1/2026 giugno

Rivista di diritto dei media

ISSN 2532-9146

DIRETTORE RESPONSABILE
Oreste Pollicino

DIRETTORI
Marco Bassini
Marina Castellaneta
Carlo Melzi d'Eril
Giulio Enea Vigevani

EDITORE
Carlo Melzi d'Eril

REDAZIONE
Cordinamento editoriale
Rebecca Bovatti (Università di Milano)
Martina Cazzaniga (Università di Milano-Bicocca)
Giulia Napoli (Università di Milano-Bicocca)

Componenti
Flavia Bavetta (Università Bocconi – Milano)
Amalia Mariana Buzura (Avvocato in Milano)
Teresa Catalano (Università di Bari)
Federico Ceci (Università di Bari)
Marco Cecili (Università di Firenze)
Francesca Di Gianni (Università di Bari)
Alessia Forte (Università di Milano)
Maria Galbusera (Università di Milano – Bicocca)
Giuseppe Gallo (Università di Messina)
Giovana Lopes (Tilburg University)
Matteo Monti (Università Bocconi – Milano)
Giuseppe Muto (Università Bocconi – Milano)
Andrea Palumbo (KU Leuven)
Federica Paolucci (Università Bocconi – Milano)
Stefania Rutigliano (Università di Bari)

SEDE
Studio legale Melzi d'Eril Vigevani
Via San Barnaba 32 - 20122 Milano
e-mail: redazione@rivistadidirittodeimedia.it

ANNO 2026 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

COMITATO SCIENTIFICO

Ernesto Apa
Avvocato in Roma

Fabio Basile
Università di Milano

Mirzia Bianca
Sapienza – Università di Roma

Raffaele Bifulco
LUISS Guido Carli

Francesca Biondi
Università di Milano

Carlo Blengino
Avvocato in Torino

Manfredi Bontempelli
Università di Milano

Elda Brogi
European University Institute

Giuseppe Busia
ANAC

Licia Califano
Università di Urbino, già GPDP

Angelo Marcello Cardani †
Università Bocconi, già AGCOM

Marta Cartabia
Università Bocconi

Corrado Caruso
Università di Bologna

Massimo Ceresa-Gastaldo
Università Bocconi

Adolfo Ceretti
Università di Milano – Bicocca

Marco Cuniberti
Università di Milano

Marilisa D'Amico
Università di Milano

Giuseppe De Marzo
Suprema Corte di Cassazione

Filippo Danovi
Università di Milano – Bicocca

Filippo Donati
Università di Firenze

Michele Faioli
Università Cattolica

Giusella Finocchiaro
Università di Bologna

Maurizio Fumogià
Suprema Corte di Cassazione

Alberto Maria Gambino
Università Europea

Gianluca Gardini
Università di Ferrara

Glauco Giostra
Sapienza – Università di Roma

Ottavio Grandinetti
Avvocato in Roma

Enrico Grosso
Università di Torino

Antonio Gullo
LUISS Guido Carli

Antonio Iannuzzi
Università Roma Tre

Simone Lonati
Università Bocconi

Nicola Lupo
LUISS Guido Carli

Enrico Maria Mancuso
Università Cattolica

Vittorio Manes
Università di Bologna

Michela Manetti
Università di Siena

Roberto Mastroianni
Università di Napoli "Federico II"

Alessandro Melchionda
Università di Trento

Luigi Montuori
GDPD

Donatella Morana
Università di Roma Tor Vergata

Antonio Nicita
LUMSA, già AGCOM

Marco Orofino
Università di Milano

Jlia Pasquali Cerioli
Università di Milano

Paolo Passaglia
Università di Pisa

Davide Petrini
Università di Torino

Vincenzo Pezzella
Suprema Corte di Cassazione

Marina Pietrangelo
ITTIG-CNR

Giovanni Pitruzzella
Corte costituzionale

Francesco Pizzetti
Università di Torino

Andrea Pugiotto
Università di Ferrara

Margherita Ramajoli
Università di Milano

Sofia Ranchordás
LUISS Guido Carli

Giorgio Resta
Università Roma Tre

Giovanni Maria Riccio
Università di Salerno

Gianpaolo Maria Ruotolo
Università di Foggia

Lucia Scaffardi
Università di Parma

Salvatore Scuto
Avvocato in Milano

Sergio Seminara
Università di Pavia

Salvatore Sica
Università di Salerno

Pietro Sirena
Università Bocconi

Bruno Tonoletti
Università di Pavia

Luisa Torchia
Università Roma Tre

Gianluca Varraso
Università Cattolica

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 Roma Tre

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE

Maria Romana Allegri
Sapienza – Università di Roma

Giulio Allevato
IE University

Benedetta Barbisan
Università di Macerata

Marco Bellezza
Dip. per la trasformazione digitale

Marco Biasi
Università di Milano

Daniela Bifulco
Corte di cassazione

Elena Bindi
Università di Siena

Paolo Bonetti
Università di Milano – Bicocca

Monica Bonini
Università di Milano – Bicocca

Fernando Bruno
AGCOM

Daniele Butturini
Università di Verona

Simone Calzolaio
Università di Macerata

Quirino Camerlengo
Università di Pavia

Nicola Canzian
Università di Milano – Bicocca

Marina Caporale
Università di Modena-Reggio Emilia

Andrea Cardone
Università di Firenze

Bruno Carotti
LUISS Guido Carli

Stefano Catalano
Università di Verona

Pier Giorgio Chiara
Università di Bologna

Salvatore Curreri
Università di Enna "Kore"

Monica Delsignore
Università di Milano – Bicocca

Giovanni De Gregorio
Católica Global School of Law

Giovanna De Minico
Università di Napoli "Federico II"

Federica De Simone
Università della Campania

Gabriele Della Morte
Università Cattolica

Luca Di Majo
Università della Campania

Federica Fabrizzi
Sapienza – Università di Roma

Fernanda Faini
Università Pegaso

Fabio Ferrari
Università di Verona

Roberto Flor
Università di Verona

Giulia Formici
Università di Parma

Federico Furlan
Università di Milano – Bicocca

Alessandra Galluccio
Università di Milano

Giovanni Battista Gallus
Avvocato in Cagliari

Emma Imparato
Università di Napoli "L'Orientale"

Elisabetta Lamarque
Università di Milano – Bicocca

Erik Longo
Università di Firenze

Valerio Lubello
Università Bocconi

Claudia Massa
Università di Napoli "Federico II"

Antonio Manganelli
Università di Siena

Paola Marsocci
Sapienza – Università di Roma

Claudio Martinelli
Università di Milano – Bicocca

Alberto Mattiacci
Sapienza – Università di Roma

Massimiliano Mezzanotte
Università di Teramo

Francesco Paolo Micozzi
Avvocato in Cagliari

Lorenzo Nannipieri
CNR-ITTIG

Costanza Nardocci
Università di Milano

Stefania Ninatti
Università di Milano – Bicocca

Piergiuseppe Otranto
Università di Bari

Omar Makimov Pallotta
Università di Macerata

Anna Papa
Università di Napoli "Parthenope"

Francesca Paruzzo
Università di Torino

Irene Pellizzone
Università di Milano

Sabrina Peron
Avvocato in Milano

Federico Gustavo Pizzetti
Università di Milano

Benedetto Ponti
Università di Perugia

Augusto Preta
International Institute of Communications

Federico Riboldi
Avvocato in Milano

Francesca Rosa
Università di Urbino

Marianna Russo
Università della Campania

Lucia Sciannella
Università di Teramo

Monica Alessia Senor
GDPD

Silvio Sonnati
Università Bocconi

Stefania Stefanelli
Università di Perugia

Giulia Tiberi
Università dell'Insubria

Luca Vanoni
Università di Milano

Scilla Vernile
Università di Milano – Bicocca

Pietro Villaschi
Università di Milano

Paolo Zicchittu
Università di Milano – Bicocca

INTERNATIONAL ADVISORY BOARD

Shulamit Almog
University of Haifa

Max Baumgart
Universität Luzern

Edoardo Celeste
Dublin City University

Agustina Del Campo
Center for Studies on Freedom of Expression and Access to Information

Elaine Fahey
City Law School, University of London

Irene Kamara
Tilburg University

Uta Kohl
University of Southampton

Krystyna Kowalik-Bańczyk
Tribunale dell'Unione europea

Michale Geist
University of Ottawa

Thomas Margoni
KU Leuven

Christopher Marsden
Monash University

Manuel D. Masseno
Instituto Politécnico de Beja

Dawn C. Nunziato
George Washington University

Miquel Pequera
Universitat Oberta de Catalunya

Marius Dragomir
Central European University

Andrej Savin
Copenhagen Business School

Bilyana Petkova
University of National and World Economy

Thomas Wischmeyer
Universität Bielefeld

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 pubblicati sulla *Rivista di diritto dei media* sono redatti dagli autori e concessi a titolo gratuito, senza oneri per gli stessi.
Tutti i contributi sono pubblicati sotto licenza "Creative Commons Attribuzione – Non commerciale 4.0 International (CC BY-NC 4.0)". La licenza consente la riproduzione, la distribuzione, la comunicazione al pubblico e la rielaborazione dei contenuti per scopi leciti e non commerciali, a condizione che sia adeguatamente attribuita la paternità dell'opera e indicata la fonte originale secondo i termini previsti dalla licenza.
Per quanto non espressamente disciplinato dalla licenza, restano applicabili le normative vigenti in materia di diritto d'autore e dei diritti connessi.
La rivista aderisce al *Code of Conduct and Best Practice Guidelines for Journal Editors* elaborato dal Committee on Publication Ethics (COPE).
La qualità e il rigore scientifico dei contributi sono garantiti mediante procedura di valutazione differenziate in relazione alla tipologia di contributi, come specificato nel Regolamento, che sono affidate a un comitato di esperti selezionati secondo criteri di competenza, rotazione e aggiornamento periodico.

The *Rivista di diritto dei media* was founded on the initiative of Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril, and Marco Bassini. The journal provides a forum for scholarly discussion on media law and brings together contributions from Italian and international scholars working in the field.
Contributions published in the journal are provided by their authors on a voluntary basis and are published without any fees or charges for authors.
All articles are published under a Creative Commons Attribution–NonCommercial 4.0 International (CC BY-NC 4.0) licence. This licence permits the reproduction, distribution, public communication, and adaptation of the material for lawful, non-commercial purposes, provided that appropriate credit is given to the author and the original source is clearly acknowledged in accordance with the terms of the licence. Matters not expressly governed by the licence remain subject to the applicable provisions of copyright law and related rights.
The journal follows the *Code of Conduct and Best Practice Guidelines for Journal Editors* developed by the Committee on Publication Ethics.
The quality and academic rigour of the journal's publications are ensured through editorial and peer-review procedures that vary depending on the type of submission, as specified in the journal's regulations. Submissions are assessed by a committee of experts selected on the basis of their expertise, with attention to rotation and periodic renewal.

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

1. "Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione e dei media, con una particolare attenzione all'impatto delle tecnologie emergenti. È facoltà della Direzione programmare la pubblicazione di numeri speciali di carattere monografico in aggiunta ai tre numeri annuali rilasciati con cadenza quadrimestrale.

2. Gli organi della rivista sono la Direzione, il Comitato scientifico, il Comitato degli esperti per la valutazione, l'International advisory board e la Redazione. L'elenco dei componenti dei predetti organi è pubblicato sul sito della rivista e su ogni fascicolo. L'elenco dei componenti del Comitato scientifico è sottoposto ad aggiornamento con cadenza quadriennale. L'elenco dei membri del Comitato degli esperti per la valutazione e dell'International advisory board è sottoposto ad aggiornamento con cadenza e annuale.

3. Ciascun numero della rivista si compone delle seguenti sezioni: "Saggi", "Note", "Cronache e commenti" e "Recensioni". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse (per esempio, "Editoriali").

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico. I contributi pubblicati nella sezione "Saggi" sono normalmente di lunghezza non inferiore alle 8.000 parole e non superiore alle 20.000 parole.

5. La sezione "Note" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere, oltre che a provvedimenti di autorità indipendenti con un impatto rilevante sulle tematiche della rivista. I contributi destinati alla sezione "Note" sono normalmente di lunghezza compresa tra le 4.000 e 10.000 parole.

6. La sezione "Cronache e commenti" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata. I contributi destinati alla sezione "Cronache" sono normalmente di lunghezza compresa tra le 2.000 e 10.000 parole.

7. La sezione "Recensioni" ospita segnalazioni e commenti relativi a opere monografiche o collettanee di recente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica redazione@rivistadidirittodeimedia.it, 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. Affinché ciascun contributo possa essere valutato preliminarmente dalla Direzione, l'autore deve inviare una versione conforme alle regole editoriali della rivista pubblicate sul sito, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri redazionali costituisce motivo di rigetto della proposta.

10. 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.

11. In caso di esito positivo, la Direzione procede ad assegnare il contributo alla sezione opportuna e a sottoporlo alla procedura di valutazione scientifica (c.d. "referaggio"). In caso di esito negativo (c.d. *"desk rejection"*), la Direzione informa l'autore del contributo del rigetto.

12. I contributi destinati alla sezione "Saggi" sono inviati alla valutazione, secondo il metodo del doppio cieco, di due revisori, di cui almeno uno scelto dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I contributi destinati alle sezioni "Note", "Cronache e commenti" e "Recensioni" sono sottoposti alla valutazione di un revisore anonimo, tendenzialmente scelto tra i membri del Comitato degli esperti per la valutazione nel rispetto dei criteri sopra ricordati. A discrezione della Direzione, i contributi in lingua straniera che presentano un taglio internazionale possono essere affidati alla valutazione di membri dell'International advisory board. 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.

13. I revisori formulano un giudizio del contributo sottoposto alla loro valutazione scegliendo tra quattro diverse opzioni: "contributo pubblicabile", quando il lavoro possa essere pubblicato nella sua veste attuale, senza necessità di revisioni anche minori; "contributo pubblicabile con revisioni non sostanziali", nel caso in cui il contributo sia ritenuto pubblicabile soltanto all'esito di alcune modifiche non impattanti sulla struttura e sul contenuto del lavoro e senza necessità di un'ulteriore valutazione; "contributo pubblicabile con revisioni sostanziali", nel caso in cui il contributo sia ritenuto pubblicabile sotto condizione di modifiche di rilevante entità che rendono necessario un nuovo giudizio da parte degli stessi revisori ovvero da parte di un revisore terzo; "contributo non pubblicabile", nel caso in cui il lavoro non presenti caratteristiche che lo rendano pubblicabile anche all'esito di eventuali modifiche sostanziali. In ogni caso, la Direzione ha facoltà di formulare un giudizio complessivo alla luce delle osservazioni preliminari da essa formulate in merito al contributo e in considerazione dell'esito delle procedure di valutazione, specialmente nel caso di giudizio divergente da parte di due revisori. È facoltà della Direzione, in caso di divergenze di giudizio, richiedere una terza valutazione ad altro esperto.

14. Una volta ricevuta comunicazione dell'esito della procedura di valutazione, in caso di giudizio positivo ovvero positivo subordinato a modifiche (sostanziali e non sostanziali), l'autore dovrà inviare una versione definitiva ed eventualmente aggiornata del contributo. Nel caso di giudizio positivo subordinato a revisioni non sostanziali, l'autore dovrà inviare il testo definitivo in modalità revisioni in modo da permettere l'individuazione delle modifiche apportate. In caso di giudizio positivo subordinato a revisioni sostanziali, l'autore dovrà inviare il testo definitivo in modalità revisioni e una scheda recante una dettagliata spiegazione delle modifiche effettuate rispetto a ciascuno dei rilievi formulati dai valutatori. Nel caso di valutazione negativa, non è consentito all'autore sottoporre nuovamente il contributo alla rivista.

15. Le valutazioni vengono archiviate dalla Redazione per almeno tre anni.

16. 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. Inoltre, la Direzione potrà eccezionalmente richiedere la valutazione di due revisori per contributi destinati alle sezioni "Note" e "Cronache e commenti".

17. La Direzione ha facoltà di disporre a suo insindacabile giudizio la pubblicazione in forma di anticipazioni di contributi che abbiano positivamente terminato la procedura di valutazione e siano stati inviati in versione definitiva dall'autore in anticipo sulla data prevista di pubblicazione del rispettivo numero. In ogni caso, l'invio del contributo e la valutazione positiva alla pubblicazione non costituiscono titolo per la pubblicazione dello stesso in forma di anticipazione, che è rimessa alla decisione della Direzione in base a fattori quali l'attualità del lavoro e i tempi di pubblicazione e lavorazione del numero in formazione.

Indice

Editoriale

15 La fabbrica dei reati inutili e la libertà di parola. Dai deepfake all'apologia mafiosa: l'eterno ritorno del diritto penale simbolico
Carlo Melzi d'Eril, Giulio Enea Vigevani

Saggi

20 Bridging UNCITRAL and EU AI Governance: A Normative Proposal for the Regulation of Automated Contracting
Sharmin N. Chougule, María Luisa Mena-Durán

59 Put the Genie Back in the Lamp? AI-Based Biometric Systems and Fundamental Rights Protection in the European Union Artificial Intelligence Act
Giulia Formici

103 L'ecosistema digitale europeo tra proclamazione assiologica ed effettività normativa
Raffaele Torino

133 I giganti digitali alla prova del pluralismo informativo e della tutela del *copyright*
Anna Chimenti, Elena Maioli Castriota Scanderbech

160 La governance della cibersicurezza nell'era digitale: una rilettura costituzionale globale
Omar Caramaschi

192 La governance della cybersecurity nell'era dell'intelligenza artificiale tra quadro normativo europeo e nazionale
Stefania Ardito

230 Ricerca medica, fascicolo sanitario elettronico e IA: la direzione della legislazione italiana
Vittorio Bachelet

256 Tra predizione e protezione dei dati: la pubblica amministrazione algoritmica al vaglio dei rischi e delle garanzie
Riccardo Merli

289 Un delicato equilibro di potere: le istituzioni religiose nella *governance* dei *social media*
Nico Tonti

313 Chiesa cattolica e cyberspazio: verso una nuova dimensione per l'esercizio della governance ecclesiale
Federico Gravino

Note a sentenza

352 *Tempus commissi delicti* del reato di omesso controllo *ex* art. 57 c.p.: tra natura istantanea ed effetti (potenzialmente) permanenti.
Federico Riboldi

358 Diritto di cronaca giudiziaria: obbligo di verifica degli sviluppi processuali al momento della pubblicazione
Marco Milani

Cronache

363 La Direttiva anti-SLAPP tra libertà di espressione, abuso del processo e tutela del pluralismo democratico
Carlo Melzi d'Eril

377 EU Enlargement: What Regulatory Landscape for Copyright and Artificial Intelligence?
Anna Vasylchenko

400 A Comparative Analysis of Regulatory Sandboxes: Models, Evolution, and Strategic Implications in the UAE and Singapore
Andrea Stazi, Riccardo Jovine

424 Riflessioni sull'evoluzione e sulla rilevanza del concetto di trasparenza algoritmica, dal GDPR all'Artificial Intelligence Act
Alessandro Oldani

448 *Best interest of the child* e *cyberspazio*: il fenomeno dello *sharenting* alla prova del diritto. Essere figli e genitori nell'epoca della sovraesposizione digitale
Marco Ciuro

Recensioni

482 Recensione a V. Pezzella, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca delle fake news, degli hate speeches e dell'intelligenza artificiale*
Rebecca Bovatti

485 Ricordo di Angelo Marcello Cardani
Oreste Pollicino

Table of contents

Editorial

15 **Manufacturing Needless Offences and Freedom of Expression: From Deepfakes to Mafia Apologia and the Eternal Return of Symbolic Criminal Law**
Carlo Melzi d'Eril, Giulio Enea Vigevani

Essays

20 **Bridging UNCITRAL and EU AI Governance: A Normative Proposal for the Regulation of Automated Contracting**
Sharmin N. Chougule, María Luisa Mena-Durán

59 **Put the Genie Back in the Lamp? AI-Based Biometric Systems and Fundamental Rights Protection in the European Union Artificial Intelligence Act**
Giulia Formici

103 **The European Digital Ecosystem: Values and Normative Effectiveness**
Raffaele Torino

