policy coordination, as it is increasingly incorporating environmental sustainability considerations[63]. Integrating social policy deeper into the European Semester could further enhance the focus on a just transition.

Financial instruments and funding programs, such as Horizon Europe, are also crucial for supporting research and innovation in areas relevant to the twin transition[64], while the Eco Design Directive, despite dating back to 2009, still plays a central role in driving digital and ecological transitions towards a common goal[65].

The Eco Design Directive, in particular, encourages manufacturers to improve products' environmental performance throughout their lifecycle, focusing on aspects such as energy efficiency, durability, recyclability, and reducing hazardous substances' use. Additional directives and initiatives, such as the Energy Labelling Directive, the European Union Ecolabel and the Design for Sustainability (D4S) Standards[66], can be followed by responsible manufacturers to complement the Eco Design Directive.

For fit-for-purpose businesses, the Corporate Sustainability Reporting Directive (CSRD) plays a crucial role, as it enhances corporate transparency and accountability regarding sustainability matters[67]. Business are required to report detailed ESG information and reports must be standardized and verified by an independent auditor, as well as prepared in a machine-readable format. This makes it possible for information to be granular, accessible, and reusable for the aims of a data-driven EU environmental governance.

Lastly, the Corporate Sustainability Due Diligence Directive (CSDDD) is

---

[60] M. Cantero Gamito - C. T. Marsden, *Artificial intelligence co-regulation? The role of standards in the EU AI Act*, in *International Journal of Law and Inforamtion Technology*, 1, 2024, 1 ss.

[61] European Parliament, *The impact of EU legislation in the area off digital and green transition*, cit.; M. Baumgart – B. Espinosa Apáez, *On the implementation of smart meters in the European Union*, cit., 500 ss.; B. Garske - W. Holz - F. Ekardt, *Digital twins in sustainable transition*, cit.

[62] European Commission, *Data Act*, in *digital-strategy.ec.europa.eu*, 26 March 2025.

[63] European Commission, *The European Semester*, in *commission.europa.eu*, 26 March 2025.

[64] European Commission, *Horizon Europe*, in *research-and-innovation.ec.europa.eu*, 26 March 2025.

[65] European Commission, *Ecodesign and Energy Labelling*, in *single-market-economy.ec.europa.eu*, 26 March 2025.

[66] *Ibid.*

[67] European Commission, *Corporate sustainability reporting*, in *finance.ec.europa.eu*, 31 May 2025.

aimed at fostering sustainable and responsible corporate behaviour across companies' value chains, including the digital ones, specifically requiring large companies to publish regular reports on the social and environmental risks they face[68].

7. Circular Economy for a Digital Sustainable Future

Not considering the recent debates on CSDDD probable future delay or modification and the EU Commission apparent deregulatory shift[69], it is without any doubt that circular economy represents a prime example of the synergistic potential of the twin transition, and this justifies a focus on it in this paragraph[70].

In compliance with the aforementioned EU directives and initiatives, digital technologies can surely play an important role in shifting from a «take-make-dispose» model to a more sustainable system of «reuse, repair, recycle, and regeneration»[71].

Firstly, data analytics and AI can inform eco-design by providing insights into product lifecycles, supply chains and material flows, facilitating the design of products that are more durable, repairable, and recyclable[72].

Combined with Iot and big data, AI can improve resource management in manufacturing processes, optimize logistics, and enhance the transparency and sustainability of supply chains. AI and IoT can also optimize waste collection and sorting processes, increasing recycling rates and reducing landfill waste[73].

As mentioned above, digital product passports can provide comprehensive and easy-to-read information about a product's origin, composition, and lifecycle, enabling better tracking, reuse, and recycling[74].

However, realizing the full potential of digitalization for the circular economy requires addressing challenges such as the lack of interoperable solu-

[68] European Commission, *Corporate sustainability due diligence*, in *commission.europa.eu*, 26 March 2025.

[69] A. Alemanno, *The Dark Side of EU Deregulation*, in *project-syndacate.org*, 26 march 2025; H. Ruschemeier, *The De-Regulatory Turn of the EU Commission*, in *verfassungsblog.de*, 26 March 2025.

[70] B. Vermeulen - A. Pyka, *The Twin Digital and Green Transition*, cit., 1 ss.; Z. Kovacic - C. Garcia Casanas - H. March, *The twin green and digital transition*, cit.; D. Diodato - E. Huergo - P. Monicada Paternò-Castello - F. Rentocchini - B. Timmermans, *Introduction to the special issue on "the twin (digital and green) transition: handling the economic and social challenges"*, cit., 755 ss.

[71] M. Antikainen - T. Uusitalo - P. Kivikyto-Reponen, *Digitalisation as an Enabler of Circular Economy*, in *Procedia CIRP*, 73, 2018, 45 ss.

[72] OECD, *AI Compute & Climate Change*, cit.; R. Nishant - M. Kennedy - J. Corbett, *Artificial intelligence for sustainability*, cit., 1 ss.; World Economic Forum, *9 ways AI is helping tackle climate change*, cit.

[73] *Ibid.*

[74] European Data, *EU's Digital Product Passport*, cit.

tions and the need for standardized data protocols[75]. Furthermore, business models need to evolve to incentivize circular practices and overcome existing obstacles to ecological transition in various sectors, starting from the clothing one.
E-commerce and B2C platforms, such as ASOS, Zalando, Vinted, are extremely popular among EU consumers, helping them to connect with repair services, facilitating second-hand markets and extending product lifespans[76]. However, unsustainable manufacturing practices, low-quality textiles and poor working conditions are often associated with these businesses, making their regulation particularly challenging in light of their transnational structure[77].

8. Conclusion and Future Perspectives

The twin transition represents a pivotal moment for the EU. While the vision of a synergistic relationship between digitalization and ecological sustainability holds big promise, its realization requires a multidimensional effort, as exemplified by the EGD and the Draghi Report[78].
This paper has highlighted the various ways in which digital technologies can drive and contribute to the ecological transition, from enabling smart energy systems and promoting the circular economy to enhancing ESG reporting and fostering eco-innovation.
However, it has also been underscored the critical need to address the digital sector's inherent environmental impact and to proactively overcome its barriers, by managing the profound social and economic consequences of the ecological transformation[79].
Robust methodologies and policy frameworks must be developed to assess the environmental impact of digital technologies across various sectors and to ensure their responsible deployment for sustainability, including data governance, interoperability standards, and incentives for circular business models[80].
In addition to this, investments in research must be made to promote sustainable economic principles within the ICT sector across all Member States[81]. Interdisciplinary approaches must be adopted, integrating not just economic, environmental and technological perspectives on the twin transition, but also the social one.
A holistic and multifaceted understanding of the twin transition, by combining twin and just transitions together, guarantees a wide range of ben-

[75] M. Antikainen - T. Uusitalo - P. Kivikyto-Reponen, *Digitalisation as an Enabler of Circular Economy*, cit., 45 ss.

[76] UN, *E-commerce and environmental sustainability*, in *un-ilibrary.org*, 28 March 2025.

[77] *Ibid.*

[78] M. Draghi, *The Future of European competitiveness. Part A*, cit.

[79] M. Mandelli - S. Sabato - M. Jessuola, *EU Economic Governance and the Socio-Ecological Transition*, cit., 619 ss.

[80] *Ibid.*

[81] M. Draghi, *The Future of European competitiveness. Part A*, cit.

efits for economy and society as a whole[82]. To this end, investments in education, skills development, and social safety nets are crucial to mitigate potential negative impacts on the labor market and to ensure social equity. By acknowledging these complexities and proactively addressing them, the EU can harness the transformative power of the twin transition to forge a more sustainable, competitive, and equitable future for all its citizens and to contribute to global efforts in addressing the urgent environmental challenges of our time.

Europe must not stifle new emerging ideas, but it must promote them and create a truly common and competitive market, securing strategic independence and enhancing its geopolitical influence. «Thus - with the words of Mario Draghi - we will build a strong and cohesive Europe, because each of its states is strong only if it is together with the others and only if it is cohesive within itself»[83].

[82] S. Sabato - M. Mandelli - M. Jessuola, *Towards an EU eco-social agenda?*, cit., 199 ss.; S. Lange - L. Denick, *Digital Reset*, cit.

[83] Words have been extracted and translated by the author from Draghi's audition at the italian Camera dei Deputati on 18 March 2025, see Camera dei Deputati, *Competitività europea, audizione Draghi*, in *comunicazione.camera.it*, 28 March 2025.

Abstract

This paper explores the European Union's strategic approach to the digital and ecological transitions, so called twin transition, as a key to ensuring long-term sustainability, competitiveness, and social equity. It shows the theoretical framework of the transition and subsequently analyzes how digital technologies, such as Artificial Intelligence and big data analytics, can act as powerful enablers of ecological sustainability. At the same time, the paper addresses the environmental and social costs associated with digital infrastructures, emphasizing the importance of specific regulatory frameworks to advance towards a more cohesive and resilient future. Environmental and digital laws are analized, focusing on the European Green Deal, Digital Services Act, Digital Markets Act, Corporate Sustainability Reporting Directive and other relevant initiatives. This makes it possible to understand how the EU can shift from a "take-make-dispose" model to a circular economy, solving the so called trilemma. De iure condendo, future perspectives are presented and assessed on the basis of the Draghi Report.

Keywords

twin transition – sustainability – digitalization - Artificial Intelligence - circular economy

Data protection e immigrazione irregolare: quali tutele (in)esistenti?*

Filomena Pisconti

Sommario

1. Intelligenza artificiale nel quadro di "criminalizzazione" delle migrazioni. La tutela delle persone vulnerabili e il processo di "colpevolizzazione" del migrante. – 2. Uno sguardo ai principali strumenti di IA nel quadro della finalità di gestione del fenomeno migratorio. Un confronto Italia-Europa, tra lesione dei diritti fondamentali e "nuove" misure di prevenzione. – 3. Il nuovo Patto sulla migrazione e l'asilo e l'influenza dell'IA sui diritti umani digitali. – 4. Diritti umani digitali e protezione delle frontiere. Quali tutele (in)esistenti?

1. Intelligenza artificiale nel quadro di "criminalizzazione" delle migrazioni. La tutela delle persone vulnerabili e il processo di "colpevolizzazione" del migrante

Le procedure utilizzate nella gestione della migrazione, dell'asilo e del controllo delle frontiere hanno inevitabilmente effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile[1], che subiscono la natura discriminatoria dei sistemi di IA utilizzati in tali contesti[2].
Il mancato equilibrio degli interessi in gioco, tra diritti individuali e sicurezza pubblica, stimola un approfondimento sulla possibilità di attuare

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

[1] Sui concetti di migrazioni e vulnerabilità cfr. M. G. Giammarinaro, *L'individuazione precoce delle vulnerabilità alla tratta nel contesto dei flussi migratori misti*, in *Questione giustizia*, 2, 2018, 129 ss.; AA. VV., *Migrazioni e vulnerabilità. La rotta del Mediterraneo centrale. Atti del II° Doctoral Colloquium dell'Accademia Diritto e migrazioni. Macerata, 5-6 dicembre 2019*, in L. Salvadego-M. Savino-E. Scotti (a cura di), Torino, 2021; M. Catanzariti, *Rischio e vulnerabilità nel modello europeo di intelligenza artificiale*, in *Società, Mutamento, Politica, Rivista Italiana di Sociologia,* 13, 2022, 73 ss.; S. Corradi, *Comprendere la vulnerabilità. Pluralismo ontologico e sistemi di intelligenza artificiale nel diritto,* in *BioLaw Journal-Rivista di Biodiritto*, 1, 2024, 5 ss.

[2] Cfr. C. Johnson-al., *Interventions on the state of sovereignty at the border*, in *Political Geography*, 59, 2017, 1 ss.; M. Longo, *The politics of borders: Sovereignty, security, and the citizen after* 9/11, Cambridge, 2017; A. Szwed, *The use of artificial intelligence in migration-related procedures in the European Union – opportunities and threats. The use of artificial intelligence in migration-related pro,* in *Procedia Computer Science*, vol. 207, 2022, 3639 ss.; H. Beirens, *Reboting the Asylum System? The role of digital tools in international protection*, in *Migration Policy institute,* 2022; M. Forti, *AI-driven migration management procedures: fundamental rights issues and regulatory answers*, in *BioLaw Journal-Rivista di Biodiritto*, 2, 2021, 433 ss.

«forme di sorveglianza di massa e di profilazione delle persone»[3], con un evidente rischio di compressione dei diritti fondamentali, convenzionalmente e costituzionalmente garantiti della personalità.
La domanda che sorge spontanea in questo quadro conflittuale è la seguente: l'IA può contribuire in quel processo di criminalizzazione del migrante che permea in maniera costante la legislazione attuale di settore?
La sorveglianza algoritmica è spesso invisibile, automatizzata e impersonale, e rende difficile per l'interessato capire quando e perché viene osservato o classificato.
Nella famosa sentenza pronunciata il 6 ottobre 2020 dalla Grande Sezione della Corte di giustizia dell'Unione europea nel caso C-511/18 – La Quadrature du Net e altri, la Corte sottolineava come la sorveglianza di massa non può diventare la regola, nemmeno per ragioni di sicurezza.
La Corte ha stabilito che la conservazione indiscriminata e preventiva dei dati è incompatibile con il diritto dell'Unione, in quanto vìola i principi fondamentali della proporzionalità, del diritto alla vita privata e della protezione dei dati personali, sanciti dalla Carta dei diritti fondamentali. Solo in presenza di una minaccia grave, reale e attuale alla sicurezza nazionale, può essere autorizzata una conservazione temporanea e sottoposta a rigorosi controlli da parte di un'autorità indipendente o giudiziaria.
Nel caso di specie, diverse organizzazioni (come La Quadrature du Net in Francia) avevano impugnato leggi nazionali che obbligavano i fornitori di servizi Internet a conservare in modo generalizzato e indiscriminato dati di traffico e di localizzazione, anche in tempo reale. Queste misure - introdotte in nome della sicurezza nazionale e della lotta al terrorismo - permettevano, dunque, l'accesso preventivo a grandi quantità di dati delle comunicazioni personali.
Nell'occasione la Corte ha avuto modo di sottolineare come l'intervento preventivo deve essere legale, necessario e proporzionato, senza mai trasformarsi in una sorveglianza indiscriminata che tratta tutti i cittadini come sospetti. La conservazione generale e indiscriminata dei dati degli utenti dei servizi Internet e di telecomunicazione non è, dunque, conforme agli artt. 7 e 8 della Carta dell'UE, fatta eccezione per casi particolari strettamente necessari alla tutela della sicurezza nazionale.
Anche nella lotta contro il terrorismo, lo Stato di diritto non può cedere a logiche di controllo massivo, ma deve sempre garantire un equilibrio tra sicurezza e libertà.
Il dato personale ha un'importanza rilevante nella società attuale ed è un elemento imprescindibile per la corretta affermazione della propria identità individuale: l'obiettivo della normativa di settore di ogni livello, infatti, è quello di evitare qualsiasi tipo di abuso da parte del titolare del trattamento e le finalità di interesse e sicurezza nazionale perseguite non possono giu-

[3] Espressioni riprese da M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali alla luce delle dinamiche di relazione tra poteri pubblici, imprese e cittadini*, in *Sistema penale*, 9, 2022, 23 ss. Cfr., anche, su questi temi D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002; G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015; G. Mobilio, *Tecnologie di riconoscimento facciale, rischi per i diritti fondamentali e sfide regolative*, Napoli, 2021; F. Mollo, *Sorveglianza di massa, rispetto della vita privata e trattamento di categorie particolari di dati nel quadro multilivello di tutela della persona,* in *Federalismi.it*, 26 luglio 2023.

stificare unlimitess interferenze nella sfera privata del singolo individuo.
Nel caso dei migranti, il bilanciamento diventa ancora più critico e complesso: le persone in movimento sono spesso prive di strumenti legali e tecnologici per comprendere o contestare decisioni dei sistemi di IA.
L'utilizzo di sistemi algoritmici, spesso associati ai big data, ha interessato, infatti, anche il settore dell'immigrazione, trovando applicazione, ad esempio, nell'attività di controllo delle frontiere nazionali, nella gestione delle prime fasi di contatto tra i migranti e le autorità nazionali, in relazione alla formalizzazione e valutazione delle domande di protezione internazionale.
Il controllo dei flussi migratori alle frontiere statali rappresenta un ambito nel quale la complessità dell'equilibrio tra diritti individuali e tutela della sicurezza pubblica è destinata a esprimersi in modo paradigmatico.
Il Centro Hermes per la Trasparenza e i Diritti Umani Digitali nel 2021[4] si interrogava sul funzionamento e sullo scopo delle innovazioni in campo tecnologico applicate alle migrazioni, analizzandole non solo da un punto di vista tecnico ma anche attraverso la lente dei diritti umani digitali.
La ricerca denunciava come vi fosse un processo di "criminalizzazione della persona migrante, rifugiata o richiedente asilo" nell'infrastruttura tecnologica italiana, come i migranti "barattassero" i dati personali e biometrici in cambio di accoglienza e informazioni per proseguire il loro viaggio e come il riconoscimento facciale usato in Italia nelle attività di indagine rischiasse di avere conseguenze molto gravi su migranti e richiedenti asilo, per l'assenza di valutazioni pubbliche sull'accuratezza degli algoritmi impiegati nel sistema di riconoscimento facciale in dotazione alla polizia.
Per quanto riguarda il primo aspetto, la ricerca evidenziava come i dati biometrici raccolti al momento dello sbarco o dell'arrivo sul territorio nazionale sono inclusi in un database che contiene potenziali sospettati ed è utilizzato per ritrovare corrispondenze di volti e identità attraverso il sistema di riconoscimento facciale: la "criminalizzazione" dei sospettati avviene, dunque, senza la possibilità che la società civile possa conoscere esattamente il numero di persone fotosegnalate per ogni categoria prevista dalla legge, e quindi in modo incontrollabile e opaco.
Riguardo al secondo aspetto, a migranti, rifugiati e richiedenti asilo viene negata la possibilità di fornire un consenso informato, configurandosi una vera e propria asimmetria informativa.
Infine, la mancata corretta supervisione degli algoritmi impiegati potrebbe comportare casi di falso positivo che porterebbero alla violazione dei diritti umani di gruppi vulnerabili.
Il tratto comune dei risultati della ricerca è che il controllo dei flussi migratori, in ogni settore, è esercitato attraverso un potere (quasi sempre) coercitivo e in maniera discriminatoria, che distingue tra persone e "non-persone".
Il concetto di "criminalizzazione" utilizzato dal Centro ricerca rievoca delle riflessioni che riguardano la scienza penalistica di settore dal contenuto criminogeno, che cerca di soddisfare la necessità spasmodica di rassicurare "a tutti i costi" la collettività: il processo di "securitarizzazione" del fenomeno migratorio ha prodotto la traslocazione del fenomeno nel settore

[4] Cfr. *Tecnologie per il controllo delle frontiere in Italia identificazione, riconoscimento facciale e finanziamenti europei*, in *protecht.hermescenter.org,* aprile 2022.

della sicurezza[5] e, dunque, del diritto penale.
L'accanimento punitivo verso il fenomeno migratorio è, infatti, retto principalmente da una impropria e strumentale applicazione del labelling approach secondo cui il "deviante", ossia «colui che si oppone all'ordine sociale», che «non è conforme alle aspettative della società riguardo al ruolo che dovrebbe essere svolto dall'individuo» coinciderebbe con lo straniero[6].
Il labelling approach costituisce tratto distintivo di un diritto della sicurezza, alimentato da una anima esasperatamente preventiva, che «divora tutti i principi dello Stato di diritto»[7].
L'inaccettabilità di un simile paradigma impone inevitabilmente la necessità di individuare un "freno d'emergenza", in particolar modo nei "nuovi" campi in cui tale esigenza si fa sempre più effettiva.
La "criminalizzazione" che avviene nelle operazioni di raccolta dei dati biometrici al momento dello sbarco o dell'arrivo sul territorio nazionale si spiega in ragione del fatto che la società civile non è in grado di conoscere esattamente il numero di persone fotosegnalate per ogni tipo previsto dalla legge, e quindi si tratta di una raccolta che si svolge in modo incontrollato e non del tutto trasparente.
Tale forma di criminalizzazione preventiva avviene senza la commissione di un reato di una decisione giudiziaria, ma attribuisce allo straniero una identità digitale da tracciale e conservare, in assenza della quasi totalità di protezione.
Il fatto che oggi i migranti siano indicati "tipi" pericolosi e che «si utilizzi ogni strumento disponibile per tentare di tenerli fuori dai confini fisici e giuridici delle democrazie occidentali»[8] è un dato costante di una certa letteratura scientifica, che va dagli studi giuridici e sociologici sulla crim-

[5] G. Campesi definisce la "securitarizzazione" come quel «processo di costruzione sociale mediante il quale un determinato fenomeno viene progressivamente attratto nella sfera dei problemi e delle questioni relative alla sicurezza». L'Autore distingue tre differenti paradigmi di questo processo relativo alla migrazione: il primo definisce la migrazione come un pericolo per l'ordine pubblico e la sicurezza dello Stato, il secondo come una minaccia di natura prevalentemente politico-identitaria, mentre il terzo come minaccia di natura socioeconomica. Cfr. Id., *Immigrazione: da questione sociale a minaccia per la sicurezza,* in *ISPI - Commentary*, 22 ottobre 2013; Id., *Migrazioni, sicurezza, confini nella teoria sociale contemporanea,* in *Studi sulla Questione criminale*, 2, 2012; A. Cavaliere, *Diritto penale e politica dell'immigrazion*e, in F. Rocchi-E. Rosi (a cura di), *Immigrazione illegale e diritto penale. Un approccio interdisciplinare*, Napoli, 2013; L. Risicato, *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?* Torino, 2019: F. Forzati, *La sicurezza penale fra rassicurazione sociale, conservatio ordinum e criminalizzazione del corpo estraneo*, in *Archivio penale,* 3, 2018, 1 ss.