133 **Digital Platforms and the Challenge of Safeguarding Information Pluralism and Copyright**
Anna Chimenti, Elena Maioli Castriota Scanderbech

160 **Cybersecurity Governance in the Digital Age: a Global Constitutional Reinterpretation**
Omar Caramaschi

192 **Cybersecurity Governance in the Age of Artificial Intelligence: The In-terplay Between European and National Legal Frameworks**
Stefania Ardito

230 **Medical Research, Electronic Health Records and Artificial Intelligence: The Direction of Italian Legislation**
Vittorio Bachelet

256 **Between Prediction and Data Protection: Risks and Safeguards in Algorithmic Public Administration**
Riccardo Merli

289 **A Tricky Balance of Power: Religious Institutions in Social Media Governance**
Nico Tonti

313 **The Catholic Church and Cyberspace: Towards a New Dimension for the Exercise of Ecclesial Governance**
Federico Gravino

Case notes

352 ***Tempus Commissi Delicti* of the Crime of Failure to Control Pursuant to Article 57 of the Italian Criminal Code: Between Instantaneous Nature and (Potentially) Permanent Effects**
Federico Riboldi

358 Judicial Reporting Privilege: The Duty to Verify Procedural Developments at the Time of Publication
Marco Milani

Comments

363 The Anti-SLAPP Directive between Freedom of Expression, Abuse of Process and Protection of Democratic Pluralism
Carlo Melzi d'Eril

377 EU Enlargement: What Regulatory Landscape for Copyright and Artificial Intelligence?
Anna Vasylchenko

400 A Comparative Analysis of Regulatory Sandboxes: Models, Evolution, and Strategic Implications in the UAE and Singapore
Andrea Stazi, Riccardo Jovine

424 The Evolution and Relevance of the Concept of Algorithmic Transparency, from the GDPR to the Artificial Intelligence Act
Alessandro Oldani

448 The Best Interest of the Child and Cyberspace: The Legal Challenges of the Sharenting Phenomenon. Being Children and Parents in the Age of Digital Overexposure
Marco Ciuro

Reviews

482 Book Review: V. Pezzella, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca delle fake news, degli hate speeches e dell'intelligenza artificiale*
Rebecca Bovatti

485 In Memoriam: Angelo Marcello Cardani
Oreste Pollicino

Editoriale

La fabbrica dei reati inutili e la libertà di parola. Dai *deepfake* all'apologia mafiosa: l'eterno ritorno del diritto penale simbolico

Carlo Melzi d'Eril, Giulio Enea Vigevani

Ogni stagione politica sembra voler lasciare il proprio marchio nel codice penale. Quella che stiamo vivendo è segnata dalla tendenza a trasformare ogni anche tenue allarme sociale in una nuova fattispecie incriminatrice. Non importa che l'ordinamento disponga già degli strumenti necessari; non importa che le nuove norme risultino vaghe, ridondanti o di dubbia utilità. Si costruiscono fattispecie sempre più simboliche, pensate per inseguire paure collettive, emergenze mediatiche o pulsioni identitarie. La recente introduzione del reato relativo ai contenuti alterati mediante intelligenza artificiale e il disegno di legge sull'apologia mafiosa ne offrono due esempi particolarmente luminosi.

Con la legge n. 132 del 2025, il legislatore ha introdotto l'art. 612 *quater* c.p., rubricato "Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale". La nuova fattispecie punisce con una sanzione detentiva non irrilevante, da uno a cinque anni, «chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità».

Tale delitto mira a contrastare i *deepfake* non consensuali, ovvero i falsi particolarmente simili alla realtà. L'elemento caratterizzante del delitto è l'uso di sistemi di intelligenza artificiale, apparentemente l'unico elemento che contraddistingue un illecito di cui l'ordinamento non sentiva davvero il bisogno. Infatti, qualunque condotta che, mediante sistemi di intelligenza artificiale, produca una rappresentazione falsa della realtà e leda beni giuridici costituzionalmente rilevanti poteva già integrare fattispecie incriminatrici esistenti.

Il caso che più di frequente possiamo immaginare è quello di un danno recato a un bene giuridico molto personale, come quello della reputazione. E la lesione della reputazione, mediante un messaggio falso ma all'appa-

renza vero, creato con i più recenti *software*, può senza alcun dubbio essere ricondotto alla tradizionale diffamazione. È oscura la ragione per cui è stata ritenuta doverosa l'introduzione di un delitto a sé stante, unicamente caratterizzato dalle modalità di consumazione. È altrettanto poco chiaro il motivo per cui la medesima offesa a un bene giuridico, sol perché realizzata con strumenti più sofisticati, debba determinare un verticale innalzamento di pena.

La nuova fattispecie sembra così costruita non a difesa di un autonomo bene giuridico da tutelare, ma attorno al semplice impiego di una tecnologia nuova. Pare infatti che il nuovo mezzo, sol perché inedito, sia ritenuto meritevole di una incriminazione "dedicata". Si penalizza qualunque danno creato con sistemi di AI, il che al di là della scarsa tassatività e precisione della fattispecie, lascia perplesso l'interprete, di fronte a un reato tutto "costruito" intorno alle modalità di realizzazione dell'offesa, senza che ciò risulti in alcun modo necessario.

L'impressione è che il ricorso all'intelligenza artificiale, solo perché finora sconosciuto, sia stato ritenuto sufficiente a giustificare l'ennesima nuova incriminazione, anche in assenza di reali lacune di tutela nell'ordinamento. In altri termini, l'intelligenza artificiale invece di essere lo strumento della condotta, si presenta come la ragione stessa dell'incriminazione.

Ma, come scrivevamo all'inizio, gli esempi scarsa perizia nella formulazione di nuove fattispecie si moltiplicano nel giro di breve tempo. Un altro caso, infatti, giace nelle commissioni di Palazzo Madama.

"Ora affronteremo i veri problemi della giustizia", prometteva la maggioranza dopo la sconfitta referendaria. E così la commissione Giustizia del Senato ha adottato una procedura accelerata per giungere all'approvazione di una legge che preveda l'introduzione dell'ennesimo reato di opinione, l'apologia della criminalità organizzata.

Lo schema è noto: si individua una questione seria, la fascinazione di molti, soprattutto giovani, per i modelli criminali, e si cerca di risolverla con la sola repressione penale, nella migliore delle ipotesi ingolfando l'ordinamento con un nuovo delitto.

Vale la pena riproporne quasi integralmente il testo oggi noto, tutto sommato breve, anche per consentire al lettore di assaporare la grave cacofonia delle scelte lessicali del legislatore, sulle quali non ci soffermeremo, essendovi ben altri e maggiori punti critici da sottolineare.

Il delitto punisce con la reclusione da sei mesi a tre anni e la multa da mille a diecimila euro chiunque «pubblicamente esalta principi, fatti o metodi propri della criminalità organizzata di tipo mafioso persone condannate per i reati di cui all'art. 416 *bis* o ne ripropone atti o comportamenti, con inequivocabile intento apologetico, con lo scopo di determinare un concreto pericolo di commettere reati simili». È previsto l'aumento di pena da un terzo alla metà se il fatto è commesso a mezzo stampa o «attraverso

strumenti telematici o informatici».
Il fatto illecito è descritto in modo talmente vago che non è facile visualizzare le condotte vietate. Uno sguardo alla relazione aiuta a comprendere l'obiettivo dei firmatari della proposta. Si vogliono punire i cosiddetti "inchini" davanti alle abitazioni dei boss durante processioni religiose, la celebrazione di funerali sfarzosi, la costruzione di monumenti, la diffusione di messaggi sulle piattaforme digitali. Ma soprattutto, a quanto è dato intendere, canzoni (e immaginiamo anche libri, film, serie televisive) che glorificano la malavita, figure o episodi a essa collegati. Fino alla esaltazione del «Matteo Messina Denaro *style*» (la citazione, assicuriamo, è testuale), ovvero la creazione della tendenza a indossare i capi d'abbigliamento del capo mafia al momento dell'arresto.
Questa fattispecie porta con sé una quantità tale di difetti da imbarazzare l'interprete che volesse elencarli tutti, lasciandolo confuso solo nella scelta da quale parte cominciare.
Anzitutto si criminalizza l'espressione di un'idea, impostazione che vorremmo davvero fosse superata in linea con l'impianto costituzionale, ma anche sovranazionale, in base al quale la libertà di espressione "copre" anche le espressioni urticanti, scioccanti o inquietanti, poiché una democrazia matura, come ci ostiniamo a credere sia la nostra, non deve temere nemmeno chi ne mette in discussione i fondamenti.
È, infatti, pericoloso in questa materia estendere l'ambito del penalmente rilevante, in quanto la inevitabile discrezionalità di giudizio che la contraddistingue rende nient'affatto complicato usare la criminalizzazione in funzioni censorie. Chi può davvero dire cosa sia l'apologia della mafia? Per di più inequivocabile? (Occam e il suo rasoio non abitano nella mente del nostro legislatore, e questo lo sappiamo).
Si dirà: il reato non punisce l'espressione che si limiti ad avere «inequivocabile intento apologetico», ma è necessario «lo scopo di determinare un concreto pericolo di commettere reati» di tipo mafioso. Il che però non dona concretezza al delitto, in quanto si sanziona l'intenzione, non la messa in pericolo del bene. L'arma violenta della pena, in altre parole, è puntata contro un comportamento che ha la consistenza di un ologramma.
Insomma, ci troviamo ancora una volta di fronte ad un uso insopportabilmente simbolico del diritto penale. Con una aggravante, però: in questo caso sembra davvero di assistere a un tentativo di autoassoluzione da parte dello Stato, o di resa mascherata. Il potere esecutivo e legislativo, incapace di realizzare un contesto civile in vera competizione con la subcultura delle consorterie, censura chi ne loda i contorni. Come ha ben scritto la professoressa Anna Sergi a commento di questo disegno di legge «è più rassicurante criminalizzare i sintomi che curare la malattia».
Resta un dato di fondo: in entrambi i casi il diritto penale viene utilizzato non come *extrema ratio*, ma come strumento simbolico di comunicazio-

ne politica: si punisce ciò che inquieta l'opinione pubblica, anche quando l'ordinamento dispone già degli strumenti necessari o quando il confine dell'illecito diventa inevitabilmente incerto. E ogni nuova incriminazione costruita per rassicurare il dibattito pubblico contribuisce un po' di più a erodere tassatività, offensività e libertà di espressione.

Di fronte a questi ennesimi esempi di bizzarria legislativa, verrebbe da dire (con… Luca Bizzarri) che i rappresentanti della maggioranza "non hanno un amico" che fermi loro la mano quando tentano di metterla all'ordinamento penale.

Saggi

Bridging UNCITRAL and EU AI Governance: A Normative Proposal for the Regulation of Automated Contracting*

Sharmin N. Chougule, María Luisa Mena-Durán

Table of contents

1. Introduction. – 2. The Expanding Role of AI in Contracting: Distinguishing AI-Assisted Formation from Automated Performance. – 3. UNCITRAL, European Legal Framework and Their Gaps. – 3.1 UNCITRAL Model Law and Automated Contracting. – 3.2 EU AI Act and other efforts. – 3.3 Wendehorst's 2024 Discussion Draft: Principles for AI in Contracting. – 3.4 Limitations in the ELI and Wendehorst Frameworks. –3.5 Other European Provisions impacting Contract Law and Consumer Protection. – 4. Common Law vs. Civil Law Approaches: Comparative Analysis: European Regulatory Initiatives vs. U.S. Common Law. – 5. Conclusion: Policy Considerations and Future Directions.

1. Introduction

The emergence of artificial intelligence in contractual processes challenges foundational principles of European private law, particularly those governing offer and acceptance, intention, attribution, and liability. Unlike traditional electronic contracting, which operates under deterministic systems that merely transmit predefined declarations of will, advanced AI systems increasingly participate in the formation and execution of contracts through autonomous decision-making, data-driven inference, and adaptive negotiation capabilities. This development raises substantive questions as to whether existing doctrines of consent and contractual responsibility suffice to regulate non-human agents that are capable of independently generating contractual terms or triggering contractual performance without direct human awareness.

The European Commission is currently debating whether to introduce de-

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

dicated regulation for automated contracting, weighing frameworks such as the UNCITRAL Model Law on Automated Contracting[1] against the potential need for a more EU-specific legal structure. The Commission is also analysing the EU-specific efforts like the European Law Institute (ELI) Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts ("ELI Guiding Principles")[2] and Professor Christiane Wendehorst's guiding principles ("Prof. Wendehorst's Principles").[3] These discussions underscore the complex interplay between technological innovation and legal certainty and reveal a regulatory and doctrinal gap, particularly regarding contract formation, liability, and enforcement. This paper explores these efforts and the evolving regulatory landscape for automated contracting, also drawing on insights from the recent 2025 Münster Colloquia on EU Law and the Digital Economy ("Münster Colloquia").[4] A brief comparative analysis of European and United States (U.S.) approaches to automated contracting is given to shed light on differences between civil[5] and common law countries.

This article argues that the European Union must adopt a hybrid regulatory model that, *de iure condito*, builds upon the principle of functional equivalence to recognise the validity of AI-generated contracts and, *de iure condendo*, introduces a differentiated liability regime allocating responsibility between the deployer and the developer of the AI system, together with mandatory transparency and human-oversight obligations to ensure accountability and trust. This model integrates and systematises elements drawn from UNCITRAL's Model Law, the ELI Guiding Principles, and the AI Act, while filling their respective gaps through a unified doctrinal and regulatory framework.

In order to develop this thesis, the article is structured as follows. Section 2 clarifies the conceptual foundations of artificial intelligence in contracting, by distinguishing between AI-assisted contract formation and

---

[1] United Nations Commission on International Trade Law (UNCITRAL), *UNCITRAL Model Law on Automated Contracting with Guide to Enactment*, New York, 2025, available at *un.org* (accessed 5 May 2025).

[2] European Law Institute (ELI), *Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts,* Vienna, 2025 (ISBN: 978-3-9505495-4-6.)

[3] C. Wendehorst, *Discussion Draft: Principles for AI in Contracting (Version 2.1)*, in *Journal of European Consumer and Market Law*, 1, 2024, 43 ss.

[4] Münster Colloquia on EU Law and the Digital Economy, *Conference on AI and Automated Contracting*, University of Münster, 9-10 January 2025, available at *jura.uni-muenster.de* (accessed 8 January 2025).

[5] On the prevalence of the civil-law tradition among EU Member States, see K. Zweigert – H. Kötz, *An Introduction to Comparative Law*, Oxford, 1998, 68 ss., noting that all continental EU jurisdictions belong to the civil-law family, with only Ireland and, partly, Cyprus following common-law traditions.

automated performance. Section 3 looks into UNCITRAL's Model Law and European efforts specific to automated contracting and limitations of these efforts. Section 4 makes a comparison between civil and common law jurisdictions to gauge if common law jurisdictions have an advantageous position. This paper then concludes with a synthesis of findings and implications for the future development of European contract law.

2. The Expanding Role of AI in Contracting: Distinguishing AI-Assisted Formation from Automated Performance

Automated contracting is no longer confined to theoretical discussions; it has permeated multiple industries, transforming transactional dynamics in finance, healthcare, real estate, supply chains, and legal services. AI-driven contract lifecycle management platforms such as KPMG's Cognitive Contract Management (CCM),[6] IBM Watson-integrated ContractPodAi,[7] and JPMorgan's COiN (Contract Intelligence)[8] system demonstrate the growing reliance on algorithmic tools and automated contracting for contract drafting, negotiation, compliance monitoring, and enforcement in our very own legal field. AI-powered tools like Juro,[9] Ironclad,[10] and Evisort[11] automate contract lifecycle management, while Kira Systems[12] and LawGeex[13] analyse agreements for risks and inconsistencies. DocuSign CLM[14] streamlines contract execution, and IBM Watson Contract

[6] KPMG, *Contract Transition in M&A: Accelerating Value with AI*, 2022, available at *kpmg.com* (accessed 31 January 2025).

[7] IBM, *Watson Discovery and ContractPodAi: Transforming Legal Excellence with AI*, 2023 available at *ibm.com* (Accessed 31 January 2025).

[8] Superior Data Science, *JP Morgan COiN: A Case Study of AI in Finance*, 2023, available at *superiordatascience.com* (Accessed 31 January 2025); Product Monk, *Meet COiN: JPMorgan's Efficiency Wizard*, 2023, available at *productmonk.io* (Accessed 31 January 2025).

[9] Juro, *AI-Powered Contract Automation for Businesses*, 2025, available at *juro.com* (accessed 31 January 2025).

[10] Ironclad, *Contract Lifecycle Management with AI*, 2025, available at *ironcladapp.com* (Accessed 31 January 2025).

[11] Evisort, *AI-Driven Contract Intelligence for Legal Teams*, 2025, available at *evisort.com* (accessed 31 January 2025).

[12] Kira Systems, *AI-Powered Contract Analysis for Risk Management*, 2025, available at *kirasystems.com* (Accessed 31 January 2025).

[13] LawGeex, *Automating Legal Contract Review with AI*, 2025, available at *lawgeex.com* (accessed 31 January 2025).

[14] DocuSign, *Contract Lifecycle Management (CLM) Solutions*, 2025, available at *docusign.com*

Analyzer[15] assists with due diligence and compliance. Despite these advancements, human oversight remains critical to ensuring contractual accuracy and mitigating algorithmic biases, while acknowledging the persistent risk of automation bias.[16] Also, the industry-specific applications of automated contracting and their implications for legal accountability may differ. The applications of automated contracting vary across industries, leading to different legal accountability challenges. For example, in finance, AI-driven contracts must comply with strict regulatory requirements, while in supply chains, they focus on efficiency and risk allocation. In healthcare, automated contracts must address patient data protection and liability concerns. These differences affect how legal responsibility is assigned, who is accountable for errors, and how disputes are resolved.[17] This sets the stage for examining whether current legal frameworks adequately address the challenges of automated contracting in the next section.

In the context of algorithmic contracting, it is essential to distinguish between AI-assisted formation and automated performance, as each raises distinct legal considerations. AI-assisted formation involves systems that operate during the pre-contractual phase-drafting terms, negotiating conditions, or even autonomously concluding agreements, where questions of consent, intention, and offer-acceptance mechanics are critical. By contrast, automated performance concerns the execution or fulfilment of contractual obligations, such as payment processing or delivery scheduling, once a contract has already been formed. While the latter generally poses fewer doctrinal challenges, it may give rise to issues of liability and risk allocation in cases of malfunction or non-performance. Recognising this divide allows for a more precise analysis of how existing legal fra-

(accessed 31 January 2025).

15 IBM, *Streamline Contract Management with Watson AI*, 2024, available at *ibm.com* (accessed 31 January 2025).

16 Automation-bias research shows that lawyers and other professionals tend to rely uncritically on machine recommendations, amplifying the risk of undetected errors in automated contracting. On automation bias in legal work see P. Laux – C. Ruschemeier, *Automation Bias and the Need for Human Oversight in Contract Review*, Working Paper, 2021, available at *ssrn.com* (accessed 31 January 2025).

17 In Quoine v B2C2 [2020] SGCA(I) 2 an unattended pricing algorithm executed trades 250 × off-market and the platform later had to litigate the reversal. The case underscores that, even in ostensibly deterministic environments, human-in-the-loop controls remain indispensable for legal accountability.

In Moffatt v. Air Canada, 2024 BCCRT 149, the British Columbia Civil Resolution Tribunal found Air Canada liable for misinformation provided by its AI chatbot regarding bereavement fares. The tribunal ruled that Air Canada was responsible for the chatbot's inaccurate information, despite the airline's argument that the chatbot was a separate entity. This case is significant for establishing corporate accountability for information provided by AI systems on company websites.

meworks should adapt to the different functions AI systems perform within contractual relationships.