[6] Sulla teoria del *labelling approach* e le migrazioni, cfr. G. Alesci, (*In-) Sicurezza e immigrazione La "colpevolizzazione" dello straniero nel diritto dell'emergenza*, in *Archivio penale*, 3, 2018, 1 ss.; M. Ruotolo, *Crimmigration: un processo marcatamente politico e mediatico*, in *Iusinitenere*, 8 aprile 2022.

[7] Cfr. M. Donini, *La robusta tradizione del diritto penale della sicurezza: illustrazione con intento critico,* in M. Donini-M. Pavarini (a cura di), *Sicurezza e diritto penale,* Bologna, 2011, 79 ss.

[8] Cfr. R. Cornelli, *La politica della paura tra insicurezza urbana e terrorismo globale,* in *DisCrimen*, 18 luglio 2018, 257.

migration[9] o sulla border criminology[10], fino agli studi che predicano la natura penale della detenzione degli stranieri nascosta dietro un'etichetta amministrativa[11].

Le procedure di identificazione allo sbarco o all'arrivo su suolo italiano sono ormai sempre più automatizzate e invasive e non sempre si fondano su una legittima base giuridica, contrariamente a quanto affermato nella recente giurisprudenza della Corte europea dei Diritti dell'Uomo in materia di divieto di trattamenti inumani e degradanti (art 3 CEDU) e di divieto di espulsioni collettive (Protocollo 4, art. 4, CEDU)[12], secondo cui è necessario che l'utilizzo di tali tecnologie, rispetto a persone che si trovano in una condizione di particolare vulnerabilità, richieda una adeguata base normativa e una corrispondente valutazione del possibile impatto in termini di rispetto dei diritti fondamentali.

In tal senso, da più parti si afferma l'esigenza di condizionare l'applicazione di sistemi autonomi basati sull'intelligenza artificiale almeno a «una procedura di human rights impact assessment, al fine di verificare se il loro utilizzo nella gestione dei flussi migratori non finisca con il pregiudicare i diritti dei migranti e dei richiedenti protezione internazionale», e, dunque, al fine di condurre una valutazione ex ante degli effetti potenzialmente lesivi dei diritti umani[13].

---

[9] Cfr. J. Stumpf*, The Crimmigration Crisis: Immigrants, Crime, and Sovereign Power,* in *American University Law Review*, vol. 56, 2, 2006, 367 ss.; per una revisione aggiornata del concetto, con particolare riferimento alla situazione italiana, cfr. A. Spena, *La crimmigration e l'espulsione dello straniero-massa,* in *Materiali per una storia della cultura giuridica*, 47(2), 2017, 495 ss.; G. L. Gatta, *La pena nell'era della "crimmigration": tra Europa e Stati Uniti*, in *Rivista Italiana di diritto e procedura penale,* 2018, 675 ss.

[10] Cfr. ad es. M. Bosworth, *Border Criminologies: How migration is changing criminal justice*, in M. Bosworth-C. Hoyle-L. Zedner (eds.), *Changing Contours of Criminal Justice,* Oxford, 2016, 213 ss.; S. Pickering-M. Bosworth-K. Franko Aas, *The Criminology of Mobility*, in S. Pickering-J. Ham (eds.), London-New York, 2015, 382 ss.

[11] M. Bosworth, *Immigration Detention, Punishment and the Transformation of Justice*, in *Social & Legal Studies,* vol. 28, 1, 2019, 81 ss.; Id., *Inside Immigration Detention*, Oxford, 2014; A. Pugiotto, *La "galera amministrativa" degli stranieri e le sue incostituzionali metamorfosi,* in *Quaderni Costituzionali,* 3, 2024, 573 ss.; G. Campesi-G. Fabini, *La detenzione della "pericolosità migrante"*, in *Materiali per una storia della cultura giuridica*, 47(2), 2017, 515 ss.; M. Pelissero, *Il vagabondo oltre confine. Lo statuto penale dell'immigrato irregolare nello Stato di prevenzione*, in M. Meccarelli-P.Palchetti-C. Sotis (a cura di), *Ius peregrinandi. Il fenomeno migratorio tra diritti fondamentali, esercizio della sovranità e dinamiche di esclusione*, Macerata, 2012, 35 ss.

[12] Cfr., in particolare, CEDU, *Ase of M.H. and Others v. Croatia*, ric. 15670/18 e 43115/18 (2022).

[13] Cfr. S. Penasa, *Migrazioni e intelligenza artificiale: nuovi percorsi di ricerca,* in *ADiM Blog - Analisi & Opinioni*, Dicembre 2021. Sul *human rights impact assessment* cfr. D. Kemp-F., Vanclay, *Human rights and impact assessment: clarifying the connections in practice*, in *Impact Assessment and Project Appraisal*, 31, 86 ss.; A. Beduschi, *International migration management in the age of artificial intelligence*, in *Migration Studies*, 9, 2020, 583 ss.; M. Forti, *AI-driven migration management procedures: fundamental rights issues and regulatory answers,* in *BioLaw Journal-Rivista di BioDiritto*, 2, 2021, 442 ss.

2. Uno sguardo ai principali strumenti di IA nel quadro della finalità di gestione del fenomeno migratorio. Un confronto Italia-Europa, tra lesione dei diritti fondamentali e "nuove" misure di prevenzione

Attualmente tra le tecnologie più invasive che utilizzano l'IA si annoverano il riconoscimento facciale biometrico e i sistemi di polizia predittiva.
Il riconoscimento facciale è un sistema di IA in grado di identificare le persone sulla base di caratteristiche fisiche o comportamentali, grazie al quale i soggetti possono essere, dunque, tracciati attraverso l'utilizzo dei propri dati biometrici.
I sistemi di polizia predittiva sono, invece, strumenti di sorveglianza di massa che utilizzano algoritmi in grado di prevedere, in termini statistici, la probabilità che venga commesso un reato e da chi possa essere stato commesso.
In Italia viene utilizzato il sistema di riconoscimento facciale denominato SARI (Sistema automatico di riconoscimento immagini) la cui funzione Real time è stata di recente ritenuta illegittima dal Garante per la protezione dei dati personali perché priva di un'adeguata base legale. Al riguardo, il Garante ha stigmatizzato i rischi derivanti da una simile tecnologia, capace di attuare delle vere e proprie forme di sorveglianza di massa[14]: l'utilizzo di un tale sistema potrebbe implicare ripetute violazioni e non a caso attualmente le TFR (Tecnologie di riconoscimento facciale) sono incluse tra i sistemi di intelligenza artificiale ad alto rischio, il cui utilizzo va adeguatamente limitato o, in alcuni casi, addirittura escluso[15].
Attualmente, il sistema SARI è utilizzato nella sola funzione da remoto, denominata Enterprise, che consente l'identificazione di un soggetto ignoto a partire da un'immagine fotografica.
Mediante una ricerca computerizzata nella banca dati AFIS, e grazie a due algoritmi di riconoscimento facciale, SARI Enterprise fornisce un elenco di immagini ordinato secondo un grado di similarità; a sua volta, la banca dati AFIS (Automated Fingerprint Identification System) rappresenta il sistema automatizzato di acquisizione delle impronte digitali, di cui fa parte il Sotto Sistema Anagrafico (SSA), che contiene, invece, le foto segnaletiche presenti nei database della polizia, insieme alle informazioni fisiche delle persone ritratte.
La conservazione e il trattamento di dati sensibili non potrebbero essere differenziati in ragione della nazionalità, così come la raccolta di dati biometrici, anche se dovesse ritenersi effettuata per finalità di polizia o per interesse pubblico, dovrebbe essere regolata da leggi o da regolamenti che ne disciplinino il trattamento alla luce della specifica funzione perseguita e che tutelino i diritti dei titolari.
L'inserimento in banca dati di polizia avviene in via di fatto, in assenza di un espresso e motivato atto normativo, per il solo fatto di appartenere a

[14] Cfr. M. Colacurci, *Riconoscimento facciale e rischi per i diritti fondamentali,* cit., 26.

[15] Cfr. A. Orlando, *La regolamentazione delle tecnologie di riconoscimento facciale nell'UE e negli USA: alea IActa est?* in *DPCE online*, 2, 2024, 1111 ss.

cittadini stranieri, fa propendere per una lettura discriminatoria del sistema.

La classificazione di tali dati come dati di polizia, anziché amministrativi, consente la cancellazione solo dopo 20 anni dal loro inserimento[16] nonostante i dati dei cittadini stranieri riguardanti il rilascio e il rinnovo del titolo di soggiorno sono dati amministrativi[17]. Se si considerassero tali dati come dati di natura amministrativa e quindi fuori dalle attività e dalle funzioni di polizia, la disciplina applicabile sarebbe quella prevista dal GDPR, sia all'art. 9 e all'art. 2 sexies del d.lgs. 196/2003, come modificati con l'emanazione del regolamento (UE) 2016/679.

Il Ministero dell'Interno, con il decreto del 24 maggio 2017, ha previsto solo l'inserimento di questi dati all'interno di un database di polizia, così determinando rischi di lesione di interessi e diritti fondamentali del cittadino straniero al trattamento dei suoi dati, inevitabilmente degradati in automatico a dati di polizia.

Sul punto è intervenuta in maniera determinante la recente decisione della Corte di giustizia dell'Unione europea (CGUE) del 26 gennaio 2023 resa nella causa C-205/21 con la quale la Corte, nell'interpretare l'art. 10 della direttiva (UE) 2016/680, ha previsto che «il trattamento di dati biometrici e genetici da parte delle autorità di polizia per le loro attività di ricerca, a fini di lotta contro la criminalità e di tutela dell'ordine pubblico, è autorizzato dal diritto dello Stato membro, ai sensi dell'articolo 10, lettera a), di tale direttiva, se il diritto di tale Stato membro contiene una base giuridica sufficientemente chiara e precisa per autorizzare detto trattamento». La Corte quindi, interpretando la disposizione anche in combinato con l'art. 12 della Carta dei diritti, ritiene che le misure e le modalità del trattamento debbano essere previste da un atto normativo in modo chiaro e preciso.

Nell'Unione europea è stata svolta una sperimentazione che ha previsto, lungo confini particolarmente interessati da flussi migratori costanti, l'utilizzo di un algoritmo denominato iBorderCtrl, in grado di rilevare le emozioni di una persona attraverso sistemi di riconoscimento facciale, al fine di individuare dichiarazioni false o contradditorie rilasciate alle autorità di frontiera da parte dei migranti[18].

IBorderCtrl è stato un progetto di ricerca e sviluppo finanziato dall'Unione Europea tramite il programma Horizon 2020, attivo dal 2016 al 2019, con l'obiettivo di sviluppare un sistema intelligente, automatizzato e portatile per i controlli alle frontiere, pensato per rafforzare la sicurezza

---

[16] Nell'ambito del d.p.r. 15/2018, l'art. 10, c. 3, lett. f), si occupa specificamente delle informazioni relative ad attività di polizia giudiziaria conclusasi con provvedimento di archiviazione, fissando in venti anni dall'emissione di tale provvedimento il termine per la conservazione dei dati.

[17] Il Garante Privacy, con il parere n. 74/2017, aveva espresso dubbi sulla attrazione dei dati personali alla materia di polizia per il solo fatto di essere conservati in banche dati di polizia.

[18] Cfr. J. Sànchez-Monedero-L. Dencik, *The politics of deceptive borders: "biomarkers of deceit" and the case of iBorderCtr,* in *Information, Communication & Society*, 2020, 1 ss; L. Hall, *Programming the machine: gender, race, sexuality, AI, and the construction of credibility and deceit at the border,* in *Internet Policy Review*, 10, 4, 2021, 1 ss.; S. Penasa, *Artificial Intelligence and the governance of migration: potentialities and pitfalls between technological neutrality and political design,* in *Opinion Juris in Comparatione. Studies in Comparative and National Law*, vol. 1, 1, 2022, 97 ss.

dell'area Schengen senza rallentare il flusso delle persone[19].
Il migrante ottiene il provvedimento di autorizzazione al passaggio della frontiera a seguito del superamento delle procedure previste da IBorderCtrl.
Il funzionamento di tale sistema si articola in due fasi. La prima fase prevede che al viaggiatore venga chiesto di fornire informazioni sulla sua persona e sui dettagli del viaggio.
Queste indicazioni vengono, poi, verificate con vari data-base per determinare se sono soddisfatte le premesse per poter effettuare l'attraversamento di frontiera.
Successivamente, al fine di accertare che le informazioni fornite siano corrette, la seconda fase del sistema iBorderCtrl prevede l'utilizzo di un sistema di lie-detecting di intelligenza artificiale gestito da una guardia di frontiera virtuale, che valuta i minimi dettagli delle loro espressioni facciali, utilizzando tecniche facciali e tecnologie di riconoscimento delle emozioni.
Il sistema IBorderCtrl, fondamentalmente basato su una valutazione di pericolosità, è stato definito come «sistema computazionale del tutto automatizzato della valutazione di pericolosità»[20].
L'obiettivo sotteso al funzionamento della nuova procedura di controllo è dichiaratamente quello di prevenire la commissione di reati nell'area Schengen da parte di soggetti extracomunitari: una finalità di prevenzione del crimine che richiede una valutazione di pericolosità su cui fondare, eventualmente, un provvedimento interdittivo.
Il progetto attualmente è stato sospeso: la fase operativa si è conclusa nel 2019 e la tecnologia di base - sviluppata tra l'altro dalla società Silent Talker, spin-off dell'Università di Manchester - è stata dismessa. In sintesi, iBorderCtrl non è mai diventato un sistema operativo attivo alle frontiere, ma ha fatto scuola dal punto di vista giuridico, quale caso emblematico sull'equilibrio tra innovazione tecnologica, tutela degli interessi commerciali e dovere di trasparenza nei progetti finanziati con fondi pubblici.
Invece, il progetto AFAR (Algorithmic Fairness for Asylum Seekers and

[19] A proposito del progetto *iBorderCtrl,* nel noto caso T-158/19 – Breyer v REA, il ricorrente, Patrick Breyer, deputato e attivista per i diritti digitali, aveva chiesto alla *Research Executive Agency* (REA) - l'Agenzia esecutiva per la ricerca della Commissione europea - accesso a vari documenti relativi al progetto *iBorderCtrl*, per sviluppare un dibattito pubblico ed etico su tali temi. REA aveva rigettato la richiesta, giustificando la scelta con l'eccezione prevista dell'art. 4 del regolamento 1049/2001 relativa alla tutela degli interessi commerciali di terzi e con un riferimento al regolamento 1290/2013, che proteggeva la riservatezza delle informazioni nei progetti Horizon 2020. A seguito della richiesta di annullamento della decisione da parte di Breyer, il Tribunale (General Court) il 15 dicembre 2021 ne accoglieva solo parzialmente alcuni profili, osservando che REA non aveva adeguatamente trattato la richiesta ai sensi degli artt. 7 e 8 del regolamento 1049/2001. Breyer aveva successivamente fatto ricorso alla CGUE per ottenere l'annullamento totale del giudizio di primo grado, sostenendo che vi era un interesse pubblico superiore a giustificare la divulgazione di quei documenti, dati i potenziali impatti sui diritti fondamentali e sulla trasparenza. Nella causa C-135/22 P – *Breyer v REA,* la Corte, con una sentenza del 7 settembre 2023, sottolineava come i possibili rischi ai diritti fondamentali generano un interesse pubblico legittimo, ma non necessariamente superiore agli interessi commerciali: per la Corte, Breyer non ha infatti dimostrato che vi sia un effettivo interesse pubblico superiore tale da giustificare il superamento dei rifiuti di accesso previsti dalla normativa.

[20] Cfr. F. De Simone, *Una nuova tipologia di misure di prevenzione: algoritmi, intelligenza artificiale e riconoscimento facciale*, in *Archivio penale*, 2, 2023, 13.

Refugees), avviato nel 2021 con un finanziamento della Volkswagen Foundation nell'ambito del programma "Challenges for Europe", è un'iniziativa interdisciplinare che coinvolge istituti come la Hertie School di Berlino, l'European University Institute di Firenze e le Università di Oxford, Copenhagen e Zagabria.
Scopo dell'iniziativa è quello di esaminare criticamente come vengono utilizzate tecnologie di automazione e intelligenza artificiale nei processi di gestione delle frontiere, delle procedure di asilo e dell'integrazione dei rifugiati.
Il gruppo di ricerca ha mappato l'adozione di strumenti come sistemi di riconoscimento facciale, rilevazione dei flussi migratori, automazione delle domande di visto, tecnologie per documenti falsi, riconoscimento delle emozioni dei soggetti.
Il progetto ha prodotto report come Automating Immigration and Asylum nel gennaio 2023, stimolando dibattiti pubblici e scientifici sull'equità degli algoritmi, e ha istituito un Tech Litigation Database, strumento destinato a raccogliere contenziosi legati all'uso delle tecnologie nei meccanismi migratori. Dai risultati emerge che tali tecnologie presentano rischi concreti di discriminazione, violazione della privacy e mancanza di trasparenza, fornendo, nello stesso tempo, un contributo essenziale per valutare in quali modalità tali tecnologie possono essere utilizzate in modo giusto, efficace e compatibile con lo Stato di diritto[21].
Invece, l'organizzazione Statewatch ha prodotto nel 2019 l'importante ricerca "Data Protection, Immigration Enforcement and Fundamental Rights"[22], realizzato in collaborazione con PICUM (Platform for international Cooperation on undocumented migrants), the Centre for European Policy Studies (CEPS) and European Migration Law, che analizza come l'interoperabilità di sistemi come Eurodac, EES o ETIAS impatti in modo sproporzionato i migranti irregolari, tramite nuove norme che mancano delle garanzie necessarie per proteggere le persone dall'esercizio arbitrario, ingiustificato o eccessivo del potere statale. Un attento monitoraggio dell'attuazione di queste norme sarà fondamentale per tutelare i diritti dei migranti irregolari.
Ancor più recentemente, l'organizzazione Statewatch nel 2025 ha prodotto un altro studio dal titolo "Automating Authority: Artificial intelligence in European police and border regimes", nel quale la Sezione 3 "Security AI in EU agencies" esamina, in particolare, i progetti e le attività avviati da eu-LISA ed Europol, nonché da Frontex, Eurojust e dall'Agenzia europea per l'asilo, basati sull'utilizzo di tecnologie come il riconoscimento facciale all'apprendimento automatico e le tecnologie predittive[23].
Non sarebbe peregrino affermare come il sistema della sorveglianza predittiva, in campo migratorio, tramite strumenti di IA rientri nel novero

[21] Cfr. D. Ozkul, *Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe*, prodotto dal Refugee Studies Centre e dall'University of Oxford (disponibile su *hertie-school.org*, gennaio 2023).

[22] Disponibile su *picum.org*.

[23] Disponibile su *statewatch.org*.

delle misure di prevenzione[24], altrimenti dette di polizia, vista la loro competenza esclusiva affidata, fino a qualche tempo fa, all'autorità di P.S.
Come noto, di queste misure non di rado si pone in discussione la natura penale amministrativa, talché è pressoché unanime il convincimento per cui siano misure amministrative, appartenenti a quel settore del diritto amministrativo che considera la sicurezza pubblica come un affare cui lo Stato deve provvedere.
La sicurezza pubblica esige provvedimenti precauzionali o cautelativi che possono incidere sulle libertà personali e, in generale, sui diritti fondamentali: il loro presupposto applicativo non è mai il reato, talché la loro natura è squisitamente cautelare, diretta a prevenire la commissione di reati, affinché la sicurezza pubblica, nell'ottica della prevenzione generale, sia salvaguardata da tale eventualità[25].
Lo sviluppo tecnologico ha sempre portato a significativi cambiamenti per l'umanità e intorno ai sistemi di intelligenza artificiale ci sono grandi aspettative. Grandi, però, sono anche i rischi in termini di tenuta del sistema giuridico, in riferimento al rispetto dei principi e dei diritti fondamentali, soprattutto quando dietro questi strumenti si celano istituti, come "nuove" forme di misure di prevenzione.
Nel sistema di iBorderctrl, ad esempio, la società viene protetta da ogni tipo d'impatto col soggetto ritenuto predittivamente "pericoloso", a cui viene limitata la libertà di circolazione tramite un provvedimento restrittivo, che esula dalle tutele proprie del diritto penale sostanziale e processuale.
IBorderctrl fondava il giudizio valutativo della pericolosità del soggetto su un giudizio di natura predittiva totalmente disancorato da qualsiasi violazione di legge, foss'anche in termini di "mero sospetto", come accade

[24] Cfr. sul punto M. Fattore*, Il sistema delle misure di prevenzione: un'introduzione possibile,* in *Sistema penale*, 1° luglio 2024; L. Lacchè, *Uno sguardo "fugace". Le misure di prevenzione in Italia tra ottocento e novecento*, in *Rivista Italiana di diritto e procedura penale*, 2, 2017, 413 ss.; Id., *La paura delle "classi pericolose". Ritorno al futuro?* in *Quaderni di storia del penale e della giustizia,* 1, 2019, 159 ss.; L. Elia, *Libertà personale e misure di prevenzione*, Milano, 1962, 23 ss.; F. Bricola, *Forme di tutela ante delictum e profili costituzionali della prevenzione*, in *Le misure di prevenzione. Atti del Convegno, Centro difesa sociale Convegni di studio "Enrico De Nicola" - Problemi attuali di diritto e procedura penale*, Milano, 1975, 29 ss.; G. Amato, *Potere di polizia e potere del giudice nelle misure di prevenzione*, in *Politica del diritto*, 1974, 331 ss.; A. De Lia, *La sconfinata giovinezza delle misure di prevenzione*, in *Archivio penale*, 1, 2017, 1 ss.; D. Pulitanò, *Misure di prevenzione e problema della prevenzione. Relazione di sintesi,* in *Rivista Italiana di Diritto e procedura penal*e, 2, 2017, 637 ss.; F. Basile, *Esiste una nozione ontologicamente unitaria di pericolosità sociale*? *Spunti di riflessione, con particolare riguardo alle misure di sicurezza e alle misure di prevenzione*, in C.E. Paliero-F. Viganò-F. Basile-G.L. Gatta (a cura di), *La pena, ancora: fra attualità e tradizione: studi in onore di Emilio Dolcini*, Milano, 2018, 955 ss.

[25] Cfr. R. Nobile, *La vulnerabilità del migrante nell'era delle smart borders e delle tecnologie lie-detecting*, in *Bio Journal - Rivista di Biodiritto*, 1, 2024, 296: «Avanza progressivamente l'orizzonte del realismo della sorveglianza, l'idea secondo cui nonostante si riconoscano e si temano gli errori di un sistema, che limita le libertà e invade i diritti, non sia possibile ormai immaginare una società senza un controllo onnipresente. In tal modo, il discorso di *iBorderCtrl* rivela una tendenza a ritrarre le forze di polizia digitali impegnate nella prevenzione del crimine e nell'immobilizzazione dei sospetti come qual-cosa di neutrale, naturalmente buona, che sembra richiamare l'immagine foucaultiana di un potere sorvegliato «attraverso una figura gerarchica continua che assicura l'obbedienza, comandata da buoni ufficiali e uomini di sostanza».

nelle misure di prevenzione.
L'idea di fondo della prevenzione è che lo Stato non deve agire reprimendo il colpevole solo dopo aver commesso il reato, «ma deve difendere sé stesso, la società e i cittadini anche da "pericoli non immediati", facendo a meno del "fardello" dei principi posti a presidio delle libertà fondamentali»[26].

3. Il nuovo Patto sulla migrazione e l'asilo e l'influenza dell'IA sui diritti umani digitali

Le più recenti disposizioni in tema di diritti digitali dei migranti e intelligenza artificiale non valorizzano la necessità di un innalzamento delle tutele nell'utilizzo di IA in materia di trattamento dei dati.
Il 14 maggio 2024 il Consiglio d'Europa ha adottato il nuovo Patto sulla migrazione e l'asilo, dopo l'approvazione del Parlamento del 10 aprile 2024[27], un pacchetto di riforme che prevede che nelle frontiere e nei centri di detenzione venga impiegata una tecnologia particolarmente invasiva, che i dati personali vengano raccolti in massa e scambiati tra le forze di polizia nell'UE e che i sistemi di identificazione biometrica vengano usati per tracciare gli spostamenti delle persone e aumentare i controlli di polizia nei confronti dei migranti sprovvisti di documenti.
L'età minima per la raccolta dei dati è stata abbassata da quattordici a sei anni e le nuove procedure di screening e di frontiera imporranno controlli di sicurezza anche verso i richiedenti asilo processi decisionali automatizzati e basati sull'intelligenza artificiale.
Le persone identificate come "rischio per la sicurezza nazionale" o per "l'ordine pubblico" saranno sottoposte a procedure accelerate con minori garanzie per il trattamento della domanda di asilo. Concetti quelli di sicurezza nazionale o ordine pubblico che ancora una volta rappresentano il criterio di esercizio della discrezionalità agli Stati membri. Governare il fenomeno migratorio in maniera adeguata e preventiva significa anche offrire ai migranti la possibilità di poter essere essi stessi destinatari di quelle condizioni di sicurezza che assicurano il rispetto dei diritti di ciascun individuo.
Sotto tale aspetto, il nuovo regolamento (UE) 1689/2024 sull'IA[28] sembra anche esso andare in una direzione poco garantista.
Secondo l'art. 6, par. 1, del regolamento, un sistema di IA è considerato ad alto rischio se soddisfa due condizioni principali: l'utilizzo come componente di sicurezza, nel senso che il sistema è impiegato come componente di un prodotto regolato dalla normativa europea, e la valutazione di conformità, nel senso il prodotto che incorpora il sistema di IA deve essere

[26] Cfr. F. De Simone, *Una nuova tipologia di misure di prevenzione,* cit., 14.

[27] Per una complessiva disamina del Patto cfr. *consilium.europa.eu.* Cfr. V. Boggini-G. D'Alconzo, *Il Patto europeo Migrazioni e Asilo: un'occasione persa*, in *Ordine Internazionale e Diritti Umani*, 2, 2024, 393 ss. Per il testo dei regolamenti/direttive del Patto, cfr. *rivista.eurojus.it.*

[28] Il testo è disponibile su *sistemapenale.it.*

soggetto a una valutazione da parte di terzi prima della sua immissione sul mercato o della sua messa in servizio ai sensi della normativa di armonizzazione dell'Unione elencata nell'Allegato I.
I sistemi rientranti in tale categoria sono quelli che, per la loro natura o per il contesto in cui vengono impiegati, possono influenzare significativamente la vita delle persone, la sicurezza o i diritti fondamentali. La normativa impone che questi sistemi rispettino rigorosi requisiti di trasparenza, sicurezza, controllo umano e gestione dei dati. L'AI Act si è limitato a inserire nella lista ad alto rischio (senza proibirli) i sistemi per esaminare le richieste d'asilo e quelli per rilevare, riconoscere o identificare le persone ai confini.
In un contesto così delicato, dove le decisioni hanno un impatto profondo sulla vita delle persone, un errore di identificazione dei bias algoritmici può portare a conseguenze ingiuste e illegittime come detenzioni prolungate, divieti di ingresso legittimo o, in casi estremi, espulsioni ingiustificate.
La previsione delle tendenze migratorie, a differenza degli emendamenti proposti dal Parlamento, non è stata inclusa nella lista ad alto rischio.
I database delle migrazioni (come EURODAC e ETIAS) dovranno essere conformi all'AI Act solo a partire dal 2030.
A proposito dei database, se originariamente lo scopo dell'EURODAC (European Asylum Dactyloscopie Database)[29] era solo quello di consentire il confronto delle impronte digitali, con la modifica introdotta con regolamento (UE) 2013/603, il suo impiego è oggi diventato funzionale al contrasto della criminalità grave.
Con il nuovo regolamento (UE) 2024/1358 su Eurodac, invece, si è data attuazione ad un ulteriore obiettivo perseguito, ovverosia quello di facilitare il controllo dell'immigrazione irregolare verso l'Unione.
L'Eurodac è stato progressivamente trasformato in uno strumento per il controllo dei migranti che richiedono protezione internazionale, così come di coloro che soggiornano illegalmente all'interno del territorio dell'Unione senza presentare tale domanda o attraversano irregolarmente una frontiera esterna dell'Unione.
L'elenco dei sistemi ad alto rischio non tiene conto dei numerosi sistemi di IA utilizzati nel contesto della migrazione e che, di conseguenza, non risultano soggetti agli obblighi del regolamento IA Act.
Mentre l'obbligo di trasparenza imporrà a tutte le autorità che utilizzano sistemi ad alto rischio di registrarne le informazioni in un database pubblico, per quanto riguarda le autorità di controllo dei flussi migratori, invece, vi sarà una sezione non pubblica del database, per evitare di monitorare eventuali esiti scorretti e discriminatori.
La sua trasformazione da database biometrico per la gestione dell'asilo a sistema di interoperabilità per un controllo della mobilità anche a sup-

[29] Cfr. I. V. D. Ploeg, *The illegal body: "Eurodac" and the politics of biometric identification*, in *Ethics and Information Technology*, 1, 1999, 295 ss.; V. Ferraris, *Eurodac e i limiti della legge: quando la protezione dei dati personali non esiste,* in *Diritto, immigrazione e cittadinanza*, 2, 2017, 1 ss.; E. Celoria-V. Ferraris, *Eurodac: dalla gestione delle domande di protezione internazionale al controllo della mobilit*à, in *Quaderni AISDUE*, 4, 2024, 11 ss.; A. Latino, *Il Regolamento Eurodac quale paradigma della (con)fusione di istanze umanitarie e securitarie,* in R. Evangelista-A. Latino (a cura di), *Con-vivere nel (dis)ordine,* Napoli, 2018.

porto dei rimpatri[30] ha portato diversi autori a guardare al nuovo sistema Eurodac come ad un tassello centrale della politica di criminalizzazione dei migranti e dei richiedenti asilo, tanto da parlare di processo di crimmigration[31].

Ricorre al trattamento dei dati anche l'European Travel Information and Authorisation System (ETIAS)[32], che rilascia un'autorizzazione elettronica per l'ingresso dei cittadini di Paesi terzi esenti dall'obbligo di visto e ha lo scopo di valutare se la loro presenza nel territorio degli Stati membri possa rappresentare un pericolo per la sicurezza, in termini di immigrazione illegale o di alto rischio epidemico.

Il nuovo regolamento europeo sull'intelligenza artificiale evidenzia spesso nei considerata come il trattamento dei dati personali debba avvenire in modo proporzionato, necessario e trasparente.

Gli algoritmi dei sistemi di IA lavorano sulla base di dati e, laddove questi siano di carattere personale, troveranno applicazione a ciascun sistema basato su tali tecnologie le regole previste dal GDPR[33], in aggiunta a quelle dell'AI Act.

La tutela accordata, infatti, al diritto alla privacy e alla protezione dei dati personali dal regolamento (UE) 2016/679 (GDPR), così come previsti dalla Carta dei diritti fondamentali, non può ritenersi limitata ai cittadini

---

30 Cfr. K. Strak, *Eurodac as an Instrument of the EU Return Policy*, in *Polish Review of International and European Law*, 7, 2018, 41 ss.

31 Cfr. N. Amelung, *"Crimmigration Control" across Borders: The Convergence of Migration and Crime Control through Transnational Biometric Databases,* in *Historical Social Research*, 3, 2021, 151 ss; B. Menez Queiroz, *The Impact of EURODAC in EU Migration Law: The Era of Crimmigration?* in *Market and Competition Law Review*, 1, 2019, 157 ss. In particolare, cfr. E. Celoria-V. Ferraris, *Eurodac: dalla gestione delle domande di protezione internazionale*, cit., 11: «Il diritto dell'Unione europea non è estraneo a questi meccanismi, tanto che efficacemente V. Mitsilegas sottolinea come in ambito europeo la criminalizzazione vada intesa «*as the threefold process whereby migration management takes place via the adoption of substantive criminal law, via recourse to traditional criminal law enforcement mechanisms including surveillance and detention, as well as via the development of mechanisms of prevention and preemption*» Anche l'evoluzione del funzionamento di Eurodac si inserisce pienamente in questo quadro».

32 Cfr. A. Procaccino, *Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione,* in *Diritto penale contemporaneo*, 1, 2023, 155: «Diciamo subito che l'entrata in funzione di ETIAS è stata rimandata ormai ben tre volte (una prima volta dal 2022 al gennaio 2023, una seconda al maggio 2023 e una terza a novembre 2023). Ciò che in questa sede più interessa è che l'ETIAS rappresenta uno degli esempi più vividi di compresenza di poteri e finalità di natura *latu sensu* amministrative e penali, tra loro intercomunicanti proprio per mezzo dell'interoperabilità delle banche dati costruita nel Regolamento».

33 Cfr. S. Tommasi, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo,* in *Revista de Dereito Brasiliera*, 27, 2020, 118: «In Europa, il Regolamento generale sulla protezione dei dati, (UE/2016/679), cd. GDPR, costituisce una componente importante dell'approccio alla tecnologia incentrato sulla persona nel contesto della duplice transizione, ecologica e digitale, delle politiche dell'UE. D'altronde non potrebbe essere diversamente in un'economia sempre più basata sul trattamento di dati, compresi quelli personali. L'attenzione al rischio di discriminazione algoritmica emerge già dal considerando 71 del GDPR, ove si legge che il titolare del trattamento dei dati deve garantirne la sicurezza e impedire effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione, delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di saluto o dell'orientamento sessuale».

dell'Unione europea.
Appare dunque evidente che il GDPR debba necessariamente applicarsi anche ai richiedenti asilo all'interno dell'Unione. Tuttavia, va rilevato come la protezione dei dati personali loro garantita possa risultare, sotto alcuni profili, meno rigorosa rispetto a quella accordata ai cittadini dell'Unione Europea.
Oltre alle disposizioni normative, anche i criteri di bilanciamento come quello di proporzione, necessità ed extrema ratio devono trovare applicazione anche in caso di trattamento di dati di migranti: la compressione del diritto deve essere proporzionata alle finalità del trattamento, così come la limitazione deve essere strettamente necessaria per il perseguimento dei interessi superiori e la scelta di compressione del diritto legittima solo extrema ratio, nel senso che l'interesse pubblico preminente non può essere in altro modo realizzato[34].
Amnesty International ha pubblicato (2024) un documento introduttivo sull'utilizzo rapido e diffuso delle tecnologie digitali nei sistemi di gestione di migranti e richiedenti asilo in tutto il mondo, inclusi Stati Uniti, Regno Unito e Unione europea.
Il documento, intitolato "Difendere i diritti dei migranti e dei rifugiati nell'era digitale"[35], mette in luce alcuni dei principali avanzamenti della tec-

[34] A proposito della necessità di bilanciamento tra esigenza di sicurezza nazionale e tutela dei diritti umani individuali, nel noto caso C-817/19 - *Ligue des droits humains* la CGUE ha emesso una delle decisioni più importanti in tema di sorveglianza, protezione dei dati personali e sicurezza. In Belgio una legge nazionale aveva recepito la Direttiva PNR (*Passenger Name Record*) dell'Unione europea che impone alle compagnie aeree di raccogliere e trasmettere alle autorità i dati personali dei passeggeri (come nome, data di nascita, itinerario, metodo di pagamento, ecc.), anche per i voli all'interno dell'UE, con lo scopo di prevenire reati gravi e atti di terrorismo. L'organizzazione *Ligue des droits humains* aveva contestato questa legge davanti alla Corte costituzionale belga, affermando che l'associazione, la raccolta e il trattamento sistematico di questi dati rappresentassero una violazione della privacy e della protezione dei dati, oltre a ledere la libertà di movimento. Non si può sacrificare il diritto alla *privacy* al fine di riconoscere una tutela anticipata e preventiva, senza una reale necessità. La Direttiva PNR dell'Unione europea impone agli Stati di raccogliere e trattare i dati dei passeggeri aerei, al fine di individuare potenziali minacce della realizzazione di fatti di reato; tuttavia, tale potere deve rispettare i diritti fondamentali individuali e i principi di proporzionalità e necessità, perché lo strumento penale - nemmeno quello preventivo – non può trasformarsi in strumento di controllo sistematico e indiscriminato dei cittadini.
Nel parere del 26 luglio 2017, la Grande sezione della CGUE si è pronunciata in senso negativo circa la compatibilità con la Carta dei diritti fondamentali del progetto di accordo tra l'Unione europea e il Canada sul trasferimento dei dati del codice di prenotazione dei passeggeri aerei. Nel parere n. 1/15 la Corte si è innanzitutto occupata della questione della base giuridica degli accordi PNR: il contenuto dell'accordo, tramite il trasferimento di dati verso il Canada e lo scambio di dati con le autorità competenti degli Stati membri, nonché con Europol ed Eurojust, persegue la finalità di garantire la sicurezza pubblica (§ 82); allo stesso tempo, l'accordo si prefigge lo scopo di garantire un livello adeguato di protezione dei dati (§ 84). Dal momento che, nel caso di specie, nessuna delle due esigenze, ovvero la sicurezza pubblica e il rispetto dei dati personali, risulta preponderante sull'altra, la Corte ha stabilito che l'accordo deve fondarsi, in via eccezionale, sia sull'art. 16(2) TFUE, relativo alla protezione dei dati, sia sull'art. 87(2)(a) TFUE, relativo alla prevenzione e all'individuazione dei reati (testo parere disponibile su *osservatoriosullefonti.it*).