A closely related issue concerns the frequent confusion between algorithmic contracts and smart contracts, two concepts that overlap yet remain fundamentally distinct. While some authors treat these terms as interchangeable,[18] closer analysis shows that their core functions emerge at different stages of the contractual lifecycle. Algorithmic contracts emphasise autonomy during the formation phase, as AI agents are capable of drafting, negotiating, or even determining contract terms with minimal human input. Smart contracts, by contrast, are primarily concerned with automation in the performance phase, executing contractual obligations automatically and without human intervention once predefined conditions are met.[19]

The technologies underlying these systems further illustrate their differences. Smart contracts are typically supported by cryptographic mechanisms and distributed ledger technologies (DLT), as seen in blockchain-based platforms such as Ethereum, while algorithmic contracts rely more heavily on artificial intelligence and machine learning techniques to generate or refine contract terms.[20] Vitalik Buterin famously referred to smart contracts as autonomous software agents, but this characterisation blurs the line between automation (execution without human input) and autonomy (decision-making during contract formation).[21] Scholars such as Scholz and Ebers emphasised the need to maintain this conceptual distinction to avoid regulatory and interpretative confusion.[22]

The Law Commission's 2021 report on smart legal contracts provides helpful clarification by distinguishing between three categories of smart legal contracts:[23] (i) Natural language contracts with automated performance,

---

[18] J. Linarelli, *Artificial Intelligence and Contracts Formation: Back to Contract as Bargain?*, Working Paper No. 6, 2024, available at *ssrn.com* (accessed 25 July 2025); C. Wendehorst, *Discussion Draft: Principles for AI in Contracting*, cit., 49.

[19] M. L. Mena Durán, *Artificial Intelligence in Contract Formation: The Shift from Automaton to Autonomy in the Case of Algorithmic Contracts*, Doctoral Thesis, King's College London, London, 2024.

[20] M. Ebers, *Artificial Intelligence, Contracting and Contract Law: An Introduction*, in M. Ebers – C. Poncibò – M. Zou (eds.), *Artificial Intelligence and the Law of Contracts*, Oxford, 2022, 19 ss.

[21] V. Buterin, *A Next Generation Smart Contract & Decentralized Application Platform*, White Paper, 2014.

[22] L. H. Scholz, *Algorithmic Contracts*, in *Yale Law Journal*, 128, 2017, 566 ss.; L. H. Scholz, *Algorithms and Contract Law*, in W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge, 2020, 141 ss.; J. Linarelli, *Artificial General Intelligence and Contract*, in *Law, Innovation and Technology*, 11, 2019, 330 ss.; Lord Sales, *Law and the Digital World*, Sir Henry Brooke Annual Lecture, 16 April 2021; C. Poncibò, *Artificial Intelligence as a Communication Tool in Contract Law*, in *European Review of Private Law*, 31, 2023, 239 ss.

[23] Law Commission of England and Wales, *Smart Legal Contracts: Advice to Government*,

where code merely executes pre-agreed obligations; (ii) Hybrid smart legal contracts, where natural language and code jointly define obligations and performance; and (iii) Solely code-based smart legal contracts, where all terms are defined and executed by code.

Algorithmic contracts partially overlap with the latter two categories but go beyond them by integrating AI's capacity for inference and autonomous decision-making in the formation phase. Thus, while smart contracts can be seen as execution tools, algorithmic contracts engage with the core contractual elements of offer, acceptance, and intention. Having established this conceptual foundation, Section 3 examines how international and European instruments address AI-driven contract formation.

3. UNCITRAL, European Legal Framework and Their Gaps

3.1 UNCITRAL Model Law and Automated Contracting

In July 2024, UNCITRAL finalised the Model Law on Automated Contracting (MLAC), a significant global benchmark for addressing AI and automation in contract formation. The UNCITRAL Model Law builds upon earlier e-commerce instruments (like the 1996 Model Law on Electronic Commerce and the 2005 Electronic Communications Convention) and aims to overcome legal obstacles to automated contracting by providing internationally accepted rules for recognising contracts made by automated systems. While not binding, the MLAC is intended as a template for national legislatures and possibly the EU to adopt or adapt, thereby harmonising approaches across jurisdictions.

The MLAC provides a foundational approach to regulating AI-assisted contract formation by distinguishing between deterministic and non-deterministic systems.[24] A deterministic system follows a set of predefined

Law Com No 401, 2021.

[24] While the UNCITRAL Model Law calls such systems "non-deterministic", machine-learning components are more precisely stochastic. Randomness is typically injected during training (e.g., data shuffling, stochastic-gradient updates), whereas the trained model's inference step is algorithmically deterministic, identical weights plus identical input always yield the same output. After the training, no random sampling is involved unless you explicitly add it (e.g., Monte-Carlo dropout, sampling from a language model with temperature > 0).

Once the system is applied in a real environment, what might disappear is predictability in the everyday sense, because the model can be exposed to inputs it has never seen. Those outputs are probabilistic estimates applied to novel data, the system's behaviour can remain uncertain and may be best characterised as stochastic rather than merely

rules and always produces the same output for a given input. There is no randomness or unpredictability in its operations, but there can be errors. Examples include smart contracts, particularly those using a certain programming language. Researchers have found that Solidity's compilation to bytecode enables syntax error detection at compile-time, while runtime errors remain difficult to catch and typically occur during contract execution.[25] A non-deterministic system, more precisely described as a stochastic system in the context of machine learning, involves elements of randomness or learning. This means the same input may yield different outputs depending on various factors, such as how the AI model was trained, stochastic processes like data shuffling or dropout during training, or the exposure to novel data post-deployment. Although the model's internal logic remains algorithmically deterministic, these probabilistic outputs are characteristic of AI-driven contract negotiations, where machine learning models predict terms based on context rather than fixed rules. This stochastic nature challenges the traditional assumptions of predictability and reliability in contract law. However, as a model law, it lacks direct applicability at the EU level and does not comprehensively address liability allocation, unexpected AI-driven actions, or consumer protection concerns. Also, since this is a supranational law, there are questions whether the MLAC's principles sufficiently align with European regulatory needs or whether additional legislative measures are necessary.

The MLAC emphasises technology neutrality and non-discrimination.

non-deterministic.

A critical distinction undergirding these technologies is the opacity of algorithmic reasoning, the lack of transparency in how an algorithm reaches its decisions or conclusions, manifesting through the inability to understand, access, or explain its reasoning process. This opacity may stem from intentional concealment (trade secrets, proprietary systems), technical complexity inherent in neural networks and machine learning models, or deliberate design choices favouring closed systems. Importantly, opacity must be distinguished from the black box problem, which constitutes a subset of opacity where reasoning is fundamentally unknowable even to the system's creators. While opacity denotes the inaccessible or unexplained nature of algorithmic reasoning, a condition potentially remediable through transparency obligations and disclosure mechanisms, the black box represents an epistemologically distinct phenomenon in which the reasoning remains inherently inscrutable. This distinction carries direct legal consequences for contract formation: opacity may be addressable through auditability requirements and explainability obligations, whereas the black box problem raises deeper questions about whether meaningful human oversight or informed consent is feasible at all. As automated contracting increasingly relies on non-deterministic AI systems capable of autonomous adaptation, this conceptual framework proves essential for calibrating liability, transparency, and accountability regimes.

[25] N. Atzei – M. Bartoletti – T. Cimoli, *A Survey of Attacks on Ethereum Smart Contracts (SoK)*, in M. Maffei – M. Ryan (eds.), *Principles of Security and Trust. POST 2017*, Lecture Notes in Computer Science, vol. 10204, Berlin – Heidelberg, 2017, 164 ss.

Using an AI or algorithm to form a contract should not cause the contract to be denied legal effect just because no human was directly involved. This principle of non-discrimination against electronic agents echoes earlier e-commerce law and is now expressly extended to highly autonomous AI contracting. The MLAC also underscores party autonomy: parties remain free to choose whether to use automated systems in contracting and to tailor how those systems operate by agreement (subject to mandatory law).[26] In essence, automation is to be accommodated within the existing fabric of contract law, not treated as an alien phenomenon.

The MLAC provides concrete rules to ensure the validity and enforceability of contracts formed by AI-powered digital assistants. Notably, art. 5 states that a contract formed using an automated system shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in the process. This directly addresses contract formation certainty: even if two AI programs negotiate and agree on terms with zero human involvement at the time of agreement, the resulting contract is as valid as any traditional contract. Art. 5 (with an optional paragraph for contract performance) essentially enshrines that lack of human awareness is no defence to contract enforcement, a critical clarification for AI-to-AI contracting scenarios.

MLAC further tackles contracts in code and dynamic terms. Art. 6 ensures that contracts are not invalid merely because their terms are represented in computer code or incorporate data that changes continuously (for example, an IoT contract with price terms linked to market data feeds). This provision is forward-looking: it legitimises smart contracts where obligations might be encoded in software and contracts that self-modify based on external data sources, both increasingly relevant with AI systems that adjust terms on the fly.

On the question of attribution and liability, art. 7 provides a default rule: actions taken by an automated system are attributed to the party on whose behalf the system operates. Specifically, between contracting parties, the parties can agree on an attribution rule (e.g. if using a third-party AI platform, they might allocate responsibility by contract). In the absence of such an agreement, the law attributes the action to the person who uses the system for that purpose. In practical terms, if a company de-

[26] M. S. Gal, *Algorithmic Challenges to Autonomous Choice*, in *Michigan Technology Law Review*, 25, 2018, 59 ss., 63. By choosing to entrust algorithms with the negotiation or drafting of obligations, parties implicitly accept the legal and practical consequences of outcomes determined by complex, data-driven processes. While this delegation may diminish predictability and direct oversight, it remains consistent with the principle of freedom of contract, which binds individuals to the results of their voluntary choices; see M. L. Mena Durán, *Artificial Intelligence in Contract Formation: The Shift from Automaton to Autonomy in the Case of Algorithmic Contracts*, cit.

ploys an AI agent to negotiate a deal, that company is responsible for the AI's contracting acts as if it had done them itself. Critically, art. 7(3) adds that attribution is not negated «on the sole ground that the outcome was unexpected». In other words, a party cannot escape a contract by arguing that its AI agent behaved in unforeseen ways, at least not automatically; the act is still attributed to them. This tackles the liability issue of AI malfunctions or unanticipated behavior: the default position is that the user of the AI bears the risk. However, MLAC recognises that this issue is delicate, so it leaves room for other laws to determine the consequences of such attribution in extreme cases (for instance, contract law doctrines of mistake or consumer protection rules could still apply via art. 7(4)).
This discussion can be further refined by drawing on Cristina Frattone's distinction between automation mistakes and autonomy mistakes. Automation mistakes refer to errors caused by technical faults or data issues, essentially failures in execution, whereas autonomy mistakes stem from the AI system's independent, though logic-based, decision-making that leads to unintended outcomes.[27] Introducing this distinction may help clarify the types of unexpected AI actions addressed under the attribution framework in art. 7(3) of MLAC, and when the exceptional rule in art. 8, which permits a party to avoid enforcement of an action attributed to them in unforeseen cases, might apply.
The question of terminology, whether to designate the human party as "user", "operator", or "deployer", is non-trivial. While the EU AI Act adopts "deployer" for the entity putting AI into use, contract law scholarship often prefers "operator" to emphasise active control over parameters. This article adopts "operator" to capture both the party using the AI and the one responsible for setting its contractual objectives, consistent with Wendehorst's framing.
Prof. Florian Möslein at the Münster Colloquia[28] examined how AI-driven contract formation necessitates a recalibration of classical contract

[27] C. Frattone, *Algorithmic Mistakes in Machine-Made Contracts: The Legal Consequences of Errors in Automated Contract Formation*, in *Uniform Law Review*, 28, 2023, 407 ss., available at *doi.org* (accessed 31 January 2025).

[28] F. Möslein, *AI Contracting and Default Rules*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at *jura.uni-muenster.de* (accessed 13 November 2025).
The challenge of reconciling algorithmic autonomy with legal attribution extends to default contractual rules. AI systems that autonomously negotiate contracts must be accompanied by explicit default rule frameworks. Prof. Möslein argues that civil law jurisdictions, which rely heavily on mandatory default rules, face particular challenges when algorithmic systems operate without human intervention during critical negotiation phases, requiring a recalibration of both statutory and contractual default mechanisms to protect party interests and ensure legal certainty.

law principles, particularly regarding the role of default rules in establishing standard terms when algorithmic systems negotiate on behalf of parties. Prof. Möslein argues that the allocation of liability between the deployer, developer, and other stakeholders involved in automated transactions requires explicit contractual design and legislative intervention to ensure that default rules do not inadvertently disadvantage parties or create unintended legal consequences.

To address truly aberrant AI behaviour, the Model Law includes an optional provision, art. 8, on unexpected actions. This provision (which states can choose to enact or not) creates a narrow exception: if an automated system's action is attributed to Party A, the other Party B cannot enforce that action as part of the contract if, under the circumstances, (a) Party A could not reasonably have expected the action, and (b) Party B knew or should have known Party A didn't expect it. This effectively codifies a kind of mistake/knowledge[29] rule for AI outputs: it prevents opportunistic enforcement of a contract term that one party's AI agreed to, when the other party realised it was a mistake or out-of-scope. Art. 8 thus introduces a measured safety valve for the most unanticipated AI-driven transactions, protecting parties from being bound by egregious AI errors – but only where the other side had reason to know something was amiss. The inclusion of this optional rule acknowledges that while automation should generally bind the user, fairness may require exceptions in edge cases of AI unpredictability. States worried about abuse could opt not to enact art. 8 or could tighten their standards.) This narrow unexpected actions exception in art. 8 closely mirrors the common-law doctrine of unilateral mistake, which voids a contract when one party was fundamentally mistaken about a term and the other party knew or ought to have known of the mistake. Both art. 8 and the unilateral mistake doctrine aim to prevent opportunistic enforcement of agreements when true assent was absent or impaired.

The MLAC also touches on transparency and disclosure indirectly. Art. 9 (Information requirements) clarifies that nothing in the model law overrides any existing legal obligations to disclose information about the design or operation of an automated system. In other words, if other law, perhaps consumer law or financial regulations, imposes duties to inform the counterparty or a regulator about how an AI negotiator works, those duties remain intact. Art. 9 importantly signals the importance of information disclosure in the operation of automated systems, as UNCITRAL's summary notes, but the model law itself stops short of imposing new disclosure mandates. It defers to other applicable law to require transpa-

[29] J. Tan Ming En, *Non-deterministic Artificial Intelligence and the Future of the Law on Unilateral Mistakes in Singapore*, in *Singapore Academy of Law Journal*, 34, 2022, 93 ss.

rency about AI use (for instance, a national law could require businesses to inform consumers when they are contracting with an AI). The model law's stance here is cautious: it acknowledges transparency as a concern but leaves specifics to national policymakers, likely because appropriate disclosure might vary by context (B2B vs B2C, etc.). Under art. 50 of the EU AI Act, businesses are required to inform individuals when they interact with an AI system, unless this is obvious from the context.[30] While this obligation will apply from August 2026, national laws can already adopt such provisions in advance. The UNCITRAL Model Law, by deferring to existing or future national laws, accommodates varying levels of transparency across jurisdictions. In contrast, the U.S. currently lacks a binding federal requirement of this nature, while the UK is considering sector-specific transparency measures.[31]

Finally, art. 10 (Non-avoidance) ensures no one can use AI to circumvent legal obligations. It states that a party cannot be relieved from the legal consequences of failing to comply with a law on the sole ground that it used an automated system. This is a catch-all rule of accountability: using an AI agent is not a get-out-of-jail-free card for legal duties. For example, if consumer protection law requires certain contract terms or procedures, a trader can't escape liability by blaming its AI for not following the law.

Collectively, the UNCITRAL Model Law provides a blueprint for addressing the fundamental uncertainties of AI contracting. The UNCITRAL Model Law on Automated Contracting (2024) has similar legal consequences to those established by Directive 2000/31/EC (the E-Commerce Directive), in that it confirms the validity of contracts formed through technological means. Like the Directive's affirmation of electronic contracting, the Model Law does not alter the substantive rules of contract formation but rather ensures that the use of automated systems does not undermine the legal effect or enforceability of agreements, thereby promoting certainty and functional equivalence in digital commerce. It establishes baseline validity of AI-formed contracts, a default liability allocation (attribution to the user of AI), a possible escape hatch for extreme AI-generated mistakes (art. 8) and reaffirms transparency and accountability principles. While comprehensive in these respects, UNCITRAL deliberately scoped the model law as a modest overlay to existing contract law, not a complete code. It does not seek to address legal issues beyond the

[30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence (AI Act), in OJ L 168, 13.6.2024, p. 1–153, art. 50.

[31] UK Department for Science, Innovation and Technology (DSIT), *A Pro-Innovation Approach to AI Regulation: Government Response*, 6 February 2024, available at *gov.uk* (accessed 9 May 2025).

contractual setting and does not cover AI ethics or algorithmic fairness, which are beyond contract law. Some complex issues, like how to handle AI systems that are non-deterministic (learning systems whose actions are not fully predictable even by their programmers), are not deeply regulated by the model law beyond the general rules noted. The Guide to Enactment (forthcoming) likely provides further guidance on such issues.
For EU purposes, the MLAC offers a ready-made solution that could be adopted (perhaps with tweaks) to harmonise AI contract law across Member States. It addresses many of the key points of legal uncertainty (formation validity, attribution of liability, etc.) in a balanced way. The question the European Commission faces is whether simply encouraging adoption of the MLAC (at national or EU level) is sufficient, or whether an alternative version with additional provisions is needed. A relevant criticism previously articulated by Emily Weitzenboeck in relation to the Model Law on Electronic Commerce, the UETA, UCITA, and Directive 2000/31/EC, also applies to the UNCITRAL Model Law on Automated Contracting. While these instruments affirm the legal validity of contracts formed through technological means, they do so without providing substantial doctrinal justification or engaging with foundational principles of contract law.[32] The regulatory emphasis remains on functional equivalence and legal certainty, but this often comes at the expense of a deeper theoretical account of autonomy, intention, and consent in technologically mediated contracting. As noted at Münster, the MLAC's generality may leave certain gaps, for instance, specific guidance on non-deterministic AI that the model law doesn't explicitly distinguish. Issues like dynamic renegotiation by AI or biased decision-making might require more tailored rules (perhaps around consumer consent or auditability). These are areas where the ELI Principles[33] and Prof. Wendehorst's draft[34] step in, potentially proposing additional provisions beyond UNCITRAL's baseline.

3.2 EU AI Act and other efforts

Beyond international initiatives, European scholars and institutions have developed complementary studies.[35] While the EU AI Act establishes ove-

[32] E. M. Weitzenboeck, *Electronic Agents and the Formation of Contracts*, in *International Journal of Law and Information Technology*, 9, 2001, 204 ss.

[33] ELI, *Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts*, cit.

[34] C. Wendehorst, *Principles for AI in Contracting*, cit.,

[35] At the Münster Colloquia:
F. Möslein, AI Contracting and Default Rules, cit. Prof. Florian Möslein (Philipps-University Marburg) has specifically addressed how algorithmic contracting challenges traditional

rarching rules for AI governance,[36] it does not explicitly regulate automated contracting. There is an absence of provisions addressing contract attribution of risks and liability, disclosure obligations, and mechanisms for addressing unexpected AI-generated contract outcomes.[37] Insights from ELI Guiding Principles and Prof. Wendehorst's Principles provide additional considerations for addressing these legal gaps.

The ELI, an independent non-profit organisation that develops law reform proposals, has been at the forefront of crafting a European-specific approach to AI in contracting. The ELI Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts (DACC Model Rules) project of 2022–2025 focuses particularly on the use of automated decision-making (ADM) and AI in consumer contracts, though many principles are broadly applicable.[38] The rationale is that consumer protection law

default rule mechanisms in civil law jurisdictions, particularly regarding how deployer liability interacts with the formation of AI-generated contracts.

C. Twigg-Flesner, *Attribution of Pre-contractual Information and Knowledge: The ELI Model Rules on Algorithmic Contracts and Beyond,* paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at *jura.uni-muenster.de* (accessed 13 November 2025).

Prof. Christian Twigg-Flesner (University of Warwick) examined how pre-contractual information and knowledge attribution must be recalibrated within the ELI Model Rules on Algorithmic Contracts, particularly given the challenges of ensuring that algorithmic systems adequately disclose material terms and risks to consumers before contract formation.

C. Busch, *Augmented Consumers and Algorithmic Consumers in AI Contracting*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at *jura.uni-muenster.de* (accessed 13 November 2025). Complementing this analysis, Prof. Christoph Busch (University of Osnabrück) investigated the transformation of consumer agency in AI-driven transactions, arguing that algorithmic contracting requires a reconceptualization of the consumer as both an augmented party (enhanced by decision-support tools) and a vulnerable subject requiring protective mechanisms against algorithmic opacity and bias.

[36] Regulation (EU) 2024/1689.

[37] The European Union does not possess a general competence to harmonise contract law. Its regulatory interventions rely primarily on art. 114 TFEU, which supports measures necessary for the functioning of the internal market, and art. 169 TFEU, concerning consumer protection. Consequently, EU legislation in this area is limited and sector-specific, targeting issues that affect cross-border transactions. Key instruments include Directive 93/13/EEC on unfair terms in consumer contracts, which prohibits clauses that create a significant imbalance to the detriment of the consumer, and Directive 2011/83/EU on consumer rights, which harmonises pre-contractual information duties, the right of withdrawal, and rules for distance and off-premises contracts. However, fundamental aspects of contract law such as formation, validity, and interpretation remain under the competence of the Member States.

[38] ELI, *Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts*, cit.

faces distinct challenges when AI tools so-called digital assistants act on behalf of consumers or traders in transactions. The project's first phase produced an ELI Interim Report on EU Consumer Law and Automated Decision-Making (Dec 2023) assessing the adequacy of the existing EU consumer acquis for Automated Decision-Making, and setting out general principles for adaptation. The second phase, formulated the actual Guiding Principles and DACC Model Rules (a quasi, "black letter" framework) for algorithmic contracts, B2C and C2B contexts in depth.

The ELI Guiding Principles and DACC Model Rules were formally adopted on 15 April 2025 and published on 19 May 2025. Structured into five chapters comprising articles with commentaries, the Model Rules establish general principles, design requirements for digital assistants, legal frameworks governing their supply, regulation of algorithmic contracts, and third-party liability provisions. ELI observes that algorithms and AI are now used in all phases of the contract lifecycle, from advertising/ offers, to negotiation and formation, to performance and enforcement . This raises questions both of validity (are these AI-mediated contracts legally sound?) and fairness (are consumers adequately protected when, say, their AI-powered digital assistant contracts with a seller's algorithm?). The goal is to ensure Europe has a clear and predictable legal framework that both enables innovation allowing automated contracting to flourish and ensures effective safeguards for parties' rights and interests, especially weaker parties like consumers. In ELI's view, increased legal certainty for automated contracting is vital to unlock AI's economic potential while maintaining trust.

The European Law Institute Interim Report identified eight guiding principles aimed at adapting EU consumer law to the challenges posed by algorithmic decision-making and AI-driven contracting, each of which reveals specific areas requiring regulatory clarification. First, it addresses the attribution of AI-powered digital assistant's actions to the consumer, clarifying when and under what conditions a consumer should be legally bound by actions autonomously undertaken by their AI-powered digital assistant. Second, the Report reaffirms that consumer law continues to apply fully to algorithmic contracts, ensuring that protective mechanisms such as the right of withdrawal and information duties remain effective even when contractual interactions occur through AI intermediaries rather than through direct human engagement. Third, it examines the fulfilment of pre-contractual information duties, seeking to determine how mandatory disclosures can be meaningfully provided in scenarios where an AI system, rather than the consumer, is responsible for the decision-making process. Fourth, it includes a principle on non-discrimination, which aims to prevent AI systems from generating discriminatory outcomes, such as personalised pricing or filtered offers that could disadvantage certain con-

sumer groups. Fifth, it considers disclosure obligations related to the use and functioning of automated decision-making systems, requiring transparency regarding the deployment of AI in contractual processes. Sixth, the report introduces the need to protect digital assistants from manipulation, particularly by preventing traders from influencing the behaviour of AI-powered digital assistant through misleading or strategically engineered data inputs. Seventh, it emphasises the necessity of determining and disclosing the operational parameters governing digital assistants, thereby ensuring that consumers have clarity over the criteria according to which their AI-powered digital assistant negotiates or concludes contracts. Finally, it highlights the issue of conflicts of interest, calling for regulatory safeguards to address situations in which the operator of a consumer's AI-powered digital assistant may have interests of its own, such as commercial affiliations, that could distort the assistant's decision-making to the detriment of the consumer.

These principles collectively aim to make consumer law AI-ready, ensuring that fundamental safeguards (like informed consent, fairness, and transparency) are preserved in an era of automated contracting. The Interim Report concluded that most existing EU consumer directives are almost ADM-ready with only minor adjustments needed. For example, rules on providing contract terms or withdrawal rights can largely accommodate AI but perhaps need explicit clarification that if an AI concludes a contract, the consumer can still exercise their rights. The report recommended that a few new provisions be added to align the law with the ELI principles.

DACC Model Rules affirm that contracts formed by AI are valid, but will stress aligning the AI's actions with the intent of the human parties. Wendehorst's Principles, discussed later in this paper, emphasise the importance of aligning AI's actions with the intent of the contracting parties. This implies a principle that even if AI negotiates, it must operate within the scope of authority given by the user. The human party's intent[39] (perhaps as configured in the AI's parameters) is key. Following Sartor's terminology, since the ultimate objective is always set by the human operator, delegating the decision-making process to AI merely explains the attribution of intent to the user, rather than creating any independent intention on the part of the AI. If the AI deviates, the law should have a way to discern whether the resulting contract reflects any real agreement. This aligns with the principle that intent, at least under English law, is tested objectively:

[39] M. Herbosch, *Contracting with Artificial Intelligence: A Comparative Analysis of the Intent to Contract*, in *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 88, 2024, NIX, 1 ss. Herbosch addresses the role of intent in contract formation: the "distance between the abstract intent to form a contract and the specific contract that the system output may have formed". Refer to the "limited value of intent" as stressed by the ECJ jurisprudence that human intent often plays a constrained role in binding contract formation.

the focus is on whether a reasonable observer would interpret the AI's actions as representing the user's manifested intent.[40] Wendehorst/ELI appear to advocate clarity that AI is a tool of its user not an independent actor with its own intent.[41]

The DACC Model Rules stress the need for clarity in attributing accountability for AI's actions to its deployers, whether natural or legal persons . This mirrors UNCITRAL's approach: the party deploying is generally responsible. Consumers and traders using AI assistants are bound by their AI's actions as if performed personally, subject to protective exceptions. In consumer cases, attribution to the consumer was principle number 1 likely ensuring a consumer isn't denied a remedy just because their AI-powered digital assistant clicked the button, but also possibly ensuring the consumer can be held to a contract their AI-powered digital assistant made if it was operating under their authority. The flip side is liability of traders using AI-powered digital assistant: if a business's AI errs, the business should be accountable to the consumer. Both aspects reinforce that the legal person behind the AI bears the consequences, not the AI itself since AI has no legal personality.

The DACC Model Rules require that parties especially businesses disclose their use of AI in negotiations or contract formation to the other side particularly if the other side is a consumer. Indeed, the ELI principles propose mechanisms such as pre-contractual disclosures to ensure AI systems operate within agreed legal and business objectives. For instance, a trader's duty might include informing a consumer that an algorithm, not a human, will assess their offer and on what basis at least in general terms. This ties into fairness, a consumer should know if they are dealing with a bot and

---

[40] Smith v. Hughes (1871) LR 6 QB 597.

[41] J. Linarelli, *A Philosophy of Contract Law for Artificial Intelligence: Shared Intentionality*, in M. Ebers – C. Poncibò – M. Zou (eds.), *Contracting and Contract Law in the Age of Artificial Intelligence*, Oxford, forthcoming, available at *papers.ssrn* (accessed 9 May 2025).

Linarelli deepens this point that legal frameworks may evolve to recognise more nuanced or distributed forms of intent, especially when decisions emerge from complex, semi-autonomous systems. It complements ELI/Wendehorst's view that contracts formed by AI must still reflect the human party's purpose and scope of authority.

Lirikë Kamberi, *The Integration of AI in Contract Law: Formation, Enforcement, and Legal Challenges from an International Perspective*, Master's Thesis, University of Vienna, 2023, available at *phaidra.univie.ac.at*, 28 ss.

Kamberi offers a clear and relevant analysis of intent in AI contracting. She explains that, under the objective theory, contracts formed by AI can be valid if the AI's actions outwardly manifest intent, even without human involvement at the moment of formation. She also acknowledges that this works well for "weak AI" but may fall short as strong AI systems act more autonomously, potentially requiring a shift toward recognizing more nuanced or hybrid forms of intent. I believe that in terms of a deterministic system, intent can be met to a certain extent at least.

how that might affect them. This approach aligns with art. 50 of the EU AI Act, which requires businesses to inform individuals when they interact with an AI system, unless this is evident from the context.[42] Although this obligation will only apply from August 2026, national legislators could adopt similar provisions earlier. ELI's vision arguably goes further, as it suggests that relevant operational parameters, such as the conditions under which a consumer's digital assistant automatically agrees to purchases, should be transparent to ensure genuine consent and to prevent traders from exploiting undisclosed settings. Such disclosure obligations address the power imbalances and information asymmetry inherent in AI-driven interactions, thereby supporting fairness, informed decision-making, and consumer trust.[43]

It could also include disclosure of certain parameters: e.g., if the consumer's own AI-powered digital assistant is set to auto-buy items up to a certain price or with certain data access, those parameters might need to be transparent so the consumer consents and the trader cannot exploit unknown settings. Greater transparency obligations would address power imbalances and information asymmetry introduced by AI.

Given ELI's awareness of unexpected outcomes/outputs as a key issue requiring harmonisation, the Model Rules incorporate a rule akin to UNCITRAL's art. 8 or other fallback liability provisions. The proposals, such as fall-back liability provisions and procedural safeguards, aim to address accountability for unexpected AI actions. For example, DACC Model Rules provide that if an AI's action falls outside a consumer's reasonable expectations, perhaps contrary to the consumer's given instructions or usual preferences, and the business knew this or should have known, then the consumer is not bound. This would protect consumers from, say, their AI-powered digital assistant making an absurd purchase due to a glitch. Traders, meanwhile, might be protected if their AI-powered digital assistant was manipulated by the other side or if an outcome was probably not intended. Essentially, ELI recommends a safety net in line with equitable principles to handle AI-induced errors or misalignment, very much in spirit with UNCITRAL's optional rule but perhaps tailored for consumer scenarios.

The DACC Model Rules impose design requirements ensuring consumers remain in control of digital assistants through parameter-setting, contract prevention mechanisms, and deactivation capabilities. Additionally, the Model Rules require digital assistants to be protected from manipulation, preventing traders from exploiting or biasing consumer-deployed AI. Conflicts of interest arising from digital assistant use must be disclosed,

[42] Regulation (EU) 2024/1689, art. 50.

[43] F. Di Porto, *Algorithmic Disclosure Rules*, in *Artificial Intelligence and Law*, 31, 2023, 13 ss.

addressing situations where AI operators have commercial affiliations distorting decision-making to consumers' detriment.
ELI's project coordinated closely with UNCITRAL. ELI representatives participated as observers in UNCITRAL Working Group sessions, ensuring cross-fertilisation and consistency. ELI does not reinvent basic validity and attribution rules but supplements them with European consumer law perspectives, particularly mandatory disclosures and fairness checks. While UNCITRAL leaves disclosure to other law, ELI mandates explicit disclosure obligations. Similarly, UNCITRAL's optional approach to unexpected outcomes becomes a structured consumer protection mechanism in the DACC Model Rules framework.
Both the ELI Model Rules and Wendehorst's draft remain non-binding as of late 2025, though the published DACC Model Rules represent the most comprehensive transnational soft law dedicated to digital assistants. They are designed to inspire EU or national legislation and guide courts in the interim. As Wendehorst notes, these principles aim to «[g]uide the application of existing law and the development of new law in relation to automated contracting».[44] In Europe's civil law tradition, such principles can influence judicial reasoning even before formal adoption, given the absence of statutory guidance on AI contracts.

3.3 Wendehorst's 2024 Discussion Draft: Principles for AI in Contracting

Professor Christiane Wendehorst's "Discussion Draft: Principles for AI in Contracting (Version 2.1)" is an influential academic contribution that complements the ELI project.[45] It sets out proposed legal principles addressing automated contracting with advanced AI. Wendehorst's contribution is significant in that it distils the core issues and corresponding solutions into a coherent set of principles, thereby addressing the uncertainty she identifies in this area.[46] As an academic draft, it doesn't have legal force, but it has been discussed at conferences (including the Münster Colloquium) and informs the ELI's work (Wendehorst is co-reporter on the ELI project).
Wendehorst notes that the proliferation of highly autonomous electronic agents in contracting has outpaced legal adaptation.[47] She observes that

[44] C. Wendehorst, *Discussion Draft: Principles for AI in Contracting*, cit., 43.

[45] *Ibid*

[46] C. Wendehorst, *Principles for AI in Contracting*, cit., 16 ss.

[47] *Ibid.*., 1 ss.

around the world, the first major disputes involving AI contracts are reaching courts, yet basic questions, e.g., should liability lie with the AI's developer, the user, the AI itself, or someone else – lack clear answers. There is surprisingly little legislation on automated contracting, creating gaps in legal certainty.[48] Thus, her draft principles aim to provide clarity and guide both application of existing law and the development of new law. They are meant as a template or inspiration for legislators and judges, similar in spirit to restatements or model principles in other fields.

Prof. Wendehorst's draft allows a clear understanding of the substance and structure of the proposed principles.

The Principles for AI in Contracting affirm that the use of AI in contracting does not negate the validity of a contract, aligning with the approach taken in UNCITRAL instruments and in U.S. frameworks such as the UETA. They confirm that machine-generated communications (data messages) may constitute legally relevant declarations of will, even in the absence of contemporaneous human awareness, and that contracts concluded with the assistance of AI should not be denied effect on the basis of form or capacity requirements alone. This position mirrors traditional doctrines on formality and capacity, under which the lack of real-time human presence does not preclude contractual validity where intent and expression are established. Consistently with UNCITRAL and UETA, the Principles anchor intention in the human decision to deploy and configure the system:[49] i.e., the «intention flows from the programming and use of the machine».[50] This anchors validity in the user's decision to entrust the AI, rather than requiring a real-time human intent.

A core principle is that AI systems have no independent legal intent; their actions must be attributable to a legal person. Wendehorst emphasises aligning AI actions with the parties' intent, which implies a principle that an AI's actions are deemed the actions of the party on whose behalf it operates (similar to UNCITRAL art.7 and UETA Section 14). This reflects classical agency principles, particularly those involving automated representatives, where the principal bears legal responsibility for authorised actions. She likely frames it as an agency principle for AI: the deploying party bears responsibility for the AI's contracts.[51] This would resolve the

[48] *Ibid.*, 1 ss., 12 ss.

[49] P. Cramer – J. Mollod – C. Rimmer, *Contract Law in the Age of Agentic AI: Who's Really Clicking Accept?*, in *newmedialaw.proskauer.com,* 8 April 2025.

[50] *Ibid.*

[51] On the varied terminology used to describe parties interacting with AI systems, see E. Mik, *Much Ado About Artificial Intelligence or: The Automation of Contract Formation*, in *Journal of Business Law*, 2021, 501 ss., 505; A. Ooi, Artificial Intelligence and Party Attribution in Contract Formation, in *Journal of Law and Technology*, 15 (2024), 99–100. The EU

"who is bound?" question in favour of the human/business behind the AI, not the developer or the AI. However, Wendehorst's introduction also raises the possibility of looking at the developer or something else in cases of unanticipated transactions. That suggests her principles might include guidance on when a developer or third party could be liable, possibly not in contract since the developer isn't party to the contract, but perhaps in compensation to the user for the AI's error. The primary contract-law rule, however, is likely that between the contracting parties, the one who put forth the AI is treated as making the contract. This is consistent with ELI's stance that AI is an agent of its deployer.

Wendehorst appears to advocate for transparency obligations. Her principles likely call for parties to disclose when they are using AI in contracting and possibly to disclose certain characteristics of the AI if relevant to the other party's decision. This ensures informed consent in AI-mediated dealings. It ties to ELI's pre-contractual disclosure principle. For instance, a principle might be that a party using an AI system to negotiate or conclude a contract should inform the other party of that fact, unless it is apparent from the circumstances. Such a rule would protect, say, a consumer from unknowingly negotiating against a sophisticated algorithm and, conversely, allow a business to understand if it is dealing with an AI-driven request. Additionally, if the AI has known limitations or propensities, e.g., it cannot process certain information, or it prioritises certain factors, disclosing that could be important, especially in consumer contexts or where asymmetry exists.

Although contract principles might not heavily delve into AI design, Wendehorst might include a principle addressing the duty of those deploying AI to use appropriate systems and prevent harm. For instance, a notion that if you employ an AI in contracting, you should ensure it has been properly tested/monitored so as to avoid causing contractual harms like severe errors. If not a formal principle, this concern is reflected in suggestions that law might look at the developer for certain faults.[52] In the absence of specific regulation, this could translate into an implied obligation of diligence in using AI.

Wendehorst clearly is concerned with AI making unanticipated tran-

---

Artificial Intelligence Act adopts the term *"deployer"* to describe the entity that puts an AI system into use, although this designation is uncommon in contract-law discourse. See also T. Allen – R. Widdison, *Can Computers Make Contracts?*, in *Harvard Journal of Law and Technology*, 9 (1996), 25 ss., 39; M. S. Gal, *Algorithmic Challenges to Autonomous Choice*, in *Michigan Technology Law Review*, 25 (2018), 59 ss., 63. In line with C. Wendehorst's *Principles for AI in Contracting*, this study uses the term *"operator"* to capture both the party relying on the AI system and the party responsible for configuring it: C. Wendehorst, *Principles for AI in Contracting*, cit., 43 ss., 49.

[52] C. Wendehorst, *Principles for AI in Contracting*, cit., 41 ss., 26 ss.

sactions or transactions resulting from technical errors.[53] One of her principles likely deals with the scenario of AI mistakes. Perhaps a principle akin to, if an AI system makes a contract beyond the scope authorised by its user due to an autonomous decision or error, the law should provide appropriate remedies (such as voidability) when enforcement would be unjust, and the counterparty knew or should have known of the mistake. This echoes UNCITRAL's unexpected outcome rule but could be framed in more general contract law terms (mistake, lack of true assent, etc.). This scenario closely resembles the doctrine of unilateral mistake, which precludes enforcement when one party is aware, or ought to be aware, of the other's error and seeks to exploit it. Wendehorst might propose criteria for when a contract is not binding due to AI deviation, balancing the need for reliability in automated contracts with fairness. Fall-back liability provisions and procedural safeguards are contemplated to handle unexpected AI actions, suggesting a structured approach to exceptions.

Implicitly, the principles reject treating the AI as a contracting party.[54] Wendehorst's framing always involves attributing to some human/legal person. This affirms the foundational principle that legal subjectivity and contractual capacity reside in natural or legal persons, not in tools or technologies. This is an important policy stance, differing from a hypothetical radical solution of granting AI legal personality (an idea floated in European Parliament discussions years ago but largely dismissed). By confirming AI is not a legal subject but a tool, the principles channel responsibility to existing persons.

Wendehorst likely stresses that clarity is needed not just nationally but ideally internationally. While not a principle per se, her commentary en-

[53] *Ibid.*, 2 ss., 23.

[54] Scholarly debates on the legal personhood of artificial agents have evolved from early explorations of electronic agents as semi-autonomous contracting entities: J.-F. Lerouge, *The Use of Electronic Agents Questioned Under Contractual Law*, in *Journal of Computer & Information Law*, 18, 1999, 403 ss.; I. Kerr, *Ensuring the Assent of Electronic Agents*, in *Berkeley Technology Law Journal*, 17, 2001, 123 ss.; A. J. Bellia, *Contracting with Electronic Agents*, in *Emory Law Journal*, 50, 2001, 1047 ss., these authors rejected the notion of granting legal personhood, emphasising the absence of consent, patrimony, or liability. E. M. Weitzenboeck, *Electronic Agents and the Formation of Contracts*, cit., examined personhood as one of several doctrinal solutions but found it unworkable. Later, F. Andrade et al., *Contracting Agents: Legal Personality and Representation*, in *Artificial Intelligence and Law*, 15, 2007, 357 ss., revisited the concept, drawing analogies with corporate entities but acknowledging unresolved difficulties in liability and enforcement. More recent approaches, such as G. Sartor, *Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents*, in *Artificial Intelligence and Law*, 17, 2009, 253 ss., and S. Chopra – L. White, *A Legal Theory for Autonomous Artificial Agents*, University of Michigan Press, 2011, shift focus from legal personhood to attribution, agency principles, and the intentional stance.

courages jurisdictions to align, hence her support of UNCITRAL's global model. This is more of a meta-point in her paper: that global consistency on fundamental rules like the validity of AI contracts is desirable to avoid legal fragmentation as automated contracts span borders.