[35] Il Documento è disponibile su *d21zrvtkxtd6ae.cloudfront.net*: «*Amnesty International recognises that digital technology could support the respect, protection and promotion of refugee and*

nologia digitale nei sistemi di gestione delle richieste d'asilo e dei flussi migratori, focalizzandosi sui sistemi che elaborano ingenti quantità di dati e sulle questioni connesse ai diritti umani che sorgono come conseguenza del loro utilizzo/trattamento.

Come è stato sottolineato, il margine di errore che può essere associato a tecnologie come il riconoscimento facciale, che risulta essere particolarmente elevato proprio in riferimento ai tipi di individui migranti, il rischio di discriminazione e stigmatizzazione nei confronti di specifici gruppi sociali (come le minoranze e le donne), derivante dalla presenza di biases cognitivi che possono caratterizzare i sistemi autonomi basati sull'apprendimento automatico, l'effettività del diritto a non essere sottoposti a una decisione completamente autonoma, la necessità di garantire una supervisione umana all'interno del processo decisionale, il diritto a un ricorso effettivo rappresentano «le principali criticità generalmente associate a queste tecnologie»[36].

L'impiego di tecnologie associate a sistemi intelligenti potrebbe impattare negativamente sulle garanzie previste dalla CEDU, in particolare il rischio di essere sottoposto a trattamenti inumani e degradanti in caso di respingimento e il divieto di espulsioni collettive – per essere ingiustamente riconsegnati in Paesi non sicuri, perché sospettati o potenziali pericolosi – oltre che il diritto a un rimedio effettivo contro le decisioni assunte a livello amministrativo, con riferimento all'(in)esistenza di rimedi giurisdizionali adeguati a fronte di decisioni assunte dalle autorità competenti in merito all'indice di pericolosità di un determinato soggetto, o alla fondatezza di una domanda di protezione internazionale, che risulti basata anche sui dati ricavati dall'utilizzo errato di algoritmi predittivi.

La raccolta di dati sensibili, come i dati biometrici, e il loro inserimento in database, spesso difficilmente accessibile ai migranti stessi, solleva legittime preoccupazioni riguardo alla proporzionalità di tali misure rispetto agli obiettivi di sicurezza pubblica[37].

---

migrants' rights in certain situations, for example through connecting people on the move with vital services and reliable information.6 Yet, it still entails risks including to the rights to privacy and non-discrimination. People on the move are increasingly perceived as "security threats", and "national security" measures are continuously implemented to exclude people based on their perceived race, ethnicity and religion, among other grounds. For example, disproportionate and unlawful surveillance and other measures increasingly used for racial profiling and policing create and sustain human rights violations and are also increasingly adopted for use against asylum seekers, refugees and migrants, broadly. These measures and uses of digital technologies are a slippery slope towards the erosion of crucial protections for communities on the move. The combination of corporate interests, a general lack of respect for the rights of people on the move, and systemic racism and discrimination can allow technology to develop faster than the sufficient safeguards and oversight required to hold an ever-growing tech sector to account» (p. 4).

[36] Cfr. S. Penasa, *Smart borders* o *invisibile walls? L'utilizzo di sistemi "intelligenti" al confine tra politiche migratorie e garanzie per gli stranieri*, in G. Del Turco-C. Milano-M. Savino-M. Tuozzo-D. Vitiello (a cura di), *Annuario Adim 2022. Raccolta di scritti di diritto dell'immigrazione*, Napoli, 2023, 54.

[37] Cfr. M. Forti, *Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della privacy dei migranti e dei rifugiati all'interno del territorio europeo*, in questa *Rivista,* 2, 2020, 218: «Il trattamento dei dati cd. "sensibili" può essere condotto se necessario pe motivi di interesse pubblico sulla base del diritto dell'Unione europea e deli Stati membri. Tale trattamento deve però rispettare i principi della *data protection,* prevedere misure specifiche per la tutela dei diritti fondamentali delle persone coinvolte

Si consideri l'art. 9 del GDPR il quale, pur vietando specificamente il trattamento di dati che possano rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, l'orientamento sessuale, nonché dati genetici, biometrici e sanitari, prevede al contempo delle eccezioni che invece lo consentono in circostanze particolari, ovvero, ad esempio, i motivi di interesse pubblico. Tale ambivalenza normativa solleva importanti interrogativi riguardo alla reale tutela dei diritti individuali e alla legittimità delle deroghe adottate, soprattutto in relazione al principio di proporzionalità e adeguatezza della compressione del diritto rispetto al raggiungimento di pubbliche finalità.

In un contesto delicato come quello dell'immigrazione, dove la necessità di garantire la sicurezza dei confini nazionali è in tensione con l'obbligo di rispettare i diritti fondamentali delle persone immigrate, il principio di proporzionalità dovrebbe infatti assumere un ruolo cruciale, vista la reale esigenza di garanzia di un effettivo bilanciamento tra situazioni giuridiche ugualmente meritevoli di tutela, ancorché tra loro potenzialmente contrastanti.

La normativa di settore conduce a scenari di potenziali abusi, in quanto, in contesti di emergenza, come quelli spesso legati alla gestione dei flussi migratori irregolari, la deroga ai principi di proporzionalità, necessità e trasparenza potrebbe essere invocata per motivare misure sproporzionate, prive delle necessarie garanzie di controllo e pubblicità e potenzialmente discriminatorie causate da distorsioni ed errori insite nel sistema algoritmico, ma giustificate dal perseguimento della sicurezza pubblica.

Il riconoscimento facciale, rientrando nella categoria di sistemi di IA "ad alto rischio", richiederebbe una rigorosa valutazione di conformità che non dovrebbe essere soggetta a deroghe, in modo da garantire che il suo uso non violi i diritti fondamentali, specie se i destinatari della normativa sono i migranti, soggetti per definizione vulnerabili

L'obiettivo primario dovrebbe essere quello di assicurare un equilibrio tra sicurezza e diritti fondamentali, un equilibrio che rappresenta non solo un obbligo legale, ma anche un imperativo morale, assolutamente essenziale per l'integrità delle società moderne e per la difesa dei diritti fondamentali negli Stati democratici e di diritto.

---

e deve essere proporzionato alle finalità perseguire. Il carattere di proporzionalità non può ovviamente essere preventivamente definito, ma deve essere riscontrato nel caso concreto. (…) La raccolta di dati "sensibili" come gli identificativi biometrici e il loro successivo deposito in database a cui il soggetto migrante ha spesso accesso perlomeno complesso e difficoltoso, può essere considerata una misura proporzionata alle finalità di sicurezza pubblica? La Corte europea dei diritti dell'uomo ha più volte specificato che, pur riconoscendo la validità di tali finalità, il diritto alla privacy e all'autonomia informativa dei soggetti coinvolti non può venir meno». Cfr., anche, Id., *Il Regolamento (UE) 2016/679 alla prova dei flussi migratori diretti verso l'Europa mediterranea. La tutela dei dati personali di rifugiati e migranti*, in D. Poletti-A. Mantelero (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna,* Pisa, 2018, 481 ss.; Id., *Il diritto alla protezione dei dati personali nell'emergenza migratoria. L'utilizzo dello smartphone e dei social media da parte di migranti e rifugiati: tra tutele per l'identità personale e preoccupazioni per la privacy,* in *CyberLaws*, 10 giugno 2020.

4. Diritti umani digitali e protezione delle frontiere. Quali tutele (in)esistenti?

I sistemi analizzati testimoniano la "postura securitaria" dell'Unione europea nell'impiego di tecnologie avanzate per la gestione dei flussi migratori nelle frontiere esterne.
È sempre più noto come, nel contesto delle migrazioni contemporanee, le tecnologie digitali stanno diventando strumenti centrali per il controllo dei confini: sistemi biometrici, algoritmi predittivi, analisi comportamentale automatizzata, riconoscimento facciale e tracciamento digitale vengono sempre più impiegati per monitorare i flussi e, talvolta, respingere persone migranti dal territorio.
Questa evoluzione solleva interrogativi cruciali sulla effettiva tutela dei diritti umani in ambito digitale, di un soggetto, il migrante, spesso "rinchiuso" nel reticolo invisibile delle tecnologie digitali, che decidono la sorte dei propri diritti personale senza trasparenza, senza contraddittorio, e talvolta senza una base giuridica solida.
In chiave propositiva, anzitutto, bisognerebbe integrare esplicitamente nei testi normativi europei (come il Patto su Migrazione e Asilo) una sezione dedicata alla protezione dei diritti digitali dei migranti.
Sarebbe utile sicuramente creare un organismo indipendente a livello europeo, o rafforzare il ruolo dell'EDPS (Garante europeo della protezione dei dati), per vigilare specificamente sull'uso delle tecnologie nei contesti migratori e di controllo delle frontiere, anche alla luce del fatto che non esiste un similare figura a livello nazionale (diversa da quella del Garante nazionale dei diritti delle persone private della libertà personale).
Non è peregrino dover affermare quanto sia importante, inoltre, introdurre l'obbligo per ogni sistema decisionale automatizzato impiegato in materia migratoria di fornire una spiegazione accessibile e traducibile all'interessato, proprio tramite un mediatore specializzato che sia in grado di spiegare l'effettivo utilizzo dei dati di ogni singolo soggetto.
Ogni sistema di sorveglianza digitale o decisione algoritmica con effetti giuridici o di fatto sulla libertà personale dei migranti dovrebbe, inoltre, tassativamente essere sottoposto ai principi di legalità e determinatezza, che ostacolino l'uso di sistemi predittivi o di bias algoritmici finalizzato a classificare i migranti come "potenzialmente pericolosi" sulla base di comportamenti, tratti biometrici, nazionalità o rotte seguite durante le proprie traversate.
Nello stesso senso, sarebbe, infine, necessario prevedere, a livello di obblighi di incriminazione specifici da parte della normativa europea, in perfetta coerenza con il principio di extrema ratio, per sanzionare l'abuso, la conservazione illegale o la diffusione indebita di dati biometrici raccolti alle frontiere, in assenza di giustificazione giuridica precisa.
La necessità di rafforzare le tutele in tale complesso ambito diventa oltremodo marcata con riferimento alle attuali di alcuni Stati membri di esternalizzare i controlli alle frontiere sul territorio di Paesi terzi.
La esternalizzazione delle procedure delle domande di asilo in strutture collocate sul territorio di Stati non appartenenti all'UE, con standard di tutela inferiori - come nel caso del Protocollo tra Italia e Albania - aumen-

terebbe in maniera esponenziale il pericolo di violazione di diritti fondamentali nelle procedure in frontiera supportate dall'impiego di sistemi dotati di intelligenza artificiale, rispetto ai quali occorre individuare le specifiche attività di monitoraggio rigoroso e le correlate responsabilità statali per i flussi di dati che transitano per finalità di gestione (e contenimento) delle migrazioni.

Abstract

Uno dei principali risultati della ricerca di Hermes Center for trasparency and digital human rights dal titolo "Tecnologie per il controllo delle frontiere in Italia" (2021) denuncia come la criminalizzazione della persona migrante, rifugiata o richiedente asilo sia inscritta nell'infrastruttura tecnologica italiana. L'impatto della digitalizzazione sul controllo dei flussi migratori è stato, inoltre, approfondito nel report di Amnesty International dal titolo "Defending the rights of refugees and migrants in the digital age" (2024) che denuncia come il crescente ricorso a tecnologie di esternalizzazione delle frontiere europee, software per la gestione dei dati, biometria e sistemi decisionali algoritmici conduce a continue violazioni dei diritti umani. Tali tematiche impongono riflessioni sul difficile bilanciamento tra l'esigenza di sicurezza pubblica e l'effettività delle garanzie previste in relazione ai diritti di privacy e dignità personale dei soggetti coinvolti, sull'assunto che l'utilizzo di una tecnologia non può considerarsi neutrale, se associato alla realizzazione di finalità di carattere politico, come quella di gestione efficiente del fenomeno migratorio.

One of the main findings of the research conducted by the Hermes Center for transparency and digital human rights, entitled "Technologies for border control in Italy" (2021), highlights how the migrant's criminalization is embedded within Italy's technological infrastructure. The impact of digitalization on the control of migratory flows was also explored in the Amnesty International report "Defending the rights of refugees and migrants in the digital age" (2024), which denounces how the increasing use of European technologies for border externalization, data management software, biometrics and algorithmic decision-making tools leads to ongoing violations of human rights. These issues call for reflection on the delicate balance between the need to ensure public safety through invasive digital technologies and the effectiveness of safeguards for the right to privacy and personal dignity of the individuals involved-based on the understanding that the use of a technology cannot be considered neutral when it is tied to political objectives, such as that of efficient management of migration.

Keywords

criminalizzazione – tutele – prevenzione – sicurezza – intelligenza artificiale

I *cloud computing services*: nuove prospettive regolatorie per un'innovazione digitale sostenibile*

Fabiana Magnolo

Sommario

1. Il cloud computing e le sfide per la sostenibilità digitale. – 2. Il panorama normativo italiano e il principio "cloud first". – 3. La regolamentazione dei servizi cloud intra Unione Europea. – 4. Protezione dei dati personali affidati al cloud e GDPR. – 5. Conclusioni e prospettive pro futuro.

1. Il *cloud computing* e le sfide per la sostenibilità digitale

Il cloud computing, o semplicemente cloud, rappresenta un modello, ad oggi particolarmente diffuso, di accesso a risorse software e hardware attraverso strumenti informatici decentralizzati[1].
I servizi di cloud computing consentono a tutti gli utenti che ne fanno richiesta di accedere a tecnologie avanzate (quali reti, server, storage, applicazioni e servizi)[2] senza dover sostenere sforzi economici significativi (ma solo un abbonamento, piuttosto modico) e possono essere offerti congiuntamente dallo stesso fornitore (anche denominato provider) o, come di consueto, da diversi fornitori (che vendono i loro servizi sulla piattaforma del provider).
Un elemento peculiare che caratterizza i modelli cloud è l'erogazione di un service: tale aspetto rivela come essi siano incentrati non sulla dimensione proprietaria, ma proprio sulla fornitura di servizi informatici da parte di

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1 Invero, il mercato del *cloud* è cresciuto in Italia, nel 2024, del 24% rispetto all'anno precedente, raggiungendo un valore di 6,8 miliardi di euro (dati del *Report 2024 dell'Osservatorio Cloud Transformation del Politecnico di Milano*).

2 Il *National Institute of Standards and Technology (NIST)*, facente parte del *Department of Commerce* degli Stati Uniti, ha affermato nella *NIST Definition of Cloud Computing* del 2011 che il «*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models*».

providers terzi, sulla base di un paradigma che la letteratura economica ha interpretato quale «nuova cultura dell'accesso»[3].
L'utilizzo sempre più massiccio della tecnologia cloud per l'archiviazione e/o l'elaborazione di dati o per servizi maggiormente complessi, ed integranti le caratteristiche suindicate, non solo da parte di privati ma anche di pubbliche amministrazioni, nella forma della cosiddetta community cloud[4], rappresenta oggi un dato di rilievo, che spinge inevitabilmente l'interprete a riflettere sull'elaborazione di soluzioni ai nuovi problemi derivanti dall'impiego di siffatte infrastrutture, le cui modalità di funzionamento erano fino a pochi anni fa per lo più ignorate dall'utente (consumatore e non) e, conseguentemente, sottratte a qualsiasi regolamentazione[5].
D'altro canto, la stessa Unione Europea indica lo studio dei problemi giuridici connessi all'uso dei servizi di cloud computing all'interno della New Consumer Agenda - Strengthening consumer resilience for sustainable recovery tra le nuove priorità e i punti cruciali di azione per il benessere dei consumatori su cui lavorare entro il 2025: nello specifico, il punto 3.2. dell'Agenda, denominato Digital Transformation mira, nella dichiarata prospettiva di uno sviluppo in linea con i principi di sostenibilità e green development, a facilitare l'effettivo diritto delle persone alla portabilità dei propri dati (come ampiamente riconosciuto nel Data Act[6]), nella prospettiva di creare un vero mercato unico e spazi comuni di dati intra UE.
In questo senso, quindi, si delinea una tendenza europea verso la ricerca di una sostenibilità dell'ambiente digitale (in conformità con gli obiettivi dell'Agenda Digitale Europea 2030), ovvero l'esigenza di costruire un sistema capace di cogliere le potenzialità dell'evoluzione tecnologica e, al tempo stesso, di tutelare i diritti fondamentali delle persone.
Nell'attuale contesto digitale altamente innovativo e complesso, la presente indagine si propone di analizzare, da un punto di vista strettamente civilistico, il tema dei servizi di cloud computing, soffermandosi in particolare sugli aspetti contrattuali, analizzando l'influsso che la classificazione di tali servizi ha sul piano sia nazionale sia sovranazionale. L'intento ulteriore è di evidenziare le problematiche relative alla protezione dei dati personali affidati al cloud ed all'identità digitale, nonché alla responsabilità del cloud provider, cercando di individuare, nel complesso, prospettive di sviluppo maggiormente eque ed improntate al principio di sostenibilità digitale.

2. Il panorama normativo italiano e il principio *"cloud first"*

A livello nazionale, è certamente opportuno partire menzionando il Piano

[3] J. Rifkin, *The age of access*, Londra, 2000.

[4] La quale espressione allude proprio al fatto che il servizio venga reso disponibile ad una specifica comunità.

[5] L. Ammannati, *Il paradigma del consumatore nell'era digitale. Consumatore digitale o digitalizzazione del consumatore?*, in F. Capriglione (a cura di), *Liber Amicorum Guido Alpa*, Milano, 2019, 436.

[6] Regolamento europeo (UE) 2854/2023 sull'armonizzazione delle norme in materia di accesso equo ai dati e al loro utilizzo, entrato in vigore l'11 gennaio 2024.

Triennale per l'Informatica nella Pubblica Amministrazione 2017-2019, approvato con DPCM del 31 maggio 2017, il quale ha avviato un processo di razionalizzazione e potenziamento delle infrastrutture di Information and Communication Technology della Pubblica Amministrazione.
L'obiettivo è di consentire alle amministrazioni un utilizzo più efficiente e flessibile delle risorse relative all'Information and Communication Technology (ICT), con elevati livelli di economicità, affidabilità e sicurezza: ciò anche nell'ottica di favorire la piena interoperabilità dei dati ed un'offerta di servizi sempre più calibrata sulle esigenze dei cittadini e delle imprese[7].
I molteplici interventi legislativi volti alla trasformazione digitale delle Pubbliche amministrazioni (PA) hanno dato vita ad una strategia evolutiva basata su vari principi, tra cui quello, ivi di particolare rilievo, "cloud first". Secondo tale principio, nel momento in cui si definisce un nuovo progetto o si sviluppano nuovi servizi, la PA deve dare priorità all'adozione del paradigma cloud rispetto a qualsiasi altra tecnologia.
A tal uopo, il processo di qualificazione cui devono sottoporsi i fornitori di servizi cloud prevede tre fasi principali, i.e. di richiesta, di ottenimento e di mantenimento della qualifica.
Inoltre, in linea con quanto previsto dal Piano Triennale, l'Agenzia per l'Italia Digitale ha effettuato il censimento del patrimonio dell'ICT delle pubbliche amministrazioni, finalizzato a classificare le infrastrutture rilevanti precipuamente in termini di affidabilità e sicurezza[8].
Il censimento – i cui risultati sono stati pubblicati come allegato alla Risoluzione dell'Agenzia n. 1 del 14 giugno 2019 – ha evidenziato un quadro di elevata frammentazione, livelli di sicurezza inadeguati ed un'elevata inefficienza in termini di spesa.
Alla luce di tali dati, è stato approvato il decreto legge 16 luglio 2020, n. 76, recante «Misure urgenti per la semplificazione e l'innovazione digitale», convertito nella legge 11 settembre 2020, n. 120, al fine di promuovere «lo sviluppo di un'infrastruttura ad alta affidabilità distribuita sull'intero territorio nazionale per la razionalizzazione e consolidamento dei centri per l'elaborazione delle informazioni», a condizione che le amministrazioni centrali dotate di data center di tipo B[9], nel rispetto dei principi di efficienza, efficacia ed economicità dell'azione amministrativa, provvedano a migrare il proprio centro elaborazione dati ed i relativi sistemi informatici presso strutture idonee. Queste ultime, pertanto, dovranno essere individuate tra: (a) il Polo strategico nazionale (attivo dal 2022), (b) infrastrutture già esistenti e rispondenti ai requisiti, (c) l'infrastruttura della Società

[7] G. Napolitano, *Il partenariato pubblico-privato per la realizzazione del Polo strategico nazionale*, in *Giornale di diritto amministrativo*, 27(6), 2021, 704.