Prof. Wendehorst's draft, being version 2.1, indicates it's evolving. It was first drafted in 2022 and refined through 2023–early 2024. The evolution likely incorporated feedback from developments like the UNCITRAL drafting sessions and interim ELI findings. At the 2025 Münster Colloquium, her principles were discussed and lightly referred to as Wendehorst's Principles, indicating they were a key reference point. They, together with the ELI Principles, highlight the consensus in Europe that AI in contracting should be treated through the lens of existing contract law doctrine (intent, attribution, consent) but sharpened with specific guidance and safeguards.

Importantly, Wendehorst is quoted as stressing the need for developing principles that can inspire future law and guide courts. She acknowledges both the dearth of legislation and the scarcity of case law to date on these issues.[55] Her approach is thus proactive: rather than wait for courts to improvise solutions, articulate principles now to shape consistent evolution of the law. This pragmatic yet forward-looking approach resonates with practitioners, it provides a reference for advising clients today, in contracts, one might incorporate some of these ideas in clauses allocating risk of AI error, for instance, and paves the way for eventual codification.

Wendehorst's principles aim to demystify AI contracting by mapping it onto familiar legal concepts: contracts formed by AI are still contracts offer/acceptance still applies, just via electronic agents;[56] the mind behind the contract is the human who deployed the AI;[57] information duties and good faith require transparency about AI involvement;[58] and if AI misfires, traditional doctrines like mistake, duty to correct errors, etc., should be invoked to prevent unfairness.[59] Her framework thus illustrates that AI contracting, while novel in mechanism, does not require a reinvention of contract law; rather, it calls for doctrinally consistent adaptations. These principles are a bridge between the status quo and a future where either legislation is enacted or case law develops providing an interim set of guidelines for all stakeholders.

---

[55] C. Wendehorst, *Principles for AI in Contracting*, cit., 3 ss.

[56] *Ibid.*, 25, 34.

[57] *Ibid.,* 3, 24, 40.

[58] *Ibid.*., 36.

[59] *Ibid.*, 3, 5, 9.

3.4 Limitations in the ELI and Wendehorst Frameworks

While both discuss AI as a tool, they do not fully account for situations where AI exceeds its programmed scope or makes contract-related decisions that are unforeseeable by its human operator**.** The principle of full attribution to the human operator assumes control over AI behavior, but in cases where machine learning-based AI autonomously adapts and modifies its own parameters, traditional liability frameworks become inadequate. Future legal frameworks should clarify whether strict liability, vicarious liability, or a novel AI-specific liability should apply when an AI breaches contractual terms autonomously or acts contrary to commercial expectations.[60] This is particularly crucial for B2B environments, where AI is increasingly used to negotiate, amend, and execute contracts without direct human supervision. A liability framework should distinguish between deterministic AI tools and self-learning AI systems**,** setting thresholds for attribution, foreseeability, and fault in AI-related breaches.

By attributing contractual responsibility to the AI operator/deployer, both implicitly relegate developer liability to secondary or non-contractual terrain. However, this allocation proves inadequate where AI system defects originate in design, training, or algorithmic architecture rather than operator error. A coherent framework must distinguish between operator liability (for authorised use and parameter-setting) and developer liability (for system design failures). The distinction matters particularly where developers retain control over core AI behaviour: algorithmic decision-making, training datasets, output boundaries, and known limitations. Under European law, the proposed AI Liability Directive (currently withdrawn) contemplated rebuttable presumptions of causality favouring victims against developers. While contract law itself cannot impose privity-based liability on non-contracting parties, tort law, particularly the revised Product Liability Directive, can hold developers accountable for defective AI systems that cause contractual harm. A developer should bear liability where: (i) the AI system contains a defect in design or training that causes foreseeable contractual errors; (ii) the developer failed to disclose known limitations or vulnerabilities; or (iii) the system's autonomous capabilities exceed those reasonably marketed to operators. This tiered approach preserves the operator's primary attribution while creating incentives for developers to exercise due diligence in system design and transparency, thereby clo-

[60] In February 2025, European Commission, *Withdrawal of the Artificial Intelligence Liability Directive Proposal*, 2025, citing "no foreseeable agreement" among EU institutions. The AILD aimed to harmonize non-contractual civil liability rules for AI-related harm, introducing measures such as a rebuttable presumption of causality and disclosure obligations. The withdrawal raised concerns about legal fragmentation and the adequacy of existing liability frameworks for AI-induced damages across Member States.

sing the producer accountability gap left open by current contract-focused instruments.

Both documents lack explicit provisions requiring AI transparency in automated contracting. Given the complexity of machine learning models, contracting parties, particularly consumers, may be unaware of how AI-generated contract terms are formed. This raises fairness, accountability, and interpretability concerns, as parties may not have access to clear justifications for AI-driven contractual decisions. EU consumer law must address the rise of AI-powered assistants ("Custobots") in consumption decisions, including the need to balance mandatory disclosures, AI vulnerabilities, and potential shifts in information duties as AI systems take on more decision-making roles.

A regulatory framework should mandate AI explainability and auditability, ensuring that contracting algorithms provide human-readable explanations of key contract terms, risks, and obligations. Additionally, data provenance and input validation mechanisms should be required to trace how contractual decisions are made, preventing fraud, manipulation, or unfair contractual obligations. The EU AI Act's high-risk AI classification should apply to AI-driven contract negotiation tools, imposing stricter compliance obligations.

Neither document fully examines blockchain-based smart contracts and their interaction with traditional contract law. While Prof. Wendehorst's Principles acknowledge algorithmic contracting, they do not address self-executing smart contracts on distributed ledger technologies (DLTs), which pose unique legal challenges, including immutability, automation risks, and lack of legal override mechanisms. When fusing the AI aspect to the smart contract through IOT, for example, in the case of parametric insurances for payouts, it is important to address the issues of contract formation and performance. Also, to note, what is applicable to AI contracting in legal terms but is not directly applicable to AI-driven or AI-infused smart contracts.

Further, in terms of the EU law on smart contracts, art. 36 of the Data Act introduces a unique provision on smart contracts in data-sharing agreements, ensuring safe termination and compliance safeguards.[61] While it acknowledges their role in data governance, it does not explicitly establish them as the primary enforcement tool for data-sharing obligations. But is it foolproof? Not entirely. The EU's stance on automated contracting, including deterministic AI in this context and smart contracts, remains an

[61] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), in OJ L 342/1, 22.12.2023, art. 36.

evolving challenge. Art. 36 lacks clear technical enforcement mechanisms and leaves critical gaps in compliance, reversibility, and liability. The effectiveness of this provision will depend on its implementation, industry standardisation, and the development of interoperable frameworks that bridge legal and technological constraints.

Both documents assume that existing contract law applies to AI-generated contracts without addressing jurisdictional conflicts in cross-border AI contracting. When an AI system autonomously forms a contract across multiple jurisdictions, questions arise concerning which legal framework applies, how disputes should be resolved, and whether AI-generated agreements can be enforced extraterritorially. This is particularly relevant for autonomous trading algorithms, AI-powered supply chain contracts, and cross-border smart contracts, where the governing law may be unclear or contested. Future regulatory frameworks should include default jurisdictional rules for AI-driven contracts, possibly modelled on private international law principles such as those found in the Rome I Regulation (EU) and the Hague Principles on Choice of Law.[62] Additionally, AI-generated contracts should include explicit jurisdictional clauses to mitigate uncertainty and ensure enforceability.

Both documents lack concrete requirements for human oversight in AI-driven contracting. While AI can autonomously execute contracts, certain high-risk transactions, such as financial agreements, healthcare service contracts, or consumer credit agreements, should include mandatory human-in-the-loop (HITL) review mechanisms. AI-driven contracts should be subject to tiered oversight levels, where high-value or high-risk transactions require human approval while low-risk, standardised contracts can proceed autonomously. Additionally, businesses deploying contracting AI systems should maintain real-time monitoring systems to detect unexpected deviations, potential legal violations, or contract execution failures. Establishing audit logs for AI decisions would ensure accountability and provide regulators with evidence in case of disputes.

Both documents overlook the need for interoperability standards in AI contract generation systems. Currently, AI contracting systems operate in silos, using proprietary algorithms and data models that hinder cross-platform compatibility. A lack of standardisation creates legal uncertainty when AI systems interpret contract clauses differently across platforms.

[62] Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Recast); Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II); Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

Establishing global AI contracting standards, similar to INCOTERMS for international trade contracts,[63] would enhance predictability, enforceability, and compatibility across AI-driven legal frameworks. Additionally, an ISO-style regulatory framework for AI contracting could define baseline rules for AI contract negotiation, execution, and dispute resolution.

Neither document sufficiently addresses data privacy risks in AI-driven contract generation. AI contracting systems rely on large datasets to predict contract terms, personalise agreements, and assess contractual risks, but this raises GDPR compliance issues when personal data is processed without explicit consent. Contracting platforms should be required to implement data minimisation principles, transparency in AI decision-making, and opt-out mechanisms for automated contract personalisation. Furthermore, privacy-preserving AI techniques, such as federated learning or homomorphic encryption, should be encouraged to ensure that contract data is processed securely without exposing sensitive information.

3.5 Other European Provisions impacting Contract Law and Consumer Protection

Current platform regulations, such as the E-Commerce Directive (2000/31/EC),[64] provide a foundation for addressing certain aspects of algorithmic decision-making, particularly in the context of online services. However, these directives fall short of comprehensively regulating automated contracting. The E-Commerce Directive focuses on ensuring transparency and liability exemptions for information society services, yet it does not address the complexity of automated decisions, such as dynamic contract modifications or platform-driven AI-based decisions that impact contractual relationships. For a more thorough regulatory framework, this section explores whether existing legal frameworks are sufficiently adaptable to AI-driven contracting or whether specific measures addressing AI's evolving role in contract law, along with targeted legislative reform, are required.

The scarcity of legal cases on automated contracting is notable. Because discussions remain largely hypothetical in the absence of litigation, ob-

[63] International Chamber of Commerce (ICC), *INCOTERMS® 2020: Rules for the Use of Trade Terms in Domestic and International Contracts*, Paris, 2019.

[64] Given that the E-Commerce Directive (Directive 2000/31/EC) confirms the legal validity of contracts concluded by electronic means, it can be understood to extend to contracts concluded by AI systems, insofar as the contract is formed through an electronic process. While the Directive does not explicitly mention artificial intelligence, its technology-neutral language and objective of facilitating electronic commerce support the interpretation that AI-driven contract formation falls within its scope.

servers (including Prof. Wendehorst) have focused on developing guiding principles to pre-emptively clarify the law. Such scarcity of legal cases on automated contracting can be attributed to a combination of factors. On one hand, existing foundational elements of contract formation, or what we can refer to as rules under the Principles of European Contract Law (PECL),[65] which are specific, structured norms that directly determine legal outcomes, such as offer, acceptance, and intention, are broad and flexible enough to address disputes involving automation, potentially reducing the need for litigation. On the other hand, a lack of awareness about the unique challenges posed by automated contracting, such as attribution of actions and liability for errors, might deter parties from bringing these issues to court. Furthermore, businesses often resolve disputes informally or through private arbitration to avoid setting legal precedents that could lead to regulatory scrutiny. Prof. Wendehorst highlights the «surprisingly little legislation on automated contracting» but not the scarcity of legal precedents.[66] Prof. Wendehorst stresses the need for developing principles that can inspire the future development of law as well as guide courts and practitioners in future automated contract-related disputes.

ELI Guiding Principles and Prof. Wendehorst's Principles give solid scaffolding for consumer AI contracting basics but leave the heavier structural beams of data governance, cross-border enforcement, B2B use, bias audits, agency doctrine, and IP ownership for later builders to install. Prof. Wendehorst's Principles are drafted for general automated contracting, whereas ELI focuses only on consumer deals. Business-to-business, platform-to-consumer, and "custobot" supply-chain scenarios therefore still lack a coherent framework. Neither instrument sets out how to decide the forum, applicable law, or enforcement when an AI agent concludes a transaction across multiple countries, a gap already flagged by private-international-law commentators.[67] Common-law questions such as when a human principal is bound (or can revoke) an AI agent's acts, or how to unwind an unauthorised order, are still "murky waters" in practice.[68] Both texts expect non-manipulation, but they stop short of prescribing concrete bias-testing, fairness metrics, or redress mechanisms for high-risk agent misalignment that regulators are now demanding. Questions over who owns and who is liable for IP generated or infringed by autonomous agents are highlighted in current case law commentary but are not tackled

[65] Commission on European Contract Law, Principles of European Contract Law (PECL).

[66] C. Wendehorst, *Principles for AI in Contracting*, cit., 3.

[67] W.S. Galkin, *AI Impact on Contract Law*, in *galkinlaw.com,* 9 May 2025.

[68] Lewis Silkin LLP, *The Rise of AI Agents: Pizza, Parameters and Problems*, in *lexology.com*, 28 January 2025.

in either set of principles. Further, the pending EU Digital Fairness Act is a consumer-interface fix, not a full AI-contracting code. It targets dark patterns, addictive design, influencer marketing and profiling transparency, and aims to plug those specific fairness gaps in current consumer law. It says nothing about ratification rules for autonomous agents, cross-border contract law, B2B deals, IP ownership or other open issues we listed, so most of those gaps remain.

4. Common Law vs. Civil Law Approaches: Comparative Analysis: European Regulatory Initiatives vs. U.S. Common Law

Another consideration in this regard is the flexibility of common law systems. Unlike codified legal systems, common law jurisdictions rely on a precedent-based approach, which shapes the evolution of contract law through judicial decisions. While common law is often perceived as more adaptable due to the absence of a comprehensive civil code, judicial constraints, such as adherence to precedent, also play a significant role in shaping its application.[69] As has been observed in legal theory, certainty and flexibility in law often serve overlapping purposes. While certainty aims to provide stability and predictability, flexibility ensures that legal norms remain adaptable to new and unforeseen circumstances.[70] This tension is especially pronounced in the domain of automated contracting, where evolving technologies demand both consistent application and context-sensitive adaptation. How this approach interacts with the complexities of automated contracting remains an open question, as it may allow for nuanced interpretations based on emerging cases while also presenting challenges in ensuring consistency and predictability.

Assuming that the common law's adaptability can be advantageous, it evolves through judicial decisions, allowing courts to interpret and adapt contract law elements in the context of AI systems. This adaptability provides a valuable framework for addressing novel issues, such as determining liability for AI's autonomous actions or assessing whether AI systems align with the contractual intent of the parties. As AI technology progresses, common law jurisdictions may be positioned to develop innovative solutions, influencing global discussions on regulating algorithmic contracts.

However, this flexibility does not come without its challenges. While the

[69] For a more in-depth analysis of the superior effectiveness of common law as opposed to civil law see N. Garoupa – C.G. Ligerre, *The Syndrome of the Efficiency of the Common Law*, in *Boston University International Law Journal*, 29, 2011, 287 ss.

[70] M. Sales, *Certainty and Flexibility in Legal Norms*, Working Paper, 2025, 2.

U.S. may be seen as a favourable environment for AI-driven corporate ventures due to its legal flexibility, there are concerns about the protection of contractual parties, particularly consumers and smaller businesses, who may not have the same negotiating power as large corporations and their decision makers (typically board members). The absence of comprehensive regulation on automated contracting in the U.S. means that the contract law under the Uniform Commercial Code (UCC)[71] and state-level common law serve as the governing framework, supplemented by sector-specific regulations where applicable. Yet, this reliance on existing legal structures raises questions about the sufficiency of protections for less powerful parties in the face of technological advancements and the increasing dominance of major corporate players.

Additionally, the U.S. legal framework provides protections for businesses through mechanisms such as freedom of contract and intellectual property rights. However, it is important to note that intellectual property law, particularly in the context of AI technologies, has faced significant scrutiny due to the unprecedented number of claims regarding violations of IP rights. These cases have highlighted some of the limitations of IP law, particularly in addressing the unique challenges posed by AI's autonomous capabilities.

In terms of legislation, many U.S. states have enacted or at least supplemented their legislation addressing blockchain technology, smart contracts, and verifiable credentials. These legislative efforts aim to provide legal recognition and frameworks for the use of smart contracts and related technologies within their jurisdictions. However, this reference is limited in scope, as the focus here is on automated contracting, which extends beyond smart contracts to include AI-driven contract formation, execution, and enforcement. Prof. Wendehorst highlights the limited legislative attention to automated contracting, with existing laws such as the U.S. Uniform Electronic Transactions Act (UETA) 1999,[72] the Model Computer Information Transactions Act (MCITA) (1999/2002),[73] and the Draft UCC Article 2 (2003)[74] only offering partial guidance rather than a comprehensive legal framework. Prof. Wendehorst observes, these offer «partial guidance rather than a comprehensive legal framework». UETA covers formation and signatures, MCITA, only law in two states, addresses software licensing and has provisions on electronic errors, and the UCC drafts would have addressed electronic contracting in sales. But none

[71] Uniform Law Commission, *Uniform Commercial Code (UCC).*

[72] Uniform Law Commission, *Final Act – 2021 Uniform Law Commission Drafting Committee*, 2021.

[73] *Ibid.*

[74] Uniform Law Commission, *Uniform Commercial Code (UCC), Draft Article 2*, 2003.

squarely grapple with advanced AI autonomy or liability nuances. Thus, gaps remain – for example, if an AI behaves fraudulently (could the user be liable for fraud if they didn't know the AI would do that?), or how to handle AI collusion (antitrust law question), or whether an AI's "knowledge" could be imputed to the principal for purposes like contract enforcement, e.g., noticing an offer term that a human might have overlooked. These questions the common law will handle incrementally. The U.S. approach, favouring freedom of contract and existing legal structures, raises questions about the sufficiency of protections for less powerful parties in the face of major corporate players. A big AI user (say, Amazon) and a consumer are not on equal footing; without specific rules, the consumer relies on courts to protect them via general doctrines. There's an ongoing debate in U.S. legal circles about whether any new laws are needed (some have proposed updates to the UCC or new uniform laws to address AI agents, but nothing concrete has passed).

The U.S. handles AI contracting under status quo contract law: valid if it looks like a contract, the user bears responsibility, there are no special duties to disclose AI use, and terms stand unless voidable under traditional defenses. It's a pragmatic approach that treats AI as just another tool (like a telephone or fax in earlier times) rather than a game-changer that demands new contract rules. This minimisation of legal change works well for now in many scenarios, but it may be tested by more complex AI behaviours. U.S. law, being largely reactive, will evolve as cases present new twists, a process that could lead to unique precedents (case law) rather than a cohesive statute.

A U.S. Professor, at the Münster Colloquia it was argued that, despite the unpredictable nature of automated contracting, the existing guardrails in contract law can still protect consumer intent.[75] This assertion reinforces the argument that common law's inherent flexibility, coupled with judicial interpretation, aims to provide a safety net for contractual parties, ensuring that AI-driven contracts remain aligned with fundamental legal principles. For instance, courts can invoke the covenant of good faith if one party's AI behaviour undermines fair dealing, or they can interpret contracts in light of reasonableness to prevent AI literalism from imposing harsh outcomes. Indeed, courts can still use the existing guardrails of contract law to protect consumers. The fact that they can use them does not, however, make those contractual rules the most adequate.

The U.S. stance is underpinned by a belief in the flexibility of common

[75] H. Gabriel, *What Does It Mean to Have "The Intention to Contract" in an AI Contract?*, paper presented at the Münster Colloquia on EU Law and the Digital Economy, Conference on AI and Automated Contracting, University of Münster, 9–10 January 2025, available at *jura.uni-muenster.de* (accessed 13 November 2025).

law to evolve organically. As noted, common law adapts through judicial decisions; American courts can extend principles or create nuanced distinctions as new fact patterns (like AI contracting disputes) come before them. Proponents of this approach argue it allows innovation to flourish without waiting for legislation and avoids the risk of rules that might soon become obsolete in the face of rapidly advancing AI tech. This view was echoed at the Münster Colloquium by the U.S. professor. The flip side is the concern that common law development may be slow and uneven. Until many cases are litigated, uncertainty remains. And common law evolution happens through often costly litigation, which can be burdensome, especially for individuals or small businesses. Additionally, American common law's adaptability might be constrained by adherence to precedent, a court might feel bound by old analogies that don't perfectly fit AI contexts . There's also the issue of fragmentation: with 50 state jurisdictions, different courts might reach divergent conclusions on AI-related issues, leading to inconsistency though adoption of UETA by most states mitigates some differences on formation.

The European and U.S. approaches to AI contracting reveal a philosophical divide: ex ante rulemaking and harmonisation versus ex post adjudication and flexibility. This section compares how each addresses the key issues of contract formation, liability allocation, disclosure, and enforceability, highlighting the implications for legal certainty and party protection. Both jurisdictions ultimately affirm that contracts formed by AI are valid, but they arrive there differently. In Europe, the intent is to explicitly codify this principle (through instruments like the UNCITRAL MLAC and potential EU laws) to remove any doubt. Art. 5 of UNCITRAL and Wendehorst's first principles provide clear statutory assurance that lack of human involvement is no cause for invalidity. The U.S., by contrast, relies on existing legal principles (UETA and case law) that have already implicitly or explicitly recognised automated contracting (Uniform Electronic Transactions Act n.d.). UETA's adoption in 49 states gives near-uniform coverage, so practically there isn't doubt in the U.S. either that AI contracts can be valid. The difference is one of framing: the EU would articulate this in new legislation (for coherence across member states), whereas the U.S. points to the established e-commerce laws and says the matter is settled. For cross-border contracts, Europe's approach might foster greater confidence if, say, an EU directive mandated all member states to honour AI-formed contracts akin to the MLAC, reducing choice-of-law concerns. However, in the European Union, the regulation of contract formation remains primarily within the competence of the Member States. General principles governing the creation of contracts, such as offer, acceptance, intention to create legal relations, and capacity, are rooted in national private law traditions and have not been subject to comprehensive harmoni-

sation at the EU level. The EU lacks a general legislative competence over contract law and may only act in this area when it intersects with specific competences conferred by the Treaties, such as consumer protection (art. 169 TFEU) or the functioning of the internal market (art. 114 TFEU). Accordingly, the EU has adopted targeted directives that regulate aspects of contract formation in defined contexts, notably in cross-border consumer contracts and digital transactions, such as the E-Commerce Directive (2000/31/EC) and the Consumer Rights Directive (2011/83/EU).[76] These instruments harmonise certain elements, like information duties and the right of withdrawal, but leave the broader framework of contract formation untouched. Thus, while EU law influences certain sectors, the foundational rules governing how contracts are formed remain a matter of national legal autonomy. It will be rather interesting to see how this will be dealt with by the Commission after the UNCITRAL's MLAC.

The U.S. approach has already harmonised state law via UETA for domestic purposes. Both approaches are thus aligned on outcome (validity), but Europe's is more proactive and uniform by design, whereas the U.S.'s is uniform by voluntary adoption of a model act and judicial consensus.

Europe is introducing the idea (through ELI/Wendehorst) of aligning AI actions with human intent explicitly. That serves to reassure that even if an AI acts, we conceptually trace it back to a human's intention (at least at the point of deploying the AI or setting parameters). U.S. law similarly uses the fiction of the user's intent being present via programming.[77] The main difference is that European discussions might lead to an explicit requirement that AI systems be used in a way that honours the intended agreement of the parties, possibly even implying an obligation to avoid or correct outcomes that stray from what the parties actually wanted.[78] U.S.

---

[76] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, in OJ L 304, 22.11.2011, 64 ss.

[77] P. Cramer – J. Mollod – C. Rimmer, *Contract Law in the Age of Agentic AI*, cit.

[78] Although not a piece of perfection, the European paradigm, underpinned by both the ELI/Prof. Wendehorst touches on embedding explicit legal obligations within AI system design to ensure that automated negotiation tools operate *strictly* in alignment with the parties' intended agreement. The ELI framework operationalises eight high-level principles into 25 enforceable model-rule articles requiring design mandates that not promise to only empower the consumer but build in legal triggers for corrective action where AI-generated terms diverge from agreed intent. Meanwhile, Prof. Wendehorst's principles serve as the policy blueprint, emphasising attribution of digital assistant actions to the deploying user, extension of consumer-law coverage to algorithmic contracts, transparency, no-barrier access, and conflict-of-interest disclosure, all of which underpin an architecture in which deviation is not tolerated and must be corrected. Together, these initiatives suggest a legal regime in which AI systems may indeed bear explicit obligations to honour intent with built-in design controls and enforceable consumer-law mechanisms that mandate detection and correction of any outcome inconsistent with

law would handle that if it rises to the level of mistake or misrepresentation, but not otherwise. So, Europe could see a slightly more subjective bend (protecting actual intent), whereas the U.S. is firmly objective (if the AI manifested assent, that's the contract, regardless of unexpressed intent).

Here, Europe leans toward clarity and possibly a bit of new allocation in extreme cases, whereas the U.S. sticks to traditional allocation (user liable) with narrow escape routes. UNCITRAL's default (user of AI is bound) mirrors UETA's rule: both converge on the principle that the person who uses an AI agent bears the consequences of its actions.[79] So, there is strong transatlantic alignment on the baseline rule of attribution. The difference emerges with Europe's consideration of unexpected outcomes. The UNCITRAL model (with art. 8) explicitly gives the defrauded/erroneously bound party an out if certain conditions are met. ELI and Wendehorst also contemplate fall-back liability rules for unexpected AI behaviour, likely meaning a structured relief maybe shifting liability to the other party or allowing contract avoidance. The U.S. has no statutory equivalent; it would rely on general doctrines and the equitable sense of a judge. In practice, a U.S. court might reach a similar result to an art. 8 scenario by saying there was no meeting of minds or by rescinding for mistake if the other party should have known. But it's not guaranteed – it requires judicial discretion. The European route seeks to ensure legal certainty by defining when an AI-caused contract isn't enforceable, whereas the U.S. leaves it uncertain but flexible.

Another point: Europe's discussions include developer liability or third-party liability in the context of AI contracting. While contract law itself in Europe will likely not impose contract liability on developers (privity remains between contracting parties), the EU is concurrently exploring AI liability in tort (the proposed and withdrawn AI Liability Directive and revised Product Liability Directive). This means Europe is thinking more holistically: if an AI defect causes contractual damage, perhaps the developer can be held accountable through those instruments. The U.S. similarly would use product liability tort to handle developer fault. So, both see that as outside contract law but relevant for overall liability.

One more subtle distinction: agency law vs. sui generis rules. The U.S. could apply agency concepts (like apparent authority) if, for example, someone's AI makes a deal, and a third party reasonably believes it was authorised. Europe might incorporate a similar idea. UNCITRAL allows parties to define attribution rules contractually, but by writing explicit rules, they might supersede or supplement traditional agency doctrine. A

what the parties actually agreed.

[79] P. Cramer – J. Mollod – C. Rimmer, Contract Law in the Age of Agentic AI, cit.

European regulation might say that the operator of the AI is deemed to have given it authority up to X, leaving less ambiguity. In the U.S., a scenario where a rogue AI did something arguably unauthorised could become a factual agency dispute (with potential outcomes of binding or not).

This is a notable divergence. European initiatives strongly emphasise transparency obligations, e.g., ELI's principles on pre-contractual information and disclosure duties.[80] The EU tends to impose duties to inform in consumer law (consider the extensive information requirements in consumer rights directives). It is likely that any EU approach to AI contracting will require at least that consumers are informed when they are interacting with an AI (complementing the AI Act's general transparency rule) and possibly that businesses disclose certain algorithmic practices. This is seen as necessary to ensure informed consent and trust in AI-mediated deals. The U.S., valuing freedom of contract and minimal interference, has not required such disclosure (except in niche state laws).

As a result, if a European and an American company each deploy an AI negotiator, the European one might be legally required to tell its counterpart that you are dealing with an AI agent, whereas the American one wouldn't unless California BOT law applied or it was in a context that triggers AI Act transparency to EU users. Over time, this could mean European consumers will expect to be told about AI involvement and can object or ask for human oversight, whereas American consumers might not even know. The practical effect is that Europe's approach could enhance fairness and autonomy; humans can decide to continue or ask for a human agent, but it may introduce overhead and potential friction in automated processes. The U.S. approach allows seamless AI-to-human or AI-to-AI interactions without mandated interruptions, arguably fostering efficiency.

Another aspect of transparency is explainability or disclosing AI parameters. The ELI principle 7 about determination/disclosure of parameters hints that Europe might require companies to disclose key factors or constraints of their AI systems in consumer contracts.[81] For example, if an AI car-buying service only searches certain dealerships or won't consider cars above a certain mileage, maybe the consumer should know that. U.S. law would consider that purely the user's responsibility or the service's voluntary feature, no law compels such detail.

Ultimately, Europe appears poised to bake transparency and disclosure obligations directly into the contracting framework (or at least strongly encourage them via model rules), whereas the U.S. relies on general anti-fraud and market forces for transparency. This reflects the broader regu-

[80] European Law Institute (ELI), *Interim Report: EU Consumer Law and Automated Decision-Making (ADM)*, Vienna, December 2023, available at *europeanlawinstitute.eu*

[81] ELI, *Interim Report on EU Consumer Law and ADM*, cit.

latory philosophies: the EU tends to impose positive duties on businesses for consumer protection, while the U.S. often relies on policing fraud and letting the rest be governed by contract and competition.

The EU has a more paternalistic tradition in consumer contracts, unfair terms control, mandatory rights, etc., and this will extend to AI. EU consumer law is being reviewed for ADM-readiness, as ELI did, ensuring that if an AI contract might circumvent some consumer rights, the law is adjusted. The ELI interim report found the directives mostly adequate with minor tweaks.[82] One can foresee explicit clarification that, for instance, a consumer using an AI does not lose their 14-day withdrawal right for distance contracts; the AI cannot waive it. Or that if an AI agrees to an arbitration clause, it's only binding if it meets normal validity requirements in EU law and may be subject to unfair terms scrutiny. The Unfair Contract Terms Directive will surely apply to AI-generated terms the same as any; if a term is unfair, causes a significant imbalance, and is not individually negotiated in B2C, it won't bind the consumer, even if an AI accepted it. Perhaps new guidance will note that the fact that a consumer's own AI negotiated a term doesn't count as individually negotiated if the consumer didn't truly understand or have influence over it. This would maintain consumer protections.

In the U.S., enforceability of terms is broad; the unconscionability doctrine exists but is narrower than EU unfair terms law. So, a potentially interesting divergence: an AI might agree to something a human consumer wouldn't, and in the EU, that term might get struck as unfair, whereas in the U.S., it might stand unless it's extreme enough to be unconscionable or illegal. This means European consumers could end up more shielded from certain exploitative outcomes of AI contracting.

A lawyer counselling a multinational company would note that in Europe, they may need to build in compliance for transparency and accountability and possibly adjust contract terms to comply with any new rules on AI-caused mistakes, whereas in the U.S. they have more freedom but also more uncertainty as to how a court might treat a weird AI scenario. The European regime (once finalised) could offer more predictability; companies know the rules of the road for automated contracts, at least within the EU single market. The U.S. regime is predictable to the extent it's just standard contract law but unpredictable in novel situations lacking precedent. Businesses favour certainty in enforceability, so many might welcome clear rules (hence support for UNCITRAL's model by global companies).

The U.S. flexibility arguably encourages faster adoption of AI, for contracting companies can experiment without needing to fulfil new legal requirements first. This favourable environment for AI-driven ventures

[82] *Ibid.*

is noted in the U.S., which may be seen as a favourable environment for AI-driven corporate ventures due to its legal flexibility. Europe's approach might impose some compliance costs or slow certain fully autonomous implementations (if, say, mandatory disclosures or human oversight are required in some cases). But Europe's aim is to ensure trust and uptake in AI by having safeguards. In the long run, both seek to promote AI in commerce, but Europe is more comfortable doing so with guardrails. The U.S. might adjust if real problems emerge; e.g., if consumers start being harmed by unseen AI negotiation tactics, political pressure could lead to targeted regulation or at least FTC guidelines (the U.S. FTC has hinted at scrutinising AI practices under its broad consumer protection mandate).

In conclusion, European and U.S. approaches are convergent in acknowledging AI contracts as valid and treating AI as a tool of humans but divergent in prescribing specific duties and remedies. Europe's path, through instruments like the ELI/Wendehorst principles and potential EU laws, strives for at least some level of legal certainty, harmonisation, and integrated consumer protection. The U.S. path relies on the adaptability of common law and existing statutes, favouring minimal intervention until absolutely necessary. For global businesses, this means navigating a possibly stricter regime in the EU with obligations to disclose AI use and handle AI mistakes in prescribed ways versus a more *laissez-faire* regime in the U.S., but with the uncertainty that courts might later impose limits unpredictably.

Both approaches have merits: Europe's provides a limited level of clarity and preventative safeguards, whereas the U.S.'s provides flexibility and immediate practicality. Over time, we may see some convergence. If the EU model proves workable and beneficial, U.S. legal thought might borrow concepts (for example, the future Restatement of Contracts could mention electronic agents). Conversely, if the U.S. experiences problems, it might accelerate regulatory responses, which could end up looking like what the EU is now contemplating.

5. Conclusion: Policy Considerations and Future Directions

The analysis conducted throughout this article demonstrates that the European legal framework for AI-driven contracting remains fragmented, incomplete, and conceptually unbalanced. While international and European initiatives, such as the UNCITRAL Model Law on Automated Contracting, the ELI Guiding Principles, and Professor Wendehorst's Principles, each provide valuable insights, none alone offers a coherent doctrinal basis capable of reconciling technological autonomy with the

foundational requirements of contract law. The resulting legal landscape is characterised by partial harmonisation, inconsistent allocation of liability, and insufficient protection of parties interacting with non-human agents. The proposed hybrid regulatory model therefore seeks to move from this fragmentation toward coherence by integrating and systematising the most robust elements of these instruments within a single European framework.

The model rests on three interdependent pillars. The first concerns validity, affirming that contracts generated by AI systems should not be denied legal effect solely due to the absence of direct human agency, provided that they satisfy the principle of functional equivalence and reflect a traceable manifestation of intent attributable to a human actor. The second pillar addresses liability, establishing a differentiated regime that allocates responsibility according to the role and influence of each actor involved in the AI system's design, deployment, and operation. Accountability can no longer remain confined to the contracting parties alone but must extend, under certain conditions, to developers and intermediaries whose technical or commercial choices materially shape contractual outcomes. The third pillar concerns transparency and human oversight, requiring that parties be informed of the use and operational parameters of AI systems in contractual processes and that meaningful human control be preserved at critical decision points to ensure fairness, predictability, and compliance with European values of autonomy and trust.

From a de *iure condendo* perspective, these three pillars translate into concrete legislative recommendations. The European Union should consider supplementing the AI Act with a dedicated legal instrument, potentially a directive or regulation on automated contracting, clarifying the validity, attribution, and liability of AI-mediated transactions. This instrument should harmonise rules governing digital representation and automated contracting across member states, ensuring cross-border consistency. It should also introduce a layered approach to liability, distinguishing between deployers, developers, and users according to their capacity to control the system and foresee its consequences. Finally, transparency and human-oversight obligations should be made mandatory for AI systems capable of autonomously concluding or materially influencing contracts.

At the same time, scholarly and industry debates reveal diverging perspectives on the desirability and extent of regulatory intervention. While some scholars maintain that existing European contract law principles grounded in autonomy, consent, and risk allocation are sufficiently flexible to accommodate AI contracting, others contend that specific legislative measures are indispensable to ensure legal certainty and uniform application across the Union. The European Commission's ongoing consultations confirm the importance of balancing regulatory clarity with the

interests of businesses, particularly small and medium-sized enterprises, which often express concern about excessive regulatory burdens. In this respect, potential policy directions include the adoption of sector-specific guidelines to address contractual practices in distinct markets, the enhancement of liability-attribution frameworks to ensure fairness in AI-mediated relationships, and the establishment of procedural safeguards for AI-induced contractual errors and misunderstandings.

As AI systems continue to reshape contractual processes, the European legal order must evolve not only to address but also to clarify the challenges raised by automated contracting. Whether through the adaptation of existing frameworks or the adoption of new legislative instruments, achieving regulatory clarity is indispensable for fostering trust, accountability, and innovation in AI-driven contractual relations. The European Commission's forthcoming policy choices will thus play a decisive role in shaping the future of AI contracting in Europe, determining whether the transition from fragmentation to coherence will remain a scholarly aspiration or become a tangible legislative achievement.

Abstract

The increasing use of AI in contract formation challenges EU private-law principles like those of consent, attribution, and liability. Existing efforts like UNCITRAL's Model Law, the ELI Guiding Principles, and the EU AI Act, address aspects of algorithmic contracting but remain fragmented. This article argues for a hybrid EU model: *de iure condito*, recognise AI-generated contracts via functional equivalence; *de iure condendo*, adopt a differentiated liability regime allocating responsibility between deployer and developer. It also calls for mandatory transparency and human oversight to secure accountability and trust. Integrating international and European initiatives, the framework enhances legal certainty, supports innovation, and protects contracting parties in the digital market.

Keywords

automated contracting – AI regulation – UNCITRAL – AI Act – algorithmic governance

Put the Genie Back in the Lamp? AI-Based Biometric Systems and Fundamental Rights Protection in the European Union Artificial Intelligence Act*

Giulia Formici

Table of contents

1. Biometric Surveillance in the Age of Artificial Intelligence: Legal Challenges and Risks. – 2. From the General Data Protection Regulation to the Artificial Intelligence Act: The EU Regulatory Responses to Automated Biometric Systems. – 2.1. Biometric Data and Fundamental Rights Before the Artificial Intelligence Act: The Role of Legislators, Courts and National Data Protection Authorities. – 2.2. From Data to Technology. Navigating the Artificial Intelligence Act and AI-Powered Biometric Systems: Between Prohibitions and Exemptions. – 3. The Constitutional Governance of AI-Powered Biometric Systems: From Dystopia to Dignity. – 3.1. Assessing the AI Act Approach to Biometric Identification Systems: Regulatory Ambition and Legal Uncertainties. – 3.2. Present and Future of Biometric Systems in the EU: Mastering the Genie of the Lamp for Good?

1. Biometric Surveillance in the Age of Artificial Intelligence: Legal Challenges and Risks

«The capability to identify individuals and to associate personal attributes with an individual has been crucial to the fabric of human society»[1].

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

This paper is an outcome of the research project "AI-Biometric Systems and Fundamental Rights Protection: Legal Challenges and Regulatory Solutions in a Comparative Perspective", coordinated by Giulia Formici, granted by the University of Parma through the Action "Bando di Ateneo 2024 per la ricerca".

[1] A. K. Jain *et al.*, *Introduction to Biometrics*, Cham, 2025, 1, also recalling the work of Alphonse

Within this context, biometric systems – tools employed to «identify or verify the identity or a claim of persons on the basis of the automated measurement and analysis of their biological (such as fingerprints and iris) or behavioural (such as signature and voice) characteristics»[2] – have played a longstanding role[3].

Based on biometric data[4] and biometric datasets[5], these technologies have recently undergone a significant transformation, driven by their integration with Artificial Intelligence (AI), data analytics techniques, machine learning, computational capabilities and advanced algorithms.[6] The advent of AI has revolutionized biometric technologies[7], enabling the processing of a vast amount of data and enhancing – and partly surpassing – manual and traditional identification systems[8]. This (r)evolution has led to impro-

Bertillon.