[8] R. Carleo, *Il futuro della memoria digitale*, in *La Magistratura*, 1(1), 2022, 1 ss., offre una lucida riflessione sul tema dell'archiviazione digitale dei dati, analizzando, in particolare, i possibili problemi legati alla nuova frontiera del *neuromorphic computing* (che dovrebbe consentire alle macchine di apprendere e pensare).

[9] Si ricorda che il Piano Triennale per l'informatica nella PA 2017-2019, agli effetti della razionalizzazione, suddivide le Amministrazioni in: 1) Poli strategici nazionali (PSN): saranno inseriti in questa categoria soggetti con *data center* caratterizzati da elevati *standard* di qualità; 2) Gruppo A: rientreranno in questa categoria le amministrazioni che dispongono di *data center* con caratteristiche che non verificano pienamente quelle richieste per i PSN; 3) Gruppo B: in pratica, le amministrazioni che residuano.

Generale d'Informatica (Sogei), se resa compatibile con i requisiti previsti dall'apposito regolamento dell'Agenzia per la sicurezza informatica o (d) soluzioni di cloud pubblico per servizi non critici.
Lo stesso decreto-legge n. 76/2020, come ulteriormente modificato dal d.l. del 14 giugno 2021, n. 82, convertito dalla legge 4 agosto 2021, n. 109, ha inoltre stabilito che l'Agenzia per la sicurezza informatica, con proprio regolamento, individua i livelli minimi di sicurezza, capacità di elaborazione, risparmio energetico e affidabilità delle infrastrutture digitali della pubblica amministrazione e definisce le caratteristiche di qualità, sicurezza, performance e scalabilità, interoperabilità e portabilità dei servizi cloud della P.A..
Con lo stesso regolamento, per di più, si individuano i termini e le modalità con cui le amministrazioni dovranno realizzare le predette migrazioni verso strutture tecnologicamente idonee.
In particolare, secondo la Strategia Cloud Italia, sebbene le pratiche internazionali e gli standards tecnici siano ampiamente applicati dai fornitori dei cloud services, data la criticità dei dati e dei servizi coinvolti, la strategia di migrazione non può prescindere da un processo di qualificazione dei fornitori di cloud pubblici e dei loro servizi. Inoltre, tale qualificazione non dovrebbe limitarsi alla valutazione degli aspetti di sicurezza supra menzionati, ma tenere conto anche di quelli 'architetturali' e organizzativi dato che anche questi possono influire sulla resilienza dei servizi forniti, ad esempio in situazioni di lock-in del fornitore[10].
Un'altra direzione importante, in linea con le iniziative e direttive dell'Agenda Digitale Europea 2030, è quella della standardizzazione, dell'armonizzazione e dell'interoperabilità dei servizi cloud: in questa prospettiva, con il coinvolgimento anche dell'Italia, a fine 2019 è stato avviato il progetto GAIA-X con l'obiettivo di sviluppare requisiti comuni per un'infrastruttura dati europea.
L'attuazione del Polo Strategico Nazionale è stata, d'altra parte, inserita tra i progetti qualificanti del Piano Nazionale di Ripresa e Resilienza trasmesso dal Governo italiano alla Commissione Europea il 5 maggio 2021 e, su proposta di quest'ultima, definitivamente approvato dal Consiglio Europeo con decisione esecutiva del 13 luglio 2021.
Nell'ambito della misura «Digitalizzazione, innovazione e sicurezza nella Pubblica amministrazione» del PNRR si sono previsti investimenti finalizzati all'implementazione dell'infrastruttura digitale e alla facilitazione del processo di migrazione verso il cloud.
Il Piano Nazionale di Ripresa e Resilienza (c.d. PNRR), quindi, considera il cloud computing uno strumento essenziale per promuovere il miglioramento delle infrastrutture e dei servizi IT della pubblica amministrazione, ove l'obiettivo principe è di portare il 75% delle PA italiane ad utilizzare tale service entro il 2026. L'esigenza dichiarata dal Governo italiano è quella di realizzare un cloud di prossimità nei prossimi anni per due motivi principali. In primis, esiste indubbiamente un'esigenza tecnologica (si pen-

[10] Si tratta di un'ipotesi (anche detta *vendor lock-in*) in cui un'organizzazione è costretta a continuare ad utilizzare il prodotto o il servizio di un determinato *provider* e non è in grado di cambiare fornitura a causa dei costi accessori, della complessità o della durata di una ipotetica migrazione.

si ad esempio all'Internet of Things o alle auto senza conducente) per cui sarebbe più utile che i server cloud fossero geograficamente vicini ai luoghi di produzione dei vari fenomeni tecnologici. In secundis, la prossimità mira a realizzare una vera sostenibilità digitale, nel pieno rispetto anche del principio di transizione ecologica[11].

3. La regolamentazione dei servizi *cloud* intra Unione europea

In seno all'Unione Europea, le prime indicazioni normative sul cloud risalgono alla Comunicazione del 19 aprile 2016 on the European Cloud Initiative, in cui la Commissione UE ha individuato due aspetti centrali: il primo è lo sviluppo di un'adeguata infrastruttura europea (European Data Infrastructure), costituita da reti per connettività ultraveloce e da adeguate risorse HPC (High Performance Computing). Il secondo, invece, è incentrato sull'implementazione di un sistema cloud di alta qualità che si concentri sul principio di condivisione dei dati (European Open Science Cloud – EOSC). Se per la European Data Infrastructure le questioni da affrontare sono tipiche della politica infrastrutturale, tra cui l'uso dei fondi europei e le modalità di cooperazione pubblico-privato, il secondo punto, per converso, merita una breve analisi – in quanto il processo di realizzazione dell'EOSC è centrale per il problema del rapporto tra nuovi servizi e tutela dei diritti.

Invero, l'obiettivo principale della Commissione Europea attraverso l'EOSC è quello di superare l'attuale frammentazione dei database e nel complesso la loro inadeguata capacità, nonché di facilitare la condivisione e il riutilizzo delle informazioni.

Nell'attuale contesto della strategia UE per il diritto digitale vi sono alcune disposizioni rilevanti per i fornitori di servizi cloud. Si fa riferimento in particolare al Regolamento generale sulla protezione dei dati (GDPR), in vigore ormai dal 25 maggio 2018; al regolamento europeo n. 2854/23 sull'armonizzazione delle norme in materia di accesso equo ai dati e al loro utilizzo (c.d. Data Act); alla strategia dell'UE per la sicurezza informatica (in particolare la direttiva sulle misure per un livello comune elevato di sicurezza informatica nell'UE – direttiva NIS2 2555/22); e ad alcune norme sulla responsabilità dei fornitori di servizi Internet (i.e. regolamento del Parlamento europeo e del Consiglio 2065/22 – Digital Services Act – relativo al mercato unico dei servizi digitali e che modifica la direttiva CE 31/2000, entrato pienamente in vigore il 17 febbraio 2024).

Per quanto riguarda le questioni critiche relative ai servizi cloud, il Data Act prevede un diritto rafforzato alla portabilità dei servizi di cloud computing, agevolando i consumatori nel passaggio da un fornitore di servizi

[11] S. Epifani, *Sostenibilità digitale. Perché la sostenibilità non può fare a meno della trasformazione digitale*, Roma, 2020. Invero, il concetto di sostenibilità digitale si inserisce, in maniera trasversale, nell'ambito dello sviluppo sostenibile (nella sua triplice dimensione ambientale, economica e sociale), principio quest'ultimo che trova (*ex post* riforma del 2022) puntuale riconoscimento costituzionale nell'art. 9 attraverso la menzione dell'interesse delle future generazioni.

di elaborazione dei dati cloud ad un altro, impedendo il lock-in del provider.
Su questo punto, si prevede di eliminare gradualmente le tariffe pass-through nei tre anni successivi all'entrata in vigore della normativa sui dati e, a medio termine, di introdurre un meccanismo di controllo sulle stesse[12].
La Commissione mira, attraverso le organizzazioni di standardizzazione europee, a fornire un nuovo quadro di interoperabilità per lo sviluppo di spazi dati europei comuni. Ciò è fatto con l'obiettivo di andare oltre l'approccio iniziale del Regolamento generale sulla protezione dei dati (GDPR) dell'UE alla portabilità dei dati personali estendendone la portata ai dati non personali. Tale ampliamento era precedentemente ostacolato dalla mancanza di importanti specificazioni tecniche – basti pensare alle API (Application programming interfaces) – e dal linguaggio giuridico che prevedeva l'interoperabilità «solo laddove tecnicamente fattibile»[13].
Tali requisiti tecnici, invero, sono rivolti principalmente agli operatori di spazi di archiviazione dei dati e ai fornitori di cloud computing i quali saranno obbligati a consentire la portabilità dei dati degli utenti e la commutabilità tra i servizi digitali.
Infine, il capitolo VII del Data Act tratta il tema del trasferimento transfrontaliero di dati non personali. L'art. 27 obbliga i fornitori di cloud computing ad adottare tutte le misure tecniche, legali ed organizzative ragionevoli, compresi gli accordi contrattuali, per «impedire il trasferimento internazionale o l'accesso governativo a dati non personali detenuti nell'Unione, laddove tale trasferimento o accesso creerebbe un conflitto con il diritto dell'Unione [...]».
Ciò significa che la Commissione ha, a tal fine, il precipuo incarico di elaborare linee guida coerenti con le raccomandazioni del Comitato europeo per l'innovazione dei dati, istituito ai sensi del Data Governance Act (DGA; Regolamento UE 868/22, in vigore dal 24 settembre 2023)[14].
A livello pratico, le norme proposte per i trasferimenti internazionali di dati hanno importanti implicazioni per i fornitori di servizi cloud, date le forti limitazioni dell'UE all'accesso da parte di governi stranieri ai dati non personali archiviati intra Unione, a meno che in materia non vi siano specifici accordi internazionali, come i trattati di mutua assistenza giudiziaria. Sembra trattarsi di una risposta diretta alle precedenti controversie suscitate dal CLOUD Act statunitense del 2018, che prevede accordi esecutivi tra il governo degli Stati Uniti e le agenzie di polizia di paesi terzi al fine di garantire l'accesso reciproco ai dati detenuti dai providers cloud nei rispettivi territori. In assenza di accordi internazionali, il DA consente il trasferimento di dati ospitati dai fornitori di cloud computing se e solo se il paese terzo fornisce un livello equo di protezione al diritto dell'UE. Se tale condizione è soddisfatta, verrà trasmessa la quantità minima di dati ammissibile in risposta alla richiesta effettuata. Ciò è, d'altronde, perfettamente in linea con i regimi di trasferimento dei dati previsti nel GDPR per

[12] *Data Act*, art. 25.

[13] GDPR, considerando 68.

[14] Sul *Data Governance Act* si veda S. Tranquilli, *Il nuovo citoyen européen nell'epoca del Data governance act*, in *Digital Politics*, 1-2, 2022, 179 ss.

i dati personali e nel DGA per i dati non personali.
D'altro canto, sempre in questa direzione, è stata sostituita la direttiva NIS[15], ovvero il primo atto legislativo dell'UE sulla sicurezza informatica, con la direttiva NIS 2[16], proprio al fine di rispondere alle crescenti minacce poste dalla digitalizzazione e dall'ondata di attacchi informatici, rafforzando, al tempo stesso, la sicurezza nelle aziende e nelle catene di fornitura, semplificando gli obblighi di segnalazione ed introducendo misure di vigilanza e requisiti di applicazione più severi, tra cui sanzioni armonizzate in tutta l'UE.
Pertanto, le aziende identificate dagli Stati membri come operatori di servizi essenziali dovranno adottare misure di sicurezza appropriate ed informare le autorità nazionali competenti di incidenti gravi, ad esempio in ipotesi di fuga di dati. I principali fornitori di servizi digitali, come motori di ricerca, servizi di cloud computing e mercati online, dovranno rispettare i requisiti di cui alla direttiva.
Ad esempio, nei considerando 101 e 102 la direttiva NIS2 stabilisce un quadro per la notifica alle autorità nazionali e ai clienti interessati di qualsiasi incidente informatico che abbia un impatto significativo in termini di interruzione operativa, perdita finanziaria o danno fisico. In caso di incidente di tal fatta, le organizzazioni in questione saranno tenute a presentare un primo rapporto entro 24 ore – un onere che mette alla prova la loro tempestiva capacità di segnalazione – uno più dettagliato entro 72 ore ed una relazione finale entro un mese.
Relativamente al Digital Services Act (DSA), invece, i fornitori di servizi cloud sono inseriti tra i destinatari degli obblighi di due diligence.
Invero, nei Considerando n. 13 e n. 28 del DSA, il cloud computing è espressamente indicato come un servizio di intermediazione, ed ergo certamente incluso nel Framework. A seconda del concreto funzionamento del servizio cloud, le regole sulle esenzioni di responsabilità per i Cloud Service Providers sono le stesse dei fornitori di servizi di semplice conduzione, caching o hosting, che a loro volta sono pressoché identiche a quelle stabilite dalla direttiva 2000/31/CE. Apparentemente, l'unica vera modifica che il DSA introduce per il mondo del cloud computing sarebbe quella di aver reso incontrovertibile che il provider di tali servizi sia esonerato da responsabilità per ciò che i destinatari dei servizi (suoi clienti) compiono alle stesse condizioni e con le stesse eccezioni che già trovavano applicazione e che continuano ad applicarsi, a seconda dei casi, ai fornitori di servizi di semplice conduzione, di caching o di archiviazione delle informazioni.
Pertanto, per quanto riguarda il regime di responsabilità del fornitore di servizi Internet (ISP), i servizi cloud devono essere equiparati alle piattaforme online[17].

---

[15] Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi.

[16] Direttiva (UE) 2022/2555, entrata in vigore il 17 gennaio 2023, in Italia il 17 ottobre 2024.

[17] Il DSA si applica ad un'ampia gamma di fornitori di servizi di intermediazione che sono classificati in base (i) al tipo di servizio della società dell'informazione fornito e in base (ii) al rispettivo settore e/o dimensione, con particolare riferimento alle piattaforme digitali.

La responsabilità dell'ISP è esclusa qualora egli non sia effettivamente a conoscenza del fatto che l'attività (o l'informazione) del cliente o dell'utente sia illecita e, per quanto riguarda le azioni di risarcimento dei danni, non abbia contezza di fatti o circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione, sempre che l'ISP – non appena venga a conoscenza di tali fatti – agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso (c.d. rimozione tempestiva)[18].
In termini concreti, per beneficiare della limitazione di responsabilità, un Cloud Service Provider dovrà procedere in via subitanea alla rimozione delle informazioni o ad impedire l'accesso alle stesse non appena viene informato o viene a conoscenza delle attività illecite, nonché adottare misure organizzative e tecniche appropriate.
L'art. 16 del DSA richiede, difatti, agli ISP (inclusi, quindi, i fornitori di servizi cloud) di creare meccanismi che consentano agli utenti di segnalare la presenza di contenuti illegali sui propri servizi e di fornire spiegazioni sufficientemente precise ed adeguatamente motivate sulle ragioni per cui li ritengono illegali, una chiara indicazione della loro ubicazione, i propri dati identificativi e la conferma della loro convinzione, improntata al principio di buona fede, circa l'accuratezza e la completezza delle informazioni e delle dichiarazioni fornite.
Inoltre, tutti gli ISP devono notificare alla persona o all'ente che ha emesso la segnalazione la propria decisione in merito alle informazioni cui l'avviso si riferisce, fornendo indicazioni sulle possibilità di ricorso.
Infine, ai sensi dell'art. 18 del DSA, nella misura in cui si qualifica come fornitore di hosting, anche un Cloud Service Provider, se viene a conoscenza di informazioni che inducano a sospettare che sia stato commesso, sia in corso di commissione o possa essere commesso un reato che comporti una minaccia alla vita o alla sicurezza di una o più persone, deve informare senza indugio le autorità giudiziarie o di polizia, fornendo le informazioni disponibili. Sommando l'onere di far fronte al meccanismo di segnalazione ed azione disciplinato dall'art. 16 e la notifica dei presunti reati ai sensi dell'art. 18, sembra chiaro che l'unico modo per un ISP, al fine di essere conforme alle previsioni normative, è dotarsi di procedure appropriate, definendo ruoli e responsabilità.

4. Protezione dei dati personali affidati al *cloud* e GDPR

Un profilo di particolare rilevanza in materia di cloud computing riguarda la protezione dei dati personali. Si tratta di un concetto che si pone in inevitabile interrelazione con il tema della sostenibilità digitale, la quale, per essere effettiva, non può prescindere da una gestione responsabile di detti dati.
Sotto tale prospettiva, il modello cloud, che prevede il trasferimento di data, generando molto spesso una circolazione transfrontaliera degli stessi,

[18] R. Bocchini, *La responsabilità extracontrattuale del provider*, in R. Bocchini (a cura di), *Manuale di diritto privato dell'informatica*, Napoli, 2023, 533 ss.

presenta evidenti criticità in termini di applicazione della disciplina prevista dal GDPR.

Come è stato correttamente sottolineato[19], invero, il modello di distribuzione dei servizi IT è stato facilitato dalla velocità delle connessioni di rete e dalla possibilità di aggregare una quantità di potenza di calcolo, prima inimmaginabile, in enormi data center.

I fornitori di servizi cloud dispongono di data farm dislocate in varie parti del mondo, gestite secondo criteri di efficienza che implicano la mobilità dei dati archiviati nel cloud: questi dati, difatti, non risiedono stabilmente nello stesso server, ma vengono continuamente spostati da un server all'altro in base alla loro allocazione ottimale, in modo da ottenere una migliore gestione delle risorse IT.

Questo processo, tuttavia, può portare alla violazione della riservatezza non solo dei dati personali degli utenti, ma anche di interi database, ad esempio di operatori telefonici o di istituti di credito[20]. Ergo, nel caso in cui un cliente si avvalga di servizi di archiviazione dei dati sul cloud, i rischi di un attacco o di un accesso non autorizzato da parte di terzi aumenterebbero, soprattutto nel caso in cui il trasferimento dei dati avvenisse al di fuori dei confini europei.

L'esigenza di proteggere i dati personali richiede l'individuazione di un titolare del trattamento che sia responsabile per eventuali violazioni del Regolamento generale sulla protezione dei dati che devono ricevere protezione indipendentemente dal territorio degli Stati (art. 3 GDPR).

Il problema dell'effettiva applicazione della tutela si sposta quindi dalla difficoltà di imporre la norma legislativa a quella di individuare il titolare del trattamento, la cui identificazione non è sempre facile ed immediata.