[2] E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Cham, 2013, 1. Biometric systems are also defined as systems referring «to measurable and distinct (preferably unique) biological, physiological or behavioural characteristics (..). Typical applications for biometrics include identification but also a measure to verify access privileges», J. Skageby, *Biometrics*, in L.A. Schintler-C.L. McNeely (eds.), *Encyclopedia of Big Data*, Cham, 2022, 118; or as «automatic pattern recognition systems establishing the authenticity of an individual's physiological traits», A. Ribera Martinez, *The Debiasing Paradox: Facial Recognition Technology and Biometric Identification Systems in the Artificial Intelligence Act*, in C. van Oirsouw *et al.* (eds.), *European Yearbook of Constitutional Law 2023. Constitutional Law in the Digital Era*, Cham, 2024, 141. For more technical information on biometrics: K. Gates, *Our Biometric Future*, New York, 2011.

[3] On the role and evolution of biometric systems, see J. Pugliese, *Biometrics. Bodies, Technologies, Biopolitics*, Abingdon, 2010; S.R. Goniwada, *Introduction to One Digital Identity. Strategies, Innovations and Future Trends*, New York, 2024. For an historical analysis of the biometric identification systems' evolution, starting from the first systems employing fingerprints, see M. Smith-S. Miller, *Biometric Identification, Law and Ethics*, Cham, 2021.

[4] For a definition of biometric data in the European Union context, see Section 2.1 of the present work.

[5] It is important to highlight that biometric systems encompass two main functions: «biometric verification (BV) or one-to-one (1:1) recognition and biometric identification (BI) – which is also known as one-to-many (1:N). While BV is usually preferred in identity management systems, a typical example of identification would be a search to identify one individual among the individuals on a watch list. Both functions process biometric data», B. Sumer, *The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?*, in *EDPL*, 2, 2024, 150. As will be underlined in Section 2 of this paper, this differentiation has profound legal implications.

[6] On the functioning of AI-based systems, see, *ex multis*, C. Posthoff, *Artificial Intelligence for Everyone*, Cham, 2024.

[7] As affirmed by Fanni, «the advent of AI has represented a game changer in the field of biometrics», S. Fanni, *The Biometric Habeas Data in the Digital and Algorithmic Era in the European Union*, in *Latin America Journal of European Studies*, 3, 2023, 22.

[8] Y. Rawat *et al.*, *The Role of Artificial Intelligence in Biometrics*, in *Proceedings of the Second International Conference on Edge Computing and Applications ICECAA 2023*, IEEE, 2023; S. Balasubramaniam

ved accuracy, robustness and speed, facilitating a shift from small-scale applications to large-scale biometric infrastructures[9].

Over the past few decades, we have therefore witnessed the emergence of a new age of life for biometric systems: these technologies are increasingly pervasive, often operating in unnoticed and apparently non-invasive ways, and are gaining prominence across various domains, both private and public[10].

Private sector actors are recognizing the potential of such systems not only to improve access to services (e.g. facial recognition instruments in personal devices) but also for employee monitoring, targeted marketing and, with the development of emotional AI recognition technologies, even the inference of individuals' emotions. Moreover, these applications are being explored across diverse contexts, including mental health assessment, the monitoring of students' concentration in educational settings and employees' focus on workplaces[11].

Similarly, in the public sphere, authorities started adopting AI-based biometric systems for a wide range of security-related purposes in public spaces such as subways, airports and stadiums, as well as in predictive policing[12], smart cities initiatives[13], border management and immigration

et al. (eds.), *AI Based Advancements in Biometrics and its Applications*, Boca Raton, 2025. For more info about the functioning of biometric algorithms, see Y. Chen, J.-C. Fondeur, *Biometric Algorithms*, in S.Z. Li-A.K. Jain (eds.), *Encyclopedia of Biometrics*, Cham, 2015, 156.

[9] B. Ray, *Biometric Systems Privacy Premier*, in *Sedona Conference Journal*, 25, 2024, 163.

[10] R. Matulionyte-M. Zalnieriute (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge, 2024.

[11] This technology «relies on a device to capture a digital image of a person's face which then transmit that information to a computer which match a person's expressions to their self-reported emotional state», J.S. Bard, *Developing Legal Framework for Regulating Emotion AI*, in *Boston University Journal of Science and Technology Law*, 27, 2023, 278. On this specific technology, see also, *ex multis*: M. Durovic-T. Corno, *The Privacy of Emotions: From the GDPR to the AI Act, an Overview of Emotional AI Regulation and the Protection of Privacy and Personal Data*, in M. Ebers-K. Sein (eds.), *Privacy, Data Protection and Data-Driven Technologies*, Abingdon, 2025, 368; I. Neroni Rezende, *Facial Recognition for Preventive Purposes: The Human Rights Implications of Detecting Emotions in Public Spaces*, in L. Bachmaier Winter-S. Ruggeri (eds.), *Investigating and Preventing Crime in the Digital Era*, Cham, 2022, 67; E. Akar, *Emotional Artificial Intelligence: Introducing the Concept of 'Emotional Privacy*, in K. Prifti *et al.* (eds.), *Digital Governance. Confronting the Challenges Posed by Artificial Intelligence*, The Hague, 2024, 65.

[12] On this topic, P. Vogiatzoglou, *Mass Data Surveillance and Predictive Policing. Contested Foundations and Human Rights Impact*, Abingdon, 2025.

[13] R. Jiang *et al.*, *Big Data Privacy and Security in Smart Cities*, Cham, 2022; G.F. Ferrari (ed.), *Innovazione e sostenibilità per il futuro delle smart cities*, Milan, 2023.

control[14], and the delivery of digital welfare services[15]. This growing use of AI-powered biometric technologies is driven by a key goal: to optimizing and boosting proficiency, accuracy and speed[16].

The renewed necessity of security, along with the demand for effective information exchange, robust network capabilities and overall operational efficiency, have contributed to the implementation of expansive, large-scale identification systems. These include «real-time remote tracking of people and vehicles and the aggregation of vast amount of data on people and their movement, networks and relationships»[17].

While automated biometric systems encompass a broad spectrum of technologies, data sources, applications and purposes – including data scraping, social scoring[18], predictive policing and mind probing –[19], facial recognition (FRTs) has certainly emerged among them as a dominant technology, using «machine learning techniques to identify any faces in a digital image, create a biometric template of those faces, and check those templates against a reference database»[20].

---

[14] N. Vavoula, *Artificial Intelligence (AI) at Schengen Borders: Automated Processing, Algorithmic Profiling and Facial Recognition in the Era of Techno-Solutionism*, in *European Journal of Migration and Law*, 23, 2021, 457. Such systems are also often employed in the humanitarian sector: M. Marelli (ed.), *Handbook on Data Protection in Humanitarian Action*, Cambridge, 2024.

[15] G. Formici, *Digital Welfare State and Fundamental Rights: The Judicial Litigation on Digital Identification Systems in Kenya and Jamaica*, in *Federalismi.it*, 26, 2022, 1 ff.; on the interesting Indian Aadhaar project see, *ex multis*, A. Gurram, *Biometric (Data) governance and Digital Surveillance: A Comparative Analysis of Biopolitics in India and China*, in T. Ostbo Kuldova *et al.* (eds.), *Policing and Intelligence in the Global Big Data Era*, London, 2024.

[16] For an in-depth analysis of the benefits and potentialities of automated biometric systems for law enforcement purposes, in terms of optimization of resource utilization, acceptability and ease of use, see G.-M. Tical, *Facial Recognition and Biometric Systems: Benefits and Challenges for Law Enforcement*, in *Land Forces Academy Review*, 2, 2025, 249.

[17] N. Lynch, *Facial Recognition Technology in Policing and Security – Case Studies in Regulation*, in Laws, 13, 2024, 1.

[18] One of the most known and recognized examples of such a complex technology is represented by the Chinese Social Credit System; on the point, see E. Consiglio-G. Sartor, *A New Form of Socio-Technical Control: The Case of China's Social Credit System*, in M. Timoteo *et al.* (eds.), *Quo Vadis, Sovereignty?*, Cham, 2023, 121 ff.

[19] As regards "mind probing", aimed at «inferring information about mental properties of persons on the basis of physiological or biometric signals», see C. Bublitz, *Banning Biometric Mind Reading: The Case for Criminalising Mind Probing*, in *Law, Innovation and Technology*, 2, 2024, 432.

[20] D. Murray, *Facial Recognition and the End of Humal Rights as We Know Them?*, in *Netherlands Quarterly of Human Rights*, 42, 2024, 147 ff. For an in-depth examination of the functioning of this famous and widespread technology – which, differently from other biometric systems, is "touchless" and do not require the contact –, see M.A. Bigos, *Let's Face It: Facial Recognition Technology, Police, Surveillance and the Constitution*, in *Journal of High Technology Law*, 22, 2021, 52; N. Menendez Gonzalez-G. Mobilio (eds.), *Next Democratic Frontiers for Facial Recognition Technology*

Despite their potential, the growing sophistication, intrusiveness and widespread adoption of biometric systems by both public and private actors, have become greatly controversial. These technologies are turning ever more ubiquitous, raising unprecedented challenges to fundamental rights. Concerns about their extensive deployment continue to intensify, fuelling debates within civil society, regulatory bodies and political arenas[21]. By intruding into private lives, AI-based biometric systems could enable public or private entities to infer individuals' preferences, lifestyles, behaviours and habits. This, in turn, allows and accelerates profiling, monitoring, control and even sanctioning activities[22].

Far from depicting a sci-fi scenario, the risk of a dystopian biometric surveillance society[23] could undermine not only – and more evidently – privacy and data protection rights but also other fundamental freedoms and rights, such as freedom of expression, assembly, due process and the right to vote[24]. This so-called "chilling effect" on fundamental rights is particularly insidious – often subtle, indirect and difficult to detect –[25] and thus able to threaten the very basis and the core values of our democratic societies. It can erode public trust[26], foster a pervasive feeling of

(FRT). The Legal, Ethical and Democratic Implications of FRT, Cham, 2025.

[21] See, for instance, the famous campaign "Reclaim your Face", promoted by the NGO "European Digital Rights" (EDRi) and supported by more than 100 other organisations.

[22] P. Fussey-D. Murray, *Facial Recognition Surveillance. Policing and Human Rights in the Age of Artificial Intelligence*, Oxford, 2025.

[23] Hu, talking about the famous movie *Minority Report*, affirms that this sci-fi movie can be used as a heuristic example able to perfectly interpret complex biometric surveillance and precrime rationales; these phenomena do not represent, nowadays, a mere fantasy or dystopian parable, but rather «a governance reality», M. Hu, *Biometric Surveillance and Big Data Governance*, in D. Gray-S.E. Henderson (eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge, 2017, 121.

[24] As clearly affirmed in N.M. Richards, *The Dangers of Surveillance*, in *Harvard Law Review*, 126, 2013, 1934. Linch talks about «the significant chilling effect on an individual's willingness to publicly disclose political views when they believe their views differ from the majority», determined by the spread of such technologies and the consequent a "spiral of silence" (J. Linch, *Face Off: Law Enforcement Use of Face Recognition Technology*, Electronic Frontier Foundation Reports, 2020, 9).

[25] As affirmed by Murray, who suggests that the impact on any fundamental right should be assessed not in isolation, but in the broader context of its interactions with other rights and freedoms, using the concept of «compound human rights harm, as a means of encapsulating broader types of harm that impact on a number of different rights simultaneously», D. Murray, *Facial Recognition and the End of Human Rights as We Know Them?*, cit., 151.

[26] On this aspect, F. Paolucci, *Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems*, in N. Menendez Gonzalez-G. Mobilio (eds.), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, cit., 71. Arwert underlines how biometric identification can affect and modify societal behaviour through the so called "surveillance cue

being constantly monitored and ultimately influence individual choices and behaviour[27].

In other words, AI-based biometric systems could reveal as tools of manipulation, categorization and classification, as well as of mass surveillance, where data are gathered not for «a specific criminal investigation but rather for an undetermined purpose, serving a mentality of "nice to have" rather than "must have" intelligence»[28]. Such widespread implementations pave the way for "dataveillance" practices[29], based on massive and indiscriminate data collection and processing[30].

Moreover, the intrinsic characteristics of these systems and the data they employ introduce further concerns. Statistical methods underpinning automated decision-making are not to be considered infallible, being marked by already recognized error rates, inaccuracies[31] and algorithmic biases: these flaws can translate into discriminatory outcomes, reinforcing exi-

effect": «The necessity of constantly watching each other can create an artificial feeling of insecurity and also in the feeling that you are not trusted by the authorities. Since trust is bidirectional, this also implies that citizens are less likely to trust these authorities», I. Arwert *et al.*, *Facial Recognition in the Public Space: Challenges and Perspectives*, in J. Bayer-C. Grimme (eds.), *Code and Conscience. Exploring Technology, Human Rights, and Ethics in Multidisciplinary AI Education*, Cham, 2025, 12. In the same book, see also F. Saeed-L. Schmidt, *FRT in Public Spaces and Their Impact on Individual and Collective Behavior*, 33.

[27] As pointed out also in the vast Court of Justice of the EU (CJEU) case-law on mass surveillance and data retention (G. Formici, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Turin, 2021; E. Kosta-I. Kamara (eds.), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive*, Oxford, 2025; N. Ni Loideain, *EU Data Privacy Lawn and Serious Crime. Data Retention and Policymaking*, Oxford, 2025. Barrett talks about the capability of these technologies to produce an «erosion of practical obscurity in public», L. Barrett, *Ban Facial Recognition Technologies for Children – And for Everyone Else*, in *Boston University Journal of Science and Technology Law*, 26, 2020, 223. On this point, see also the considerations of the EU Agency for Fundamental Rights (FRA), *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, 2019 and of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Facial Recognition*, 2021. On facial recognition and the perils for rule of law: M. Qandeel, *Facial Recognition Technology: Regulations, Rights and the Rule of Law*, in *Frontiers in Big Data*, 1, 2024, 1.

[28] P. Vogiatzoglou, *Mass Surveillance, Predictive Policing and the Implementation of the CJEU and ECtHR Requirement of Objectivity*, in *European Journal of Law and Technology*, 10, 2019, 1.

[29] E. Papada-A. Vradis, *The Birth of Spatial Trasgression: Genealogies and Regulatory Instruments in the Use of Facial Recognition Technologies in the UK*, in V. Galis *et al.* (eds.), *Critical Perspectives on Predictive Policing*, Cheltenham, 2025, 42.

[30] I. Barkane-L. Buka, *Prohibited AI Surveillance Practices in the Artificial Intelligence Act: Promises and Pitfalls in Protecting Fundamental Rights*, in V. Galis *et al.* (eds.), *Critical Perspectives on Predictive Policing*, cit., 127.

[31] L. Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, in *William & Mary Bill of Rights Journal*, 30, 2021, 337, underlining the need to establish proper safeguards able to diminish the risks of misidentification.

sting inequalities[32]. Additionally, biometric data, by nature, are (almost) immutable and cannot consequently be modified, restored or reissued in the event of a data breach[33], therefore making any misuse, abuse or function creep[34] particularly dangerous.

Systems such as ClearView AI[35], implementing data scraping techniques[36] to collect biometric data aimed at building extensive databases, highlight the urgent need to safeguard sensitive data, even those voluntarily – often thoughtlessly – shared online. This example also reveals one of the most profound issues posed by biometric surveillance systems: «the incremental change from visible to invisible data collection», which undermines traditional mechanisms of "individual participation", consent and awareness[37]. This shift calls for a «new regime and status for a "novel" corporality»[38]

---

[32] On algorithmic bias and discrimination, *ex multis*, P. Schuetz, *Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for Adaptive Legal Framework*, in *Minnesota Journal of Law & Inequality*, 39, 2021, 221; E. Haber, *Racial Recognition*, in *Cardozo Law Review*, 43, 2021, 71, who talks about racial recognition underlining the racist bias to the detriment of black people and certain specific ethnical groups; see also A. Ribera Martinez, *The Debiasing Paradox*, cit.

[33] For a technical perspective on the risks of data breaches: I.-T. Stoica, *The Future Risk of Biometric Data Theft in Cybersecurity*, in *International Journal of Information Security and Cybercrime*, 13, 2024, 49.

[34] Function creep occurs «whenever the original purpose for which the data collection is justified is overreached and the biometric data is used for other purposes», P. Faraldo Cabana, *Technical and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes*, in A. Zavrsnik-K. Simoncic (eds.), *Artificial Intelligence, Social Harms and Human Rights*, London, 2023, 46. Some scholars also highlight the risks connected to the unintentional collection of additional information that can be inferred from biometric data, such as medical related information: on this point, see H. Al-Assam *et al.*, *Privacy in Biometric Systems*, in S. Zeadally-M. Badra (eds.), *Privacy in a Digital, Networked World*, Cham, 2015.

[35] In 2020 «Clearview Al had more or less secretively scraped the internet for face images of individuals and aggregated a database containing 3 billion pictures. In October 2021, the number had climbed to 10 billion pictures. When users of the company's application upload a portrait of an individual onto the application, all pictures of the individual that are stored in the database, together with the links to the websites from which the photographs were scraped, are shown within seconds. (..) By linking the portraits in Clearview's database to other online information about the data subjects, their identities are accessible to and can be compiled for anybody using Clearview's application, without the data subjects being aware of it», C. Dul, *Facial Recognition Technology vs Privacy: The Case of Clearview AI*, in *Queen Mary Law Journal*, 3, 2022, 1-2.

[36] On the face scraping or web scraping systems, see B. Zhao, *Web Scraping*, in L.A. Schintler-C.L. McNellu (eds.), *Encyclopedia of Big Data*, Cham, 2023.

[37] A. Sprokkereef-P. de Hert, *Biometrics, Privacy and Agency*, in E. Mordini-D. Tzovaras (eds.), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Cham, 2012, 97.

[38] S. Fanni, *The Biometric Habeas Data in the Digital and Algorithmic Era in the European Union*, cit.

shaped by algorithmic instruments and marked by blurring boundaries between digital, physical and biological realms, especially in contexts of AI-powered identification and verification.
Consequently, it is crucial to determine innovative safeguards, requirements, guarantees and even limitations «to prevent a dystopian digital and algorithmic surveillance from taking over»[39] and to protect what is termed "projected corporality"[40] – suggesting that the body has become endangered not only in its physical dimension but, increasingly, in its digital form. Ensuring "informational self-determination"[41] also in the face of automated biometric systems thus represents a serious and urgent challenge.
Against this backdrop and considering the pressing call for renewed regulatory solutions, the present paper aims to analyse the efforts currently underway within the European Union (EU) to develop measures and safeguards able to address the existing or emerging issues posed by the proliferation of AI-based biometric systems.
Section 2.1 provides a concise yet essential overview of the regulatory framework that characterised the legal landscape prior to the recent introduction of the Artificial Intelligence Act (AI Act)[42]. It also examines the significant – although limited – case law on AI-based biometric technologies, as well as decisions issued by national Data Protection Authorities, with particular emphasis on the Italian experience.
Section 2.2. then examines the key provisions of the AI Act disciplining AI-powered biometric systems. Finally, the concluding Section critically evaluates the current landscape, highlighting both the strengths of the existing framework and the open issues and complex questions that demand clear and comprehensive answers. These reflections are intended to provide a blueprint for further discussion on how – as suggested by the paper's title – to control the (AI-)genie of the lamp, if not return it to its world.

[39] Ivi, 24.

[40] *Ibid.*

[41] On this extremely relevant concept, see S. Rodotà, *Il diritto di avere diritti*, Bari-Rome, 2013 and, for an English version, S. Rodotà, *New Technologies and Human Rights Facts, Interpretations, Perspectives. A report for a Fundamental Rights Agency's Discussion*, in *Comparative Law Review*, 11, 2020, 29. Rodotà talks about a renewed "disaggregation" of the body (and, therefore, of the identity), determined by the collection of data able to reduce an individual's identity to a single identifying detail.

[42] 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) [2024] OJ L 2024/16.