In realtà, nella pratica, sembra esserci una certa distanza tra il titolare del trattamento ai sensi dell'art. 4(7) GDPR (solitamente l'azienda cliente che si affida ad un fornitore di servizi cloud) e il responsabile del trattamento ai sensi dell'art. 4(8) (il fornitore di servizi cloud): dato che il settore in questione è spesso caratterizzato dall'esternalizzazione dei servizi, in sostanza, più lunga è la "catena" del cloud, più difficile diventa per il titolare del trattamento garantire la conformità al GDPR.

La crescente adozione di architetture operative che prevedono la compartimentazione e la suddivisione delle funzioni relative al trattamento dei dati, con competenze integrate e concorrenti, vede, infatti, la presenza di una pluralità di titolari del trattamento e un'integrazione delle rispettive competenze, relegando spesso la funzione del titolare del trattamento ad un ruolo più formale che sostanziale. Quest'ultimo, nelle organizzazioni complesse, ha il compito di definire le finalità del trattamento ed è responsabile in caso di trattamento illecito, ma spesso è privo di effettivo potere di determinazione e controllo sulle modalità di trattamento delegate a terzi[21].

---

[19] A. Mantelero, *La privacy all'epoca dei big data*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1216.

[20] T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informazione e dell'informatica*, 36(39), 2021, 474.

[21] A. Mantelero, *GDPR tra novità e discontinuità – Gli autori del trattamento dati: titolare e responsabilità*, in *Giurisprudenza italiana*, 171(12), 2019, 2778.

Il flusso di dati risultante dalla fornitura di servizi di cloud computing può essere qualificato come un flusso tra due titolari autonomi del trattamento dei dati o tra un titolare del trattamento dei dati e un responsabile del trattamento dei dati. Nel primo caso, l'autonomia delle parti escluderebbe la responsabilità del cliente per qualsiasi illecito da parte del fornitore di servizi cloud; quando, d'altro canto, il fornitore del servizio cloud è considerato un autonomo titolare del trattamento, il cliente non avrebbe più alcuna funzione di gestione in relazione al trattamento dei dati effettuato tramite il servizio.

Si è molto dibattuto sulla qualificazione giuridica del fornitore, cioè se questa figura contrattuale possa essere ricondotta al ruolo di titolare o di responsabile del trattamento.

In virtù della natura dell'attività professionale esercitata dal fornitore di servizi cloud, la tesi maggioritaria tendeva ad attribuirgli la qualifica di responsabile del trattamento, cioè di soggetto giuridico incaricato, dal cliente, della conservazione dei dati, come se fosse una sorta di mandatario proprio in ragione della natura dell'attività espletata.

Al contrario, nelle relazioni business-to-business (B2B; i.e. commercio interaziendale), l'utente del cloud ha lo status di controller, cioè di titolare del trattamento dei dati.

Tuttavia, a ben vedere, la qualificazione del fornitore di servizi cloud come responsabile del trattamento non può essere riconosciuta a priori: ciò sembrerebbe dipendere dal margine di potere contrattuale riconosciuto all'utilizzatore del cloud in sede di predisposizione della regolamentazione contrattuale.

Difatti, è possibile ricorrere alla figura dei cosiddetti «contitolari del trattamento» prevista dall'art. 26 GDPR.

Il co-trattamento si realizza ogniqualvolta due o più titolari del trattamento determinino congiuntamente finalità e mezzi del trattamento: ciò è particolarmente opportuno per la gestione dei servizi di cloud computing dove può sussistere il rischio di confusione tra i vari ruoli[22].

Il GDPR è intervenuto in maniera molto marcata nella definizione degli obblighi a carico del fornitore, prevedendo agli articoli 28, 32 e 34 una serie di accorgimenti e misure di sicurezza tecniche e organizzative[23] che ciascun responsabile è tenuto ad adottare affinché i trattamenti offerti nell'erogazione del servizio possano soddisfare i requisiti dettati dal

[22] L. Valle-B. Russo-G. Bonzagni-D. Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE*, in *Contratto e Impresa Europa*, 18(1), 2018, 399.

[23] Le misure di sicurezza imposte dal GDPR includono: la pseudonimizzazione, la cifratura dei dati personali, la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza di sistemi e servizi in via permanente, la capacità di ripristinare la disponibilità e l'accesso ai dati in caso di interruzioni fisiche o tecniche. Su questo punto, il Gruppo di lavoro per la protezione dei dati dell'articolo 29 della direttiva 95/46/CE aveva già espresso il proprio parere nel 2010 (parere n. 3 del 2010) secondo cui era necessario adottare un processo volto all'adozione di misure giuridiche, organizzative e tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, volti anche a dimostrare che le operazioni di trattamento dei dati già effettuate erano state eseguite nel rispetto del Regolamento europeo sulla *privacy* allora vigente.

Regolamento stesso, al fine di garantire la massima tutela dei diritti degli interessati dal trattamento.
Il tema della protezione dei dati personali diventa, invero, ancora più complesso quando il titolare del trattamento, in quanto professionista-imprenditore, utilizza servizi cloud per archiviare dati personali di terze parti. Aziende e professionisti, infatti, si affidano sempre di più alla tecnologia cloud per gestire aspetti del proprio business, esternalizzando l'archiviazione di documenti contenenti dati, anche sensibili, sia dei propri partner commerciali e/o collaboratori subordinati, sia dei propri clienti.
In questo contesto, quindi, è il cliente professionale che, nella scelta di un determinato servizio tra quelli disponibili sul web, definisce autonomamente le modalità di gestione ed il regime di sicurezza a cui sottoporre le informazioni in suo possesso. Ivi, allora il titolare dovrà aver cura di acquisire il consenso del diretto interessato al trattamento, anche prima di affidare tali dati al responsabile o, ancora, ad eventuali sub-responsabili.
Ciò nonostante, se a livello teorico è facile dedurre che l'onere ricada sul titolare del trattamento, nella pratica potrebbe risultare difficoltoso per quest'ultimo predisporre documenti informativi completi da sottoporre al diretto interessato del trattamento, in assenza del supporto e della collaborazione del fornitore del servizio cloud.
Occorre inoltre rilevare che, sebbene sia stata riconosciuta la possibilità di istituire tali reti di sub-responsabili nei rapporti B2B, il GDPR, finalizzato alla tutela dei dati personali delle persone fisiche, ne pone principalmente la responsabilità sul titolare del trattamento o, nel contesto cloud, sul cliente professionale.
La norma può essere desunta da una lettura dell'art. 28(1) GDPR, che impone al titolare del trattamento l'obbligo di scegliere solo «responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato», a pena di responsabilità e/o corresponsabilità[24].
Per quanto riguarda, invece, il profilo sanzionatorio, l'art. 82 GDPR ha previsto due forme di responsabilità: una a carico del titolare del trattamento che risponde del danno cagionato dal suo trattamento in violazione del GDPR; l'altra a carico del responsabile che risponde del danno cagionato in caso di inosservanza degli obblighi previsti dal GDPR e ad esso specificatamente diretti o quando ha agito in modo non conforme o

[24] Sul punto, si veda la decisione dell'Autorità svedese per la protezione dei dati, dell'11 dicembre 2020, (disponibile online) che ha multato l'Università di Umeå di 550.000 corone svedesi per violazione delle normative sulla protezione dei dati. Nello specifico, tuttavia, non è stata imposta alcuna sanzione ai sensi del GDPR poiché gli eventi si erano verificati prima della sua entrata in vigore. L'Università di Umeå, tra le altre violazioni, avrebbe elaborato ed archiviato i dati personali, relativi alla vita sessuale e alla salute, dei suoi dipendenti nel servizio *cloud* di una nota azienda americana, senza designare un responsabile del trattamento appropriato. La decisione del Garante svedese della protezione dei dati appare rilevante in quanto segue le orme della nota sentenza *Schrems II* (CGUE, C-3111/18, 16 luglio 2020) sostenendo che il trasferimento di dati personali in un *cloud* situato negli Stati Uniti innescherebbe di per sé un rischio elevato per tali dati poiché gli interessati sarebbero limitati nella loro capacità di far valere i propri diritti.

contrario alle legittime istruzioni del titolare del trattamento[25].
In quest'ultima ipotesi, nei rapporti B2B in ambito cloud, il responsabile del trattamento è tenuto a risarcire i danni, anche non patrimoniali, subiti dall'interessato, oltre a rispondere delle eventuali sanzioni amministrative irrogate dalle competenti autorità di controllo.

5. Conclusioni e prospettive *pro futuro*

L'impressione che si ricava da queste premesse relative alle problematiche giuridiche del cloud, osservate attraverso il prisma privatistico, è quella di un tema che appare meritevole di ulteriori approfondimenti e analisi, data anche la rapidità dell'evoluzione tecnologica e legislativa.
Invero, oltre al ruolo svolto dalla normativa europea, sembrerebbe opportuno implementare uno schema contrattuale al fine di una migliore regolamentazione del cloud computing[26].
Dall'analisi della prassi commerciale emerge inoltre l'essenza di qualsiasi tipo di garanzia, l'esclusione di responsabilità per danni causati all'utente e la presenza di clausole limitative l'identificabilità dell'entità dei danni provocati dal fornitore del servizio cloud. La definizione del regime normativo, difatti, rappresenta un passaggio di fondamentale importanza: il provider è spesso localizzato oltre i confini nazionali, e i dati degli utenti vengono inviati, tramite la rete, a sistemi ubicati in Paesi il cui ordinamento giuridico prevede un regime di tutela della privacy inferiore rispetto a quello europeo.
È quindi necessario cercare di costruire una struttura negoziale equilibrata che consenta al cliente di avere maggiore certezza.
Poiché le soluzioni offerte nell'ambito del cloud computing sono rappresentate da un'ampia varietà di possibili modelli di servizio, combinazioni di tecnologie rese disponibili e software adottati, sarà necessario esplicitare nel contratto tutti i presupposti alla base della scelta della soluzione adottata e del fornitore del servizio.
Uno scenario alternativo o quantomeno concorrente, allora, potrebbe essere quello di ipotizzare una forma di "co-regolamentazione[27]", in cui le regole siano suggerite dal mercato (magari attraverso il contributo degli stakeholders del settore, come la Cloud Security Alliance, e degli studiosi del diritto delle nuove tecnologie) e condivise dalle autorità di settore, se-

[25] N. Busca, *Cloud computing e tutela della privacy nei rapporti commerciali B2B*, in *Studium juris*, 2020, 26(11), 1336.

[26] F. Trubiani, *I contratti di cloud computing: natura, contenuti e qualificazione giuridica*, in *Diritto dell'informazione e dell'informatica*, 38(2), 2022, 395 ss.

[27] Il termine "co-regolamentazione" è per sua natura ambiguo. L'espressione è spesso utilizzata come termine generico per riferirsi a forme di cooperazione tra mercato e autorità che sono strumentali al perseguimento di obiettivi regolatori. La co-regolamentazione è generalmente intesa come una forma di regolamentazione degli *stakeholder* che è promossa, indirizzata, guidata o controllata da una terza parte (sia essa un organismo ufficiale o un regolatore indipendente) solitamente dotata di poteri di scrutinio, controllo e, in alcuni casi, sanzionatori. Sul problema della co-regolamentazione si veda U. Malvagna-M. Rabitti, *Filiere produttive e Covid-19: tra rinegoziazione e co-regolamentazione*, in Nuovo diritto civile, 4(3), 2020, 369 ss.

condo lo schema del «circolo regolatorio»[28].
Si tratta, cioè, di un meccanismo che parte dal basso, dalla spinta regolativa del mercato, e introduce nel sistema delle regole – o quantomeno delle linee guida immediatamente operative – che possono poi, se necessario, essere prese in considerazione dal legislatore e tradotte in precetti normativi[29].
Nella letteratura americana, l'elaborazione di linee guida di best practice è vista come un modo positivo per regolamentare efficacemente tali rapporti contrattuali, in particolare per facilitare la portabilità dei dati nel cloud[30]: a ben vedere, i codici di condotta possono essere utili anche, più in generale, per definire meglio la politica del fornitore di servizi cloud in materia di conservazione dei dati personali degli utenti.
L'impressione attuale, ergo, è di trovarsi ancora di fronte, da un lato, ad un quadro normativo frammentato ed indefinito e, dall'altro, alla necessità di procedere alla costruzione di modelli contrattuali adeguati per il settore cloud: in questo senso, appare quindi centrale proprio il ruolo dell'interprete, chiamato ad inquadrare, nei termini suddetti, questi nuovi strumenti tecnologici in inevitabile contemperamento con istanze sociali certamente meritevoli di tutela.

[28] F. Bassan, *Potere dell'algoritmo e resistenza dei mercati in Italia*, Soveria Mannelli, 2019.

[29] D'altro canto, come ha sottolineato A. Zoppini, *Il diritto privato e i suoi confini*, Bologna, 2020, 28 ss., vi sono regole e principi (come quelli condivisi nel commercio internazionale) che si impongono nei rapporti privati con la loro stessa forza e che, in quanto riconosciuti e condivisi, svolgono una funzione normativa indipendentemente dalla loro adozione formale.

[30] K. Żok, *Cloud Computing Contracts as Contracts For The Supply Of Digital Content: Classification and Information Duty*, in *Masaryk University Journal of Law and Technology*, 13(2), 2019, 151.

Abstract

Nell'attuale contesto digitale sempre più innovativo e complesso, il presente lavoro si propone di analizzare, da un punto di vista strettamente civilistico, il tema dei servizi di cloud computing, soffermandosi in particolare sugli aspetti contrattuali ed indagando l'influsso della classificazione di tali servizi sul nostro ordinamento (con uno sguardo anche al ruolo riconosciuto al cloud computing all'interno del Piano Nazionale di Ripresa e Resilienza italiano) e la responsabilità (e i limiti della sua identificabilità) del fornitore di cloud services. Si cercherà, invero, di individuare i profili giuridici impattati dall'utilizzo di detti servizi, i quali richiedono un inevitabile ripensamento, ma non necessariamente in toto, delle categorie giuridiche tradizionali al fine di puntare ad una maggiore sostenibilità digitale (Agenda Digitale Europea 2030). Più specificamente, si analizzeranno, anche alla luce della legislazione europea (in special modo, del Digital Services Act, DSA, entrato pienamente in vigore il 17 febbraio 2024), le principali problematiche, con precipuo riferimento alla protezione dei dati personali affidati al cloud ed all'identità digitale, cercando di ipotizzare una chiave di lettura per proporre rinnovati modelli contrattuali che si traducano in accordi tra user e provider maggiormente improntati all'equilibrio inter partes e che assicurino al cliente maggiore certezza del rapporto anche in termini di riconoscimento giuridico della responsabilità (ed, ergo, di ammissibilità di clausole di esclusione della stessa) del fornitore di servizi cloud.

In the current increasingly innovative and complex digital context, this paper aims to analyze, from a civil law standpoint, the topic of cloud computing services, focusing in particular on the contractual aspects and investigating the influence of the classification of such services on our legal system (with a look also at the role recognized to cloud computing within the Italian National Recovery and Resilience Plan) and the responsibility (and the limits of its identifiability) of the cloud services provider. Indeed, it will try to identify the legal profiles impacted by the use of these services, which require an inevitable rethinking, but not necessarily in full, of traditional legal categories in order to aim for greater digital sustainability (European Digital Agenda 2030). More specifically, this research will analyze, also in light of European legislation (notably, the Digital Services Act, DSA, which came into force on February 17th, 2024), the main problems, with particular reference to the protection of personal data entrusted to the cloud and digital identity, trying to hypothesize a key to propose renewed contractual models which result into agreements between users and providers that are more oriented towards balance among parts and that ensure the customer greater certainty of the relationship also in terms of legal recognition of the liability (and, then, the admissibility of disclaimers) of the cloud service provider.

Keywords

cloud computing - sostenibilità digitale - Strategia Cloud Italia - digital policy europea - protezione dati personali

Minori e social media, tra norme e violazioni: i risultati di una ricerca empirica*

Mario D'Avino

Sommario

Introduzione. – 2. Contesto e scopo della ricerca. – 3. Metodologia e strumenti. - 4. Obiettivi prefissati. – 5 Analisi dei dati. – 6. Conclusioni.

1. Introduzione

Nell'era digitale, i concetti di diritti e privacy subiscono una profonda trasformazione, presentando sfide significative per la protezione dei minori. L'accesso aperto a un web illimitato, insieme alla scarsità di controlli, aumenta i rischi di cyberbullismo, una minaccia grave per la salute mentale dei giovani. Verranno esaminate le problematiche relative alla privacy dei minori e le misure preventive contro il cyberbullismo, suggerendo l'importanza del monitoraggio da parte di genitori e agenzie educative. Verranno discusse come le misure di parental control possano supportare questa protezione. Si approfondiranno i nuovi diritti online, come l'identità digitale e la libertà di espressione, alla luce di normative come il GDPR, evidenziando la necessità di un aggiornamento costante delle leggi in risposta all'evoluzione tecnologica. Lo studio proporrà un'analisi sul trattamento dei dati personali dei minori, evidenziando il delicato equilibrio tra libertà di circolazione dei dati e diritto alla privacy e sulle implicazioni legali del cyberbullismo, con particolare attenzione alle condotte lesive attraverso i social network. La parte conclusiva esplorerà l'impatto dei social media sulla vita sociale e psicologica dei giovani, basandosi su ricerche condotte in Campania.

Si sottolinea l'urgenza di garantire una protezione adeguata per i minori, attraverso l'implementazione di normative efficaci e programmi educativi che coinvolgano famiglie e scuole.

Le misure previste dalla Legge n. 71/2017, recentemente integrate e rafforzate dalla Legge n. 70 del 2024, offrono un quadro normativo più ampio e articolato per il contrasto al cyberbullismo e al bullismo. Quest'ultima introduce una definizione estesa dei fenomeni, promuove interventi educativi e formativi anche nei confronti dei responsabili, e istituisce un

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

tavolo tecnico interministeriale per il coordinamento delle azioni. Tuttavia, per affrontare efficacemente le sfide di un mondo digitale in continua evoluzione, è necessario un approccio integrato e collaborativo che coinvolga istituzioni, scuole, famiglie e società civile.

2. Contesto e scopo della ricerca

L'attività di indagine, intitolata Social media e giovani: esplorando il mondo digitale dei teenager**,** è stata condotta in un contesto scolastico, indirizzata agli studenti di scuola secondaria di primo e secondo grado della regione Campania. Nella società odierna l'uso dei social media è una delle attività più comuni tra gli adolescenti, tanto da diventare parte integrante della loro vita e contesto chiave in cui esprimono le principali sfide legate all'età. Negli ultimi dieci anni, infatti, i social network sono diventati uno dei mezzi di comunicazione più usati tra i ragazzi. Di conseguenza, le relazioni interpersonali hanno subìto grandi cambiamenti e diverso è il modo di comunicare degli adolescenti e di relazionarsi tra loro e con i genitori. La tradizionale socializzazione faccia a faccia è sempre più sostituita dai social network, che consentono l'interazione con l'altro senza la necessità della presenza fisica degli interlocutori. Considerando le trasformazioni sopraripportate, e visto che, per una buona socializzazione tra coetanei in adolescenza, le abilità sociali hanno un ruolo essenziale, è importante valutare l'impatto che l'uso dei social media può avere su queste abilità dei teenager. Pertanto, lo scopo di questa ricerca è quella di studiare il rapporto dei ragazzi con i social media per poterne identificare eventuali problematiche o criticità, punti negativi o positivi.

3. Metodologia e strumenti

Lo strumento di ricerca usato è il questionario costituito da una serie di domande che mirano a raccogliere informazioni in modo standardizzato attraverso la metodologia dell'indagine.
Il questionario, semi strutturato e in forma anonima, è ritenuto non solo lo strumento di misura più opportuno per raccogliere informazioni circa le variabili oggetto di ricerca, ma anche lo strumento di comunicazione più funzionale fra il ricercatore e il rispondente, Prima della somministrazione sono stati definiti ai partecipanti gli obiettivi e i temi di interesse per l'indagine, spiegando, inoltre, che i dati inseriti – coperti da anonimato – sarebbero stati usati esclusivamente per finalità di ricerca scientifica e non commerciali, e che i risultati sarebbero stati resi noti al termine del lavoro d'indagine. Il questionario è stato realizzato con Google Moduli e si compone di dodici domande, così suddivise:

- due inerenti agli aspetti anagrafici dello studente:
  - Età
  - Sesso

- una legata al grado di scuola:
  - Quale grado di scuola frequenti?

- Una relativa al tipo di social media utilizzato:
  - Istagram
  - Facebook
  - Snapchat
  - TikTok
  - Altro

- Una relativa alle norme di comportamento sui social media:
  - Conosci le norme di comportamento sui social media?

- Due relative ad eventuali messaggi minacciosi o spiacevoli ricevuti ed eventuale segnalazione:
  - Sai come segnalare un comportamento inappropriato sui social media?
  - Hai mai pubblicato o condiviso informazioni personali sui social media?

- Una relativa al cyberbullismo:
  - Sai cosa significa "cyberbullismo"?

- Due relative ai messaggi di insulto e conseguenze legali:
  - Hai mai insultato, minacciato o molestato qualcuno online?
  - Conosci le conseguenze legali delle violazioni delle norme sui social media?

- Tre riguardanti contenuti inappropriati ed eventuali comportamenti:
  - Cosa fai se incontri contenuti inappropriati sui social media?
  - Sai come segnalare un comportamento inappropriato sui social media?
  - Cosa fai se incontri contenuti inappropriati sui social media?

Le domande sono state strutturate sia a risposta multipla, con la possibilità di indicare una sola scelta tra quelle suggerite, sia a risposta aperta, per dar modo di esprimere liberamente e soggettivamente alcuni punti.

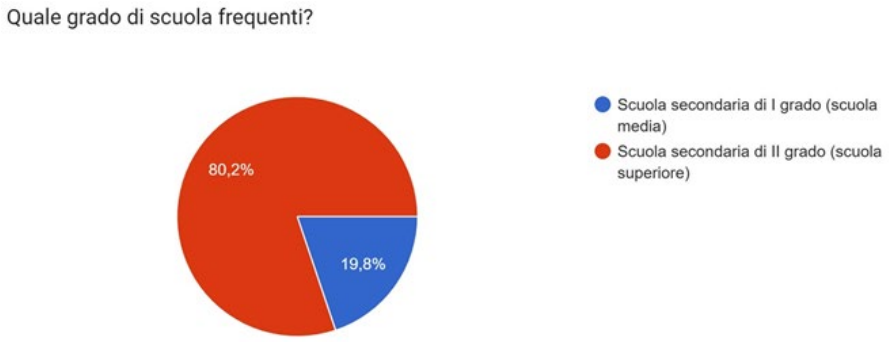
4. Obiettivi prefissati

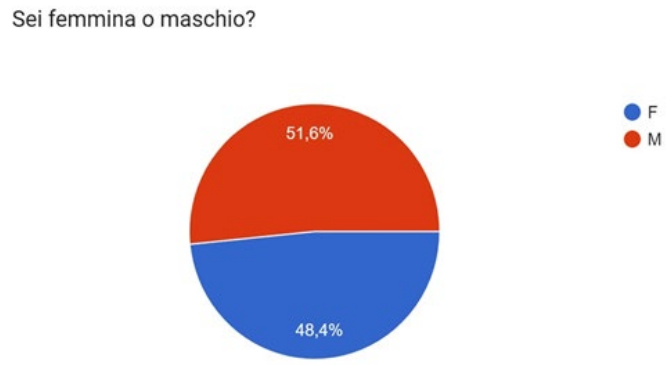
La ricerca è stata condotta con l'intento di analizzare determinate tematiche legate ai social media ed il modo in cui essi vengono considerati dagli studenti coinvolti. Come ogni cosa, infatti, anche i social hanno i loro pro e i propri contro: dall'aspetto della comunicazione all'azzeramento di tutte quelle occasioni casuali di interazione umane.
Il Questionario sui social media per i minori ha avuto come obiettivi principali:
1. Raccogliere informazioni sui comportamenti e sulle abitudini dei mi-

nori riguardo all'uso dei social media.
2. Valutare il livello di consapevolezza dei minori sui rischi e le potenziali minacce presenti sui social media.
3. Individuare le problematiche più comuni che i minori incontrano durante l'utilizzo dei social media.
4. Fornire indicazioni e consigli utili per proteggere i minori da contenuti inappropriati o pericolosi sui social media.
5. Promuovere una maggiore consapevolezza e responsabilità nell'uso dei social media tra i minori.

5. Analisi dei dati

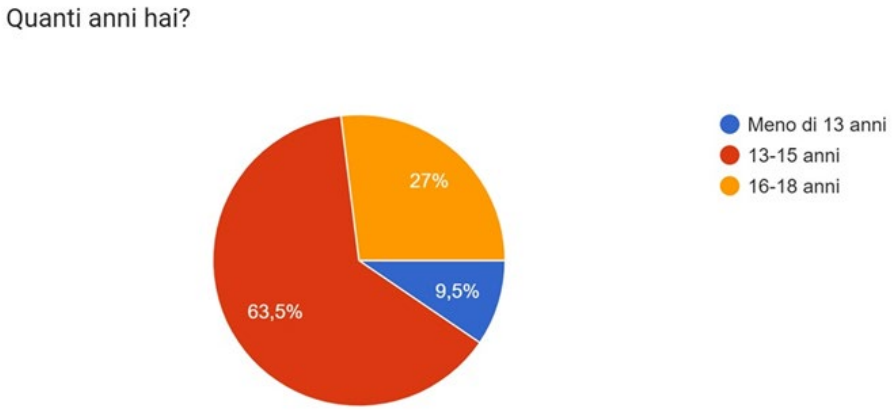
Le domande del Questionario intendevano approfondire gli aspetti relativi alla consapevolezza che i giovani hanno della rete virtuale.
Hanno aderito alla ricerca 1260 alunni di scuola secondaria di I e II grado di cui 1010 della scuola secondaria di secondo grado e 250 di scuola secondaria di primo grado, di cui 650 maschi, 610 femmine.





Le fasce di età degli studenti sono comprese tra i 16 e i 18 anni, pari a 340; 13 e i 15 anni, pari a 800; meno di 13, pari a 120.
Questa suddivisione delle fasce di età degli studenti che utilizzano i social network ci fa riflettere su diversi aspetti.
Innanzitutto, notiamo che la fascia di età più consistente tra gli utilizzatori di social network è quella compresa tra i 13 e i 15 anni, con ben 800 studenti. Questo dato fa emergere quanto i social network siano diventati parte integrante della vita dei ragazzi adolescenti, utilizzati intensamente per comunicare, condividere contenuti e restare in contatto con amici e coetanei.

Risulta interessante osservare un discreto numero di studenti di età inferiore ai 13 anni che utilizzano i social network, pari a 120. Questo dato indica l'importanza di educare i più giovani all'uso responsabile e consapevole di internet e dei social media, così da prevenire rischi legati alla privacy, alla sicurezza e all'adozione di comportamenti scorretti online.
Infine, la fascia di età compresa tra i 16 e i 18 anni, pari a 340 studenti, conferma l'utilizzo dei social network diffuso anche tra i "giovani adulti", che li utilizzano per diversi scopi, dalla comunicazione al networking, passando per la condivisione di interessi e la ricerca di informazioni.
In definitiva, la suddivisione delle fasce di età degli studenti che utilizzano i social network ci offre uno spaccato della realtà digitale in cui viviamo, evidenziando l'importanza di promuovere un approccio consapevole e responsabile all'uso dei mezzi digitali, sia tra i più giovani che tra gli adulti.



Per quanto riguarda l'utilizzo dei social media, si è rilevato che TikTok[1] è il social network più popolare tra gli studenti, con 530 studenti[2]; Istagram[3], è il secondo social network più utilizzato, con 520 studenti[4] che lo utilizza-

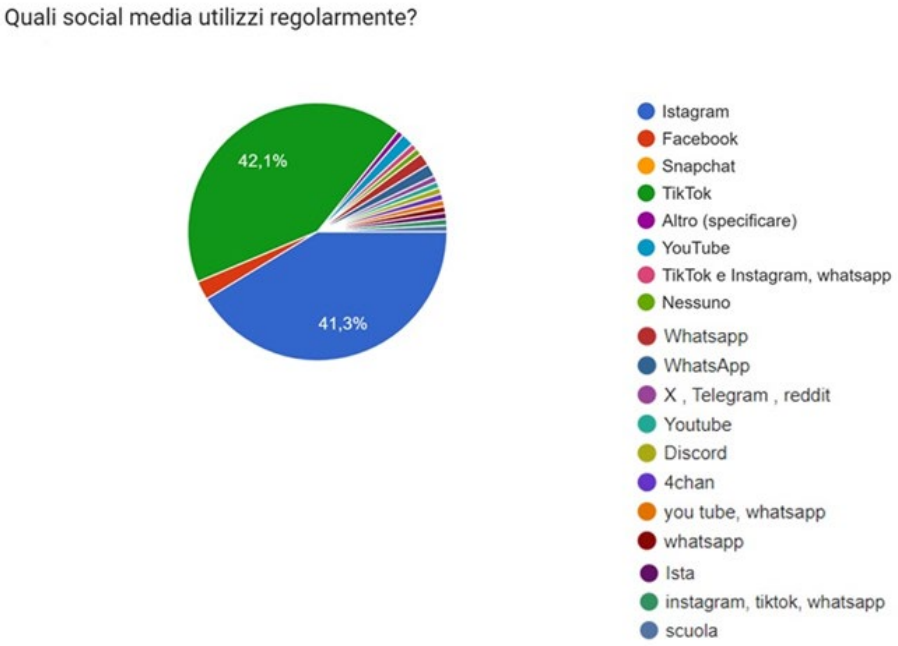
[1] TikTok è la piattaforma leader per i video brevi in mobilità. La nostra missione è ispirare creatività e portare buonumore. Le sedi centrali di TikTok si trovano a Los Angeles e Singapore. Inoltre TikTok dispone di uffici in altre sedi quali New York, Londra, Dublino, Parigi, Berlino, Dubai, Giacarta, Seul e Tokyo. (Fonte: sito ufficiale tiktok.com)

[2] Dalle Condizioni generali Tik Tok. Aggiornato ad agosto 2023, è precisata l'età minima al punto 4.3 Per utilizzare la Piattaforma, gli utenti devono avere almeno 13 anni. Effettuiamo dei controlli per assicurare il rispetto dei limiti d'età e, in caso di ragionevoli sospetti, disponiamo la chiusura del profilo degli utenti che hanno meno di 13 anni o che consentono a utenti di età inferiore ai 13 anni di usare il loro profilo. La nostra decisione di disporre la chiusura del profilo per una violazione dei limiti d'età può essere contestata laddove si ritenga che vi sia stato un errore.

[3] Instagram è un servizio di rete sociale statunitense che permette agli utenti di scattare foto, applicarvi filtri e condividerle via Internet. Nel 2012 Facebook, Inc. la acquistò per 1 miliardo di dollari. L'applicazione web, sviluppata da Kevin Systrom e Mike Krieger, è stata lanciata il 6 ottobre 2010.

[4] All'apertura dell'apposita sezione "*about*" del sito Instagram (about.instagram.com), troviamo il messaggio: "Continuiamo ad impegnarci per rendere Instagram un ambiente più sicuro per i membri più giovani della nostra community. Anche in questo caso tra le varie norme e indicazioni viene specificato che l'età minima obbligatoria per poter utilizzare Instagram è di 13 anni e da tempo ormai chiediamo ai nuovi utenti di indicare la propria età quando si registrano per un account. Anche se molte persone sono oneste nel

no; Facebook è utilizzato solo da 30 studenti, il che indica una diminuzione della popolarità tra gli studenti.
Gli altri studenti si distribuiscono tra X, Telegram, Youtube, Reddit, Whatsapp, Discord e 4Chan, con una percentuale inferiore.
Ciò rispecchia appieno la situazione odierna, infatti molte applicazioni sono passate in secondo piano, si pensi al boom iniziale di Facebook, ormai utilizzato da una percentuale bassa di adolescenti contraddistinta dal 2,4 %.
I teenager italiani utilizzano principalmente Instagram e TikTok perché sono piattaforme popolari tra la loro generazione e offrono un modo facile e divertente per esprimersi, connettersi con gli amici, scoprire nuove tendenze e seguire i propri influencer preferiti. Inoltre, entrambe le piattaforme offrono una vasta gamma di strumenti creativi e opzioni di personalizzazione che consentono loro di creare contenuti unici e coinvolgenti. Questo rende Instagram e TikTok particolarmente attraenti per i teenager che cercano di esprimere la propria creatività e di condividere il proprio mondo con gli altri.



I successivi grafici ci illustrano la consapevolezza che gli studenti hanno nei confronti delle norme di comportamento sui social media (1140 su 120 alunni dichiara di conoscere le norme di comportamento), e le conseguenze legali delle eventuali violazioni delle stesse (1150 su 210 alunni dichiara di conoscere le conseguenze legali). Va evidenziato come una percentuale, se pur minima ha in qualche modo violato le norme di comportamento,

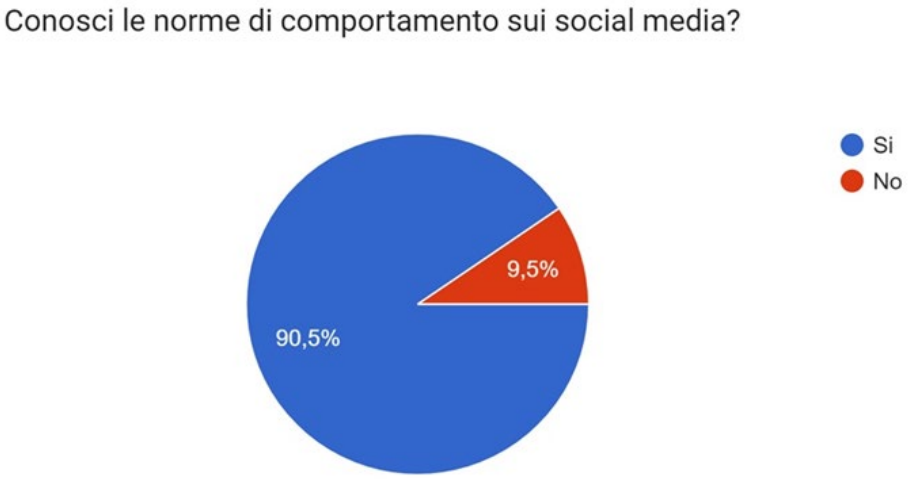
fornire questo dato, siamo consapevoli che spesso i giovani mentono sulla propria data di nascita. Vogliamo fare di più per evitare che questo accada. Sappiamo purtroppo che la verifica dell'età online è complicata ed è un tema che molte aziende nel nostro settore stanno affrontando. Per rispondere a questa sfida, stiamo sviluppando nuove tecnologie di intelligenza artificiale e apprendimento automatico che possano aiutarci a garantire la sicurezza degli adolescenti e ad applicare nuove funzioni appropriate per l'età.

infatti alla domanda: Hai mai insultato, minacciato o molestato qualcuno online, 170 studenti su 1090 ha risposto positivamente. È importante comunicare, ascoltare e favorire la partecipazione, il confronto e il dialogo con gli studenti da parte dei docenti, in un'ottica di condivisione degli aspetti legati ai comportamenti errati utilizzati dai ragazzi inconsapevoli delle conseguenze legali. Negli ultimi anni sono sempre più spesso attivi progetti realizzati con le scuole e gli uffici scolastici regionali in collaborazione con le forze dell'ordine per sensibilizzare i giovani studenti all'utilizzo consapevole dei media.

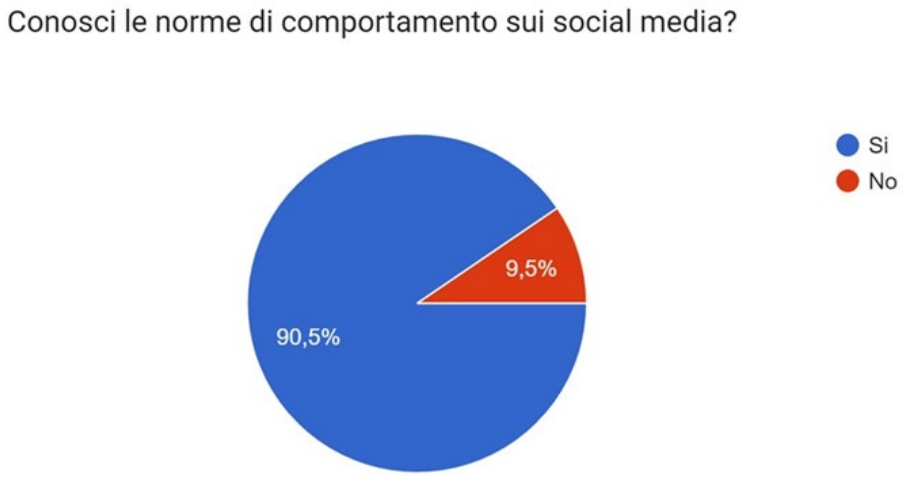
Un esempio è la Campagna Itinerante di educazione alla legalità "Una Vita da Social" progetto educativa itinerante della Polizia di Stato e del Ministero dell'Istruzione nell'ambito del progetto "Generazioni Connesse". Un tour con oltre 70 tappe sul territorio nazionale sui temi dei social network e del cyberbullismo, curati dal personale del Servizio di Polizia Stradale e Postale, unitamente al personale di altri Compartimenti.

Il mezzo multimediale, che gira nelle varie città d'Italia prevede attività formativa/informativa, diretta a studenti, insegnanti delle scuole di primo e secondo grado sui rischi e pericoli della rete Internet con particolare riguardo all'uso consapevole dei social network.

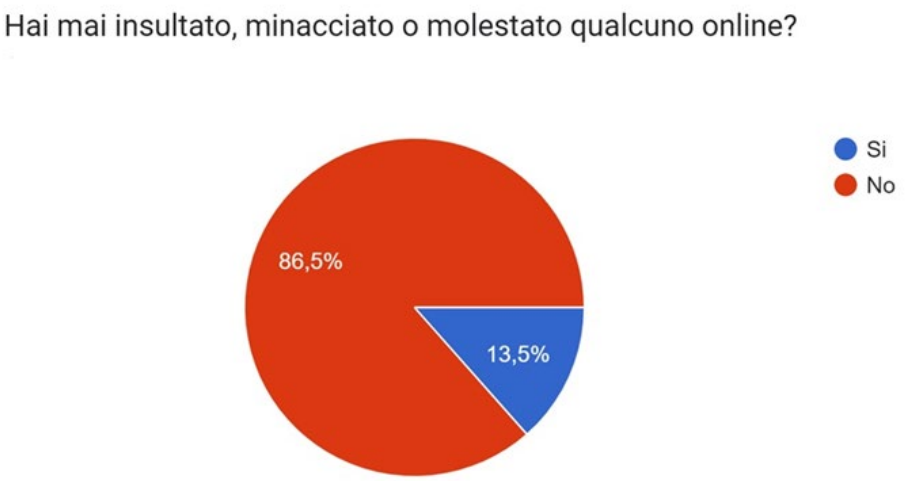
Vengono curati ed approfonditi altresì i temi della sicurezza stradale nonchè dei reati a sfondo discriminatorio, di consapevolezza e tutela dei diritti umani con personale specializzato della Polizia Stradale e dell'Osservatorio per la Sicurezza Contro gli Atti Discriminatori della Direzione Centrale della Polizia Criminale.[5]



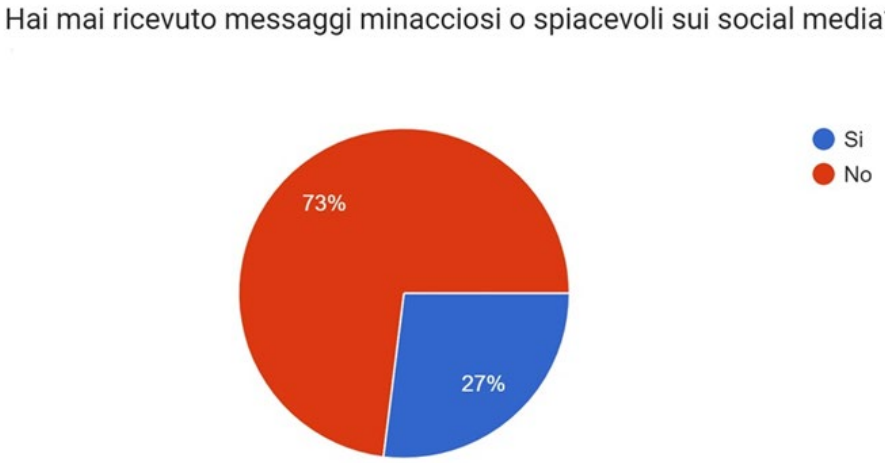
[5] Fonte: Ministero dell'Istruzione e del Merito.