2. From the General Data Protection Regulation to the Artificial Intelligence Act: The EU Regulatory Responses to Automated Biometric Systems

2.1. Biometric Data and Fundamental Rights Before the Artificial Intelligence Act: The Role of Legislators, Courts and National Data Protection Authorities prior to AI Act

In recent years, the abovementioned risks and challenges associated with AI-based biometric systems have become increasingly prominent in the EU social, political and legal debate. Scholars, civil society and institutions have voiced serious concerns regarding the widespread use of FRTs and the alarming rise of biometric surveillance practices[43].

Such complex and delicate discussions prompted – even prior to the adoption of the AI Act – legislators, policymakers, as well as Courts and national Data Protection Authorities, to undertake serious reflection on the necessary safeguards and regulatory solutions to be implemented. In fact, while the more recent adoption of the AI Act undoubtedly introduced tailored and unprecedented legislative provisions and obligations addressing the specific questions posed by new algorithmic and automated tools, this groundbreaking intervention benefitted from an existing – albeit fragmented – framework of safeguards that, over the past decades, has provided initial guarantees and protections for biometric data and their processing.

The General Data Protection Regulation (GDPR)[44] – characterized by a risk-based approach and combining a «constitutional-oriented perspective»[45] with the aim of ensuring the proper functioning of the EU internal data market – devotes several important provisions to biometric data. These are defined in art. 4 (n. 14), as «personal data resulting from specific

[43] Concerns and regulatory indications, suggesting specific guarantees and safeguards in this field, were also underlined by the EU Agency for Fundamental Rights (FRA), *Facial Recognition Technology*, cit., 2019 and of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), *Guidelines on Facial Recognition*, cit.; United Nations Human Rights Office of the High Commissioner, *Report: The Right to Privacy in the Digital Age*, 2021; European Data Protection Board, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 2022.

[44] 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) (Text with EEA relevance) [2016], OJ L 119/1.

[45] P. Dunn, *The Artificial Intelligence Act: A Tile in the EU's Digital Risk-Based Approach*, in O. Pollicino *et al.* (eds.), *La disciplina dell'Intelligenza Artificiale*, Milan, 2025, 141.

technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data». As is evident – through a widely discussed definitional choice[46] that has also had implications for the AI Act[47] –, the particularly sensitive nature of such data alone is not sufficient for them to be classified as "biometric" and therefore included in the "special categories of data"; on the contrary, what is also required is that the data be processed with the specific purpose of identification. As a consequence, the processing of photographs, for instance, «should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural personal» (Recital 51).

The GDPR therefore establishes that the nature, together with the intended use, of biometric data necessitate specific safeguards: the recognition of these data as part of "special categories of data" creates what has been described as «a bridge between the traditional legal regulation of secrets (where access by unauthorized third parties in itself might pose risk to the person, because of the very content of those data) and data protection law (where the protection is content-neutral, based on the link to the data subject, and the risk posed by combining and processing otherwise trivial data by digital means)»[48].

As was already the case under the previous Data Protection Directive[49],

[46] Several scholars have identified critical issues arising from the GDPR's definition of biometric data, such as the limited scope, able to restrict the applicability of GDPR's guarantees and to limit them exclusively to identification systems; on this point: E.J. Kindt, *Privacy and Data Protection Issues of Biometric Applications*, cit.; E.J. Kindt, *Having Yes, Using No? About the New Legal Regime for Biometric Data*, in *Computer Law & Security Review*, 34, 2018, 523; R. Ducato, *Il riconoscimento facciale tra rischi di "mitridatizzazione sociale" e prospettive di regolamentazione*, in L.E. Rios Vega *et al.* (EDS.), *I diritti fondamentali nell'era della digital mass surveillance*, Naples, 2021; G. Mobilio, *Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies*, in *Internet Policy Review*, 1, 2023, 1; E. Kavoliunaite-Ragauskiene, *Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union*, in *Journal of Human Rights Practice*, 16, 2024, 658.

[47] See Section 2.2 of this work.

[48] *Ex multis*, see A. Jori, *Article 9*, in I. Spiecker Dohmann *et al.* (eds.), *General Data Protection Regulation. Article-by-Article Commentary*, Munich, 2023, 403; see also C. Kuner *et al.* (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020; A. Thiene, *Commento all'Art. 9 (Trattamento di categorie particolari di dati personali) del Regolamento (UE) 2016/679 - I Principi generali*, in R. D'Orazio *et al.* (eds.), *Codice della Privacy e Data Protection*, Milan, 2021, 240.

[49] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L 281/31.

the GDPR sets out a general prohibition on the processing of special categories of data (art. 9(1)), accompanied, however, by an extensive list of exceptions. These include: explicit consent (art. 9(2)(a)); processing necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law (b); processing necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (c); processing necessary for reasons of substantial public interest (g) or of preventive or occupational medicine (h) or of public interest in the area of public health (i), as well as processing for scientific or historical research or statistical purposes (j). Moreover, art. 9(4) allows Member States to maintain or introduce further conditions or limitations regarding the processing of sensitive data. This has resulted in a fragmented and often vague regulatory landscape: the broad scope of exceptions, coupled with the intervention of national legislators, have limited the strength of the general prohibition[50].

Further fragmentation of the applicable EU regulatory framework arises from the exclusion from the scope of application of the GDPR of the processing of personal data by law enforcement authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences. Such delicate and important activities, in fact, are governed by a separate regime established under the Law Enforcement Directive (LED)[51] and the corresponding national implementing measures[52]. In par-

[50] As affirmed by Kindt, «it will be important to recognize the risks and functionalities of biometric data systems, starting from the collection and storage of the data, not just during its processing or use, and to reconsider broadly worded exceptions that provide loopholes for companies, governments and authorities to exploit», E.J. Kindt, *A First Attempt at Regulating Biometric Data in the European Union*, in A. Kak (ed.), *Regulating Biometrics. Global Approaches and Urgent Questions*, AI Now Institute, 2020, 68. Other relevant provisions can be identified in art. 6 on the legitimacy of processing (on this point, Policy Department for Citizens' Rights and Constitutional Affairs, *Biometric Recognition and Behavioural Detection Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on their Current and Future Use in Public Spaces*, 2021); art. 35 on the Data Protection Impact Assessment and art. 22 on automated individual decision-making.

[51] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

[52] "It is necessary to move toward an assessment of national legislation that either specifies the GDPR requirements or implements the LED, as Member States might adopt exemptions or derogations that modulate the safeguards eventually available to individuals when their data are processed for law enforcement and forensic purposes», P. Faraldo Cabana, *Technical*

ticular, art. 10 of the LED allows the processing of special categories of data only when strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only in cases: a) where authorized by EU or national laws; b) required to protect vital interests of the data subject or another person; or c) where such processing relates to data which are manifestly made public by the data subject.

As the abovementioned rules illustrate, both the GDPR and the LED didn't totally prohibit the processing of biometric data but rather imposed specific restrictions and additional requirements[53]. In doing so, they offered an initial framework of safeguards concerning biometric surveillance, in the absence of legislations specifically governing the underlying AI technology and the systems overall.

It is precisely on the basis of these provisions[54] that national Courts and Data Protection Authorities (DPAs) have, over the past decades, exercised various forms of oversight concerning the legitimacy of AI-based biometric systems. Through this process, they developed relevant interpretations of existing legal instruments and sought to derive protections applicable also to the deployment of AI-biometric systems.

One prominent example is the case *R (Bridges) v. Chief Constable of South Wales Police*[55], in which UK Courts addressed the world's first legal challenge to the use of FRTs by law enforcement authorities. Departing from the High Court's ruling[56] and grounding its reasoning in data protection provisions – deriving from the GDPR, in a prior Brexit phase – as well as in the European Convention on Human Rights (ECHR), the Court of Appeal for England and Wales found the live-automated FRT employed by South Wales Police violated art. 8 ECHR. The Court considered the system disproportionate and infringing on privacy and data protection rights; it also raised concerns regarding the potential impact on the principle of non-discrimination, freedom of expression and the right to peaceful

and Legal Challenges of the Use of Automated Facial Recognition Technologies for Law Enforcement and Forensic Purposes, cit., 38.

[53] Despite the critical issues and fragilities characterizing the GDPR and LED provisions concerning biometric data – i.e. the limited definition provided as well as the debated distinction between verification and identification; on these points, see Authors *supra* notes 46 and 48.

[54] It is worth mentioning that the GDPR and LED are not the only disciplines applying to biometric data: there are also other provisions in EU law regulating biometric data in specific sectors and areas such as EU border control measures (B. Sumer *et al.*, *AI Act's Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data*, in K. Prifti *et al.* (eds.), *Digital Governance*, cit., 165.

[55] *R (Bridges) v. South Wales Police*, 2020, EWCA Civ 1058, Court of Appeal.

[56] *R (Bridges) v. South Wales Police*, 2019, EWHC 2341, High Court.

assembly[57].

In the same year, the French Administrative Tribunal of Marseille ruled on the use of FRTs in schools for security purposes. In its decision No. 1901249 of 27 February 2020, the judges found the implementation of this innovative biometric technology unlawful due to the absence of a proper legal basis justifying such a significant intrusion into the private sphere, and the failure to meet the requirements of necessity and proportionality, established for the processing of biometric data. The lack of an opt-out mechanism further exacerbated the risks, with possible implications not only for data protection and privacy, but also for the right to education[58].

While the case law at both national and supranational level[59] remains limited – although relevant –, the contribution of national DPAs has been instrumental in shaping legal guarantees in response to the growing collection and processing of biometric data by automated systems. In Italy, for instance, the *Garante per la protezione dei dati personali* has intervened in several notable cases, applying the GDPR provisions. In the decisions

[57] An in-depth analysis, which also proposes some connections and parallelisms between the decision of the UK Courts and the provisions included in the EU (at that time) AI Act Proposal, see A. Pin, *A Novel and Controversial Technology. Artificial Face Recognition, Privacy Protection and Algorithmic Bias in Europe*, in *William & Mary Bill of Rights Journal*, 30, 2021, 291; but also L. Woods, *Automated Facial Recognition in the UK: The Bridges Case and Beyond*, in *EDPL*, 3, 2020, 455; A. Adimi Gikay, *Regulating Use by Law Enforcement Authorities of Live Facial Recognition Technology in Public Spaces: An Incremental Approach*, in *Cambridge Law Journal*, 83, 2023, 414; N. Ni Loideain, *Lawfulness and Police Use of Facial Recognition in the United Kingdom: Article 8 ECHR and Bridges v. South Wales Police*, in R. Matulionyte-M. Zalnieriute (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, cit., 155.

[58] On this case, F. Paolucci, *Riconoscimento facciale a scuola: il caso francese*, in *Ius in Itinere*, 8 December 2020. More generally-G. Mobilio, *When the Kids Aren't Alright: The Use of Facial Recognition Technologies at School*, in K. Prifti *et al.* (eds.), *Digital Governance*, cit., 41. See also N. Menendez Gonzalez-G. Mobilio, *Between Prohibited Risks and High Risk: The Regulation of Facial Recognition Technology*, in O. Pollicino *et al.* (eds.), *La disciplina dell'Intelligenza Artificiale*, cit., 182, for the analysis of another ruling of the French *Conseil d'Etat* on the legality of the use of FRTs in criminal investigations.

[59] ECtHR, *Glukhin v. Russia*, App. No. 11519/20, 4 July 2023. In this first decision specifically addressing FRTs, the Strasbourg judges recognized the absence of a pressing social need making the adoption of such technologies proportionate and necessary in a democratic society. On this decision, see M. Zalnieriute, *Glukhin v. Russia App. No. 11519/20 Judgement*, in *American Journal of International Law*, 4, 2023, 699; C. Jasserand, *Facial Recognition in Public Spaces and the Principle of Necessity*, in N. Menendez Gonzalez-G. Mobilio (eds.), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, cit., 49; 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 this Journal, 3, 2023, 189.

regarding *Sari Real Time*[60]*, ClearView AI*[61] or the municipality of Trento and its biometric surveillance and smart cities projects[62], the DPA blocked and/or sanctioned the use of such biometric identification technologies, emphasizing the lack of a sufficient and proper legal basis, the dangers of indiscriminate and massive surveillance and the risks to fundamental freedoms such as freedom of expression and assembly. The Authority also underlined legal challenges and unlawful practices determining pervasive sense of surveillance, potential bias and function creep, also with regards to innovative and rather unnoticed instruments of web scraping. In these decisions, the *Garante* found the processing of biometric data illegitimate, also citing a lack of transparency, insufficient accountability and the absence of a proper prior Data Protection Impact Assessment (DPIA).
All the aforementioned interventions[63], alongside the emerging case-law, marked a significant step in the evolution of the legal framework surrounding biometric identification systems. The GDPR, the LED, but also the long-standing Court of Justice of the EU (CJEU) case-law on data retention and mass surveillance mechanisms[64], together with the principles and rights established by the Charter of Fundamental Rights of the EU, have

[60] Decision No. 9309458, 26 Febraury 2020 (F. Mollo, *Il trattamento dei dati biometrici nel quadro della strategia europea dei dati, fra rischi di mass surveillance e tutela dei diritti fondamentali*, in *Nuovi Autoritarismi e Democrazie: Diritto, Istituzioni, Società*, 2, 2023, 103; A. Pin-L. Scaffardi, *Tra protezione dei dati e intelligenza artificiale, in Europa e oltre*, in *DPCE Online*, 64, 2024, 1029).

[61] Decision No. 50, 10 February 2022 (T. Sica, *Dati biometrici, tutela del singolo e opportunità di mercato*, in *Rivista di Diritti Comparati*, 2, 2022, 1; J. Piemonte, V. Papakonstantinou, *Il caso Clearview AI: uno stress test per il Regolamento generale per la protezione dei dati e la proposta di Regolamento sull'intelligenza artificiale in relazione alle nuove sfide poste dal riconoscimento facciale*, in *Ciberspazio e Diritto*, 73, 2023, 43.

[62] Decision No. 9977020, 11 January 2024. On this point, as well as on other relevant decisions of the Garante (i.e. decision No. 7496252, 21 December 2017, recognizing a differentiation between face detection and face recognition technologies), see G. Formici, *Sistemi di Intelligenza artificiale per l'identificazione biometrica*, in V. Ricciuto-R. D'Orazio (eds.), *Il diritto europeo dell'Intelligenza Artificiale*, forthcoming.

[63] More recently, the *Garante* also adopted Decision No. 10167745, 11 September 2025 on the use FRTs for face boarding operations in Italian airports; on this case, see F. Paolucci, *Riconoscimento facciale in aeroporto: tanto rumore per (quasi) nulla?*, in *Diritti Comparati*, 30 September 2025. An analysis of decisions adopted by other national Data Protection Authorities is available in I. Barkane, *Questioning the EU Proposal for an Intelligence Act: The Need for Prohibitions and a Stricter Approach to Biometric Surveillance*, in *Information Polity*, 27, 2022, 147; Policy Department for Citizens' Rights and Constitutional Affairs, *Biometric Recognition and Behavioural Detection*, cit.

[64] On mass surveillance case-law in the EU and the principles established, see, *ex multis*, S. Kuhlmann, *Government Use of Facial Recognition Technologies under European Law*, in R. Matulionyte-M. Zalnieriute (eds.), *The Cambridge Handbook of Facial Recognition in the Modern State*, cit., 127; but also G. Formici, *The Long and Winding Road: The Data Retention Discipline in the European Union Between Judicial Intervention and Legislative Resistance*, in *Verfassunsgblog*, 24 November 2024. See also the Authors recalled *supra* note 27.

all contributed to identifying risks, affirming safeguards concerning biometric data processing and limiting the emergence of indiscriminate and generalized forms of biometric surveillance.

It can therefore be stated that the EU legal landscape prior to the AI Act «[wa]s not devoid of norms that are directly or indirectly applicable» to biometric systems for identification purposes, including their use in law enforcement. However, «these various norms, which have different targets and are from multiple sources, create a kind of legal patchwork that could undermine the lawful use of this technology»[65]. In other words, the layered and sometimes contested[66] framework of supranational and national regulations applicable to the processing of biometric data failed to offer a coherent and comprehensive regime capable of properly and vastly addressing the unique and complex challenges – already highlighted in Section 1 – posed by AI-driven biometric systems. While the importance of the safeguards enshrined in the GDPR and the LED is undeniable, it is equally accurate to observe that «AI is not explicitly mentioned in the GDPR but many provisions in the GDPR are relevant to AI, and some are indeed challenged by the new ways of processing data that are enable by AI»[67].

In this context, the rapid proliferation of AI-based biometric systems underscored the urgent need for a legal framework able to regulate not only the data but also the underlying technology, thus avoiding to uniquely rely on the interpretative efforts promoted by Courts or DPAs to fill legislative gaps.

Starting from these premises and recognizing the necessity for a normative (re)action, in recent years different regulatory approaches began to surface at the supranational level. In its Resolution of 6 October 2021 on "AI in criminal law and its use by the police and judicial authorities in

---

[65] V.L. Raposo, *The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal*, in *European Journal on Criminal Policy and Research*, 29, 2022, 515; J. Purshouse, L. Campbell, *Automated Facial Recognition and Policing: A Bridge Too Far?*, in *Legal Studies*, 42, 2022, 209.

[66] According to Zalnieriute, the GDPR provisions on biometric data processing are too reliant on procedural safeguards and are not able to protect against abuse of power and violations of freedoms and rights (i.e. chilling effect), M. Zalnieriute, *Beyond Procedural Fetishism: The Inadequacy of GDPR in Regulating Facial Recognition Technologies and Public Space Surveillance*, in M. Ebers-K. Sein (eds.), *Privacy, Data Protection and Data-Driven Technologies*, cit., 328. For critical issues regarding data protection provisions established even before the GDPR, see P. De Hert, *Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Debate*, in P. Campisi (ed.), *Security and Privacy in Biometrics*, Cham, 2013, 369.

[67] European Parliamentary Research Service (Author: Giovanni Sartor), *The Impact of the GDPR on artificial intelligence*, 2020, III. See also G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024.

criminal matters" (2020/2016/INI), the European Parliament «stresse[d] that the use of biometric data relates more broadly to the principle of the right to human dignity forming the basis of all fundamental rights guaranteed by the Charter» (Para. 30). For this reason, a moratorium on the use of remote identification systems – such as FRTs for law enforcement purposes – was invoked «until the technical standards can be considered fully fundamental rights compliant, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies; notes that where the above criteria are not fulfilled, the systems should not be used or deployed» (Para. 27)[68].

This heightened attention was then reflected in the preparatory works leading up to the AI Act. Among the most relevant documents are the Guidelines issued by the High-Level Expert Group, established by the Commission[69], as well as the Commission's White Paper on Artificial Intelligence[70]. The latter dedicated considerable space to biometric identification technologies, specifically with regards to "remote biometric identification systems", including FRTs in public spaces – thus using a terminology and framing that will be echoed in the AI Act.

Reiterating the distinction – already acknowledged under the GDPR and national DPAs decisions – between identification and authentication tools[71], the Commission affirmed the profound implications of the former

[68] In the same document, the European Parliament also affirms «its great concern over the use of private facial recognition databases by law enforcement actors and intelligence services, such as Clearview AI, a database of more than three billion pictures that have been collected illegally from social networks and other parts of the internet, including from EU citizens; calls on Member States to oblige law enforcement actors to disclose whether they are using Clearview AI technology, or equivalent technologies from other providers; recalls the opinion of the European Data Protection Board (EDPB) that the use of a service such as Clearview AI by law enforcement authorities in the European Union would 'likely not be consistent with the EU data protection regime'; calls for a ban on the use of private facial recognition databases in law enforcement», Para. 27.

[69] Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* (2019) and *Policy and Investment Recommendations for Trustworthy AI*, 2019. In the first document, the Expert Group underlined that «A proportionate use of control techniques in AI is needed to uphold the autonomy of European citizens. Clearly defining if, when and how AI can be used for automated identification of individuals and differentiating between the identification of an individual vs the tracing and tracking of an individual, and between targeted surveillance and mass surveillance, will be crucial for the achievement of Trustworthy AI. The application of such technologies must be clearly warranted in existing law», 33.

[70] European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM(2020)65, 19 February 2020.

[71] "Remote biometric identification should be distinguished from biometric authentication

for fundamental rights. These include impacts on human dignity, privacy and data protection, the principle of non-discrimination, the rights of vulnerable groups, as well as the freedoms