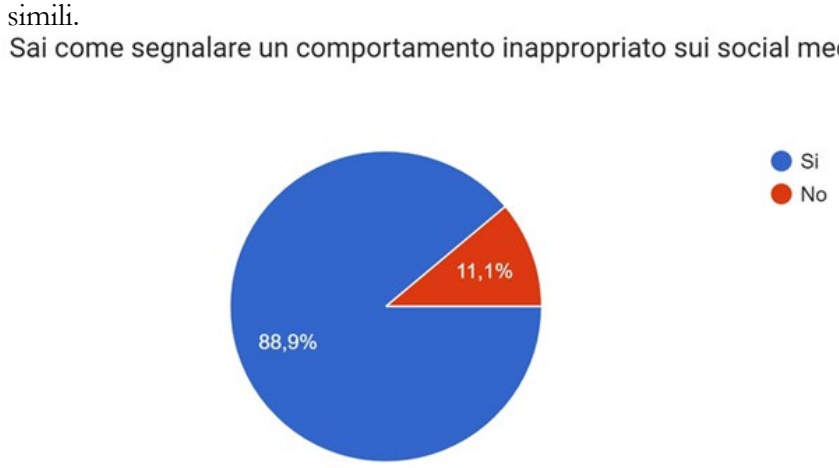
Secondo i dati, il 13,5% degli alunni ha ammesso di aver insultato, minacciato o molestato qualcuno online. Questo tipo di comportamento è molto preoccupante e può avere gravi conseguenze per le vittime coinvolte. È importante sensibilizzare gli studenti sui rischi e sulle conseguenze delle azioni online e promuovere un uso responsabile e rispettoso della tecnologia.
Invece l'86,5% non ha mai insultato, minacciato o molestato nessuno online. Questo dato suggerisce che la maggior parte degli studenti si comporta



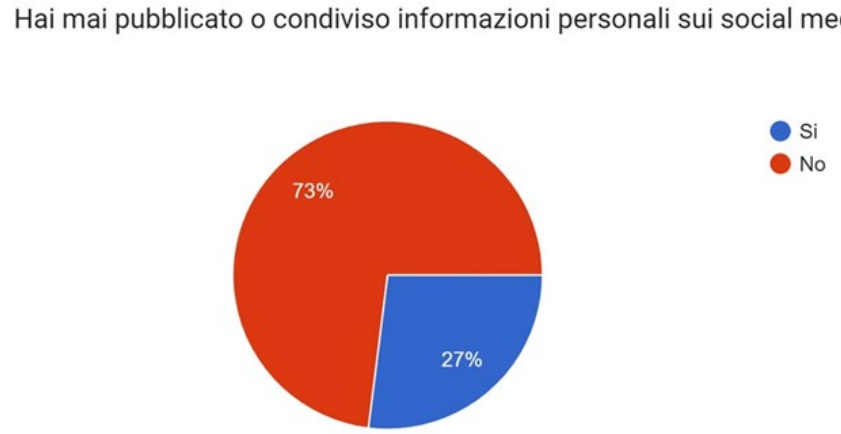
in modo rispettoso e civile sulle piattaforme digitali.
Le risposte degli studenti coinvolti nella somministrazione del Questionario hanno determinato che, mentre il 27% ha dichiarato di aver ricevuto almeno una volta messaggi minacciosi o spiacevoli. Questi dati indicano che la maggior parte degli studenti non è vittima di cyberbullismo, ma c'è comunque una percentuale significativa di giovani che si trova ad affrontare situazioni di questo genere online. È importante sensibilizzare sul tema e promuovere comportamenti rispettosi e sicuri sui social media.



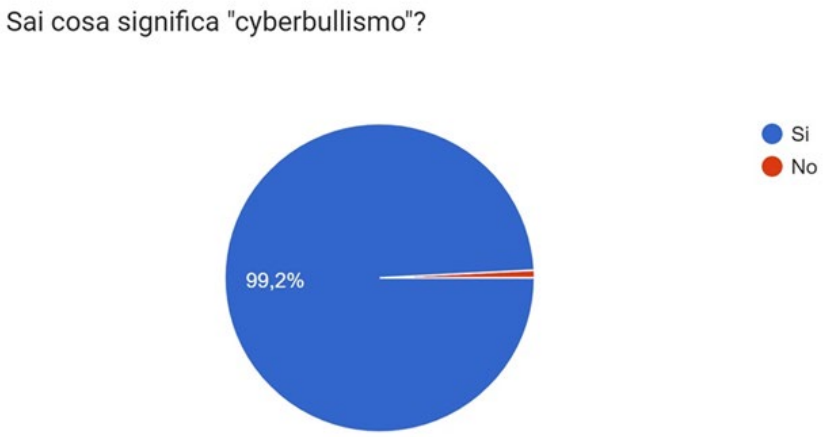
Un dato positivo, del grafico successivo, rileva che la maggior parte degli studenti conosce come segnalare un comportamento inappropriato sui social media. Questo dimostra che c'è una consapevolezza crescente sull'importanza di garantire un ambiente online sicuro e rispettoso. Tuttavia, è importante continuare a educare e sensibilizzare gli studenti su queste tematiche per garantire che tutti sappiano come agire in caso di situazioni simili.



Il 27 % degli studenti ha condiviso o pubblicato informazioni personali sui social network, come ad esempio foto, video, pensieri o dettagli sulla propria vita privata. Questo comportamento espone gli studenti al rischio di privacy e sicurezza online, poiché queste informazioni potrebbero essere facilmente condivise con persone non autorizzate o utilizzate in modo dannoso. È importante che gli studenti siano consapevoli dei rischi e delle conseguenze di condividere troppo di sé stessi online e che adottino misure per proteggere la propria privacy e sicurezza.



Solo 10 alunni su 1250 non conosce il termine cyberbullismo, questo indica che la maggior parte degli studenti è consapevole del fenomeno e delle conseguenze negative che può avere sull'individuo che ne è vittima. Tuttavia, c'è ancora un numero significativo di studenti che non sono consapevoli del fenomeno del cyberbullismo e dei suoi pericoli. Ciò sottolinea l'importanza di continuare a sensibilizzare e educare i giovani su come riconoscere e affrontare il cyberbullismo, così come promuovere comportamenti rispettosi e positivi online.



Come già ampiamente discusso, tra i molteplici strumenti previsti dalla Legge n. 71 del 2017 per contrastare il cyberbullismo, spicca la possibilità per il minore vittima di abusi di agire personalmente. Tale facoltà, disciplinata dall'articolo 2 della legge, intitolato 'Protezione della dignità del minore', rappresenta uno dei pilastri fondamentali dell'intero impianto normativo. Con l'entrata in vigore della Legge n. 70 del 2024, questa disposizione è stata ulteriormente valorizzata e integrata in un quadro più ampio di prevenzione e tutela, che include anche misure educative e rieducative rivolte ai minori responsabili di condotte illecite, nonché il potenziamento del ruolo delle famiglie e delle istituzioni scolastiche nella promozione di un uso consapevole delle tecnologie digitali.
In base ai risultati della ricerca condotta su un campione di 1260 studenti di scuola secondaria di primo e secondo grado della Campania, si possono trarre diverse conclusioni sul rapporto tra i giovani e i social media.

Alcuni aspetti importanti emergono dalla ricerca che va sicuramente approfondita con una più accurata analisi e magari diffusione in altri territori scolastici:
un utilizzo diffuso dei social media: la stragrande maggioranza degli studenti intervistati utilizza regolarmente i social media come Facebook, Instagram, Snapchat e TikTok. Questo conferma che i social media sono ormai parte integrante della vita quotidiana dei teenager. Andrebbero appurate quante ore vengono trascorse al giorno sui social media, al fine di considerare un potenziale rischio di dipendenza da queste piattaforme digitali.
Un impatto sulla vita sociale: I social media influenzano notevolmente le relazioni sociali tra i giovani, anche se non necessariamente in modo negativo. Possono facilitare la comunicazione e la condivisione di esperienze, ma allo stesso tempo possono causare isolamento e alimentare conflitti tra pari. Su questo punto sarebbe interessante valutare in che modo gli studenti possono essere influenzati dalle figure degli influencer sui social media, spesso imitandone i comportamenti e gli stili di vita.
In conclusione, i social media rappresentano uno strumento potente e pervasivo nella vita dei teenager, che può avere effetti sia positivi che negativi sulla loro salute mentale, il loro benessere e le loro relazioni sociali. È importante sensibilizzare i giovani sull'uso consapevole dei social media e promuovere un equilibrio tra la vita online e offline.

5. Conclusioni

È chiaro che i nuovi diritti dell'era online rappresentano una sfida importante per la società moderna. La protezione dell'identità digitale, la libertà di espressione online e il diritto alla reputazione sono temi cruciali che devono essere affrontati con attenzione e cautela. Inoltre, la questione della privacy e della protezione dei dati personali è diventata sempre più rilevante con l'avvento dell'intelligenza artificiale. È essenziale trovare un equilibrio tra l'utilizzo dell'IA per migliorare la vita delle persone e la necessità di tutelare i diritti individuali. Il Regolamento GDPR rappresenta un importante passo avanti nella protezione della privacy, ma è chiaro che ci sono ancora molte sfide da affrontare. È fondamentale che la normativa venga costantemente aggiornata per garantire una tutela efficace dei diritti individuali nella società digitale in continua evoluzione.
Il rapporto del minore con il web è oggetto di grande attenzione e approfondimento. Le normative europee e nazionali, seppur non sempre esplicite, forniscono un quadro normativo che mira a proteggere i minori dai rischi connessi all'utilizzo del web. Tuttavia, rimangono ancora molte questioni aperte e dubbi riguardo all'applicazione e all'interpretazione di tali norme, specialmente in contesti come il consenso dei minori al trattamento dei propri dati personali e la responsabilità degli amministratori di social network e siti web.
È necessario continuare a lavorare per garantire una maggiore protezione dei minori nel contesto digitale, migliorando le legislazioni esistenti e promuovendo azioni concrete contro il cyberbullismo e gli abusi online. Solo

attraverso un impegno comune tra istituzioni, genitori, educatori e operatori del settore sarà possibile assicurare un ambiente sicuro per i minori su internet e promuovere una cultura digitale responsabile e consapevole.
Le misure per contrastare il cyberbullismo previste dalla Legge n. 71/2017 offrono strumenti importanti, come la possibilità per le vittime di richiedere l'oscuramento dei contenuti dannosi online e la responsabilità dei genitori nel monitorare l'uso dei social network da parte dei propri figli. Tuttavia, con l'entrata in vigore della Legge n. 70 del 2024, il legislatore ha introdotto un approccio più ampio e strutturato, che integra queste misure con azioni educative, rieducative e riparative, rivolte sia alle vittime sia ai minori autori di condotte illecite[6].
La nuova normativa prevede, tra l'altro:

- l'istituzione di un tavolo tecnico interministeriale per il coordinamento delle politiche di prevenzione e contrasto del bullismo e del cyberbullismo;
- l'obbligo per i genitori di orientare i figli a un uso corretto delle tecnologie digitali e di vigilare attivamente sul loro comportamento online;
- l'attivazione di progetti educativi personalizzati, anche per minori di età inferiore ai 14 anni, che includono attività di volontariato, laboratori creativi, sport e percorsi di mediazione penale minorile[7].

In questo contesto, la mediazione scolastica si configura come una strategia particolarmente efficace per gestire i conflitti tra studenti in modo costruttivo, promuovendo la valorizzazione della vittima, il recupero del bullo e un clima di rispetto reciproco all'interno delle istituzioni scolastiche. La Legge 70/2024 riconosce e valorizza tali pratiche, sottolineando l'importanza di formare adeguatamente i mediatori scolastici e di investire nelle risorse necessarie per garantire il successo di questi programmi.
Affrontare il cyberbullismo richiede dunque un approccio multidisciplinare e integrato, che coinvolga attivamente famiglie, scuole, istituzioni, forze dell'ordine e associazioni del territorio. Solo attraverso un impegno comune e una consapevolezza diffusa sarà possibile contrastare efficacemente questo fenomeno e tutelare il benessere dei minori.
Infine, la nuova legge sottolinea l'urgenza di azioni educative e di sensibilizzazione, affinché i giovani comprendano i rischi legati a un uso irresponsabile dei social media, come il cyberbullismo, le violazioni della privacy e i comportamenti inappropriati. Le scuole, in collaborazione con le forze dell'ordine e le organizzazioni del terzo settore, devono promuovere comportamenti rispettosi e sicuri online, fornendo supporto concreto alle vittime. È essenziale anche il coinvolgimento attivo di genitori ed educatori, affinché possano guidare i giovani verso un uso consapevole e responsabile delle tecnologie digitali.
Solo con un approccio olistico, educativo e collaborativo possiamo costruire un ambiente digitale sicuro e positivo per le nuove generazioni.

---

[6] Cfr. *normattiva.it*

[7] *Bullismo e cyberbullismo, dal 14 giugno entra in vigore la nuova legge. Interventi mirati per minori difficili: la strada della mediazione e dei progetti educativi*, in *orizzontescuola.it*, 10 giugno 2024.

Abstract

Nell'era digitale in cui viviamo, i diritti e la privacy dei minori stanno affrontando una rivoluzione senza precedenti. L'accesso illimitato al web, caratterizzato da scarse misure di controllo, presenta gravi sfide per la protezione della privacy e la prevenzione del cyberbullismo, un fenomeno che minaccia il benessere psicologico dei giovani. Questo capitolo analizza come tutelare la privacy dei minori, garantendo il loro diritto a un accesso sicuro a Internet e affrontando le problematiche legate al cyberbullismo, incluse le normative vigenti. Si approfondiscono i nuovi diritti digitali, l'importanza della protezione dell'identità personale, e le sfide poste dall'intelligenza artificiale in relazione al GDPR. Viene esaminata la necessità di un equilibrio tra la libertà di circolazione dei dati e la protezione dei minori, con un focus sulle normative europee e nazionali. Attraverso un'indagine condotta su studenti della Campania, si esplorano le dinamiche sociali e psicologiche legate all'uso dei social media. Il capitolo sottolinea l'importanza di un approccio integrato che coinvolga genitori, educatori e istituzioni nella lotta contro il cyberbullismo e nella promozione di una cultura digitale responsabile. Le misure legislative, come la legge n. 71/2017 e la legge n. 70 del 2024, offrono strumenti importanti, ma è fondamentale integrare tali normative con programmi educativi e di prevenzione. Solo attraverso un impegno collettivo sarà possibile creare un ambiente online sicuro e supportare il benessere dei minori nell'era digitale.

In the digital era we live in, the rights and privacy of minors are facing an unprecedented revolution. Unlimited access to the web, characterized by weak control measures, presents serious challenges for privacy protection and the prevention of cyberbullying, a phenomenon that threatens the psychological well-being of young people. This chapter analyzes how to safeguard minors' privacy while ensuring their right to safe internet access and addressing issues related to cyberbullying, including existing regulations. It delves into new digital rights, the importance of protecting personal identity, and the challenges posed by artificial intelligence in relation to GDPR. The need for a balance between the free circulation of data and the protection of minors is examined, with a focus on European and national regulations. Through a survey conducted among students in Campania, the social and psychological dynamics related to social media use are explored. The chapter emphasizes the importance of an integrated approach involving parents, educators, and institutions in the fight against cyberbullying and the promotion of responsible digital culture. Legislative measures, such as Law No. 71/2017 and No, 70 del 2024, provide essential tools, but it is crucial to integrate these regulations with educational and prevention programs. Only through collective commitment can a safe online environment be created and the well-being of minors supported in the digital age.

Keywords

Era digitale – cyberbullismo – privacy dei minori – prevenzione – consapevolezza

Elenco autori

Marco Bassini
assistant professor of Fundamental Rights and Artificial Intelligence, Tilburg University

Tobia Eugenio Boaro
allievo ordinario in Scienze giuridiche, Scuola Superiore Sant'Anna

Amalia Mariana Buzura
avvocato in Milano

Marina Caporale
professoressa associata di Diritto amministrativo, Università degli Studi di Modena e Reggio Emilia

Alice Civitella
dottoranda di ricerca in Scienze strategiche e giuridiche dell'innovazione per la difesa e la sicurezza, Università degli Studi di Torino - Centro Alti Studi per la Difesa

Mario D'Avino
professore a contratto, La Sapienza - Università di Roma; giudice onorario presso il Tribunale per i minorenni di Napoli

Giovanna De Carne
dottoranda di ricerca in Diritto internazionale, Università degli Studi di Bari "Aldo Moro"

Federica De Simone
ricercatrice di Diritto penale, Università degli Studi della Campania Luigi Vanvitelli

Isabella de Vivo
dottoranda in Storia dell'Europa, La Sapienza-Università di Roma

Luca di Majo
ricercatore di Istituzioni di diritto pubblico, Università degli Studi della Campania Luigi Vanvitelli

Massimo Durante
professore ordinario di Filosofia del diritto, Università di Torino

Aldo Franceschini
assegnista di ricerca in Diritto processuale penale, Università degli Studi di Napoli Federico II

Irene Kamara
assistant professor of Cybercrime Law and Human Rights, Tilburg University

Fabiana Magnolo
dottoranda di ricerca in Diritto internazionale, Università del Salento

Ugo Pagallo
professore ordinario di Filosofia del diritto, Università di Torino

Christian Pallante
dottorando di ricerca in Diritto e sicurezza, Università degli Studi di Foggia

Ludovica Paseri
assegnista di ricerca in Filosofia del diritto, Università di Torino

Eugenia Perrone
senior legal advisor, CDP Cassa Depositi e Prestiti

Filomena Pisconti
ricercatrice di Diritto penale, Università degli Studi di Bari "Aldo Moro"

Alessandro Rosanò
ricercatore di diritto dell'Unione europea, Università degli studi di Parma

Gabriele Rugani
assegnista di ricerca in Diritto pubblico comparato, Università di Pisa

Marianna Russo
ricercatrice in Diritto del lavoro, Università degli Studi della Campania Luigi Vanvitelli

Antonio Vertuccio
dottorando di ricerca in Internazionalizzazione dei sistemi giuridici e diritti fondamentali, Università degli Studi della Campania Luigi Vanvitelli

Pietro Villaschi
ricercatore di Diritto costituzionale e pubblico, Università degli Studi di Milano

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

media LAWS

ANNO 2025 - CODICE ISSN 2532-9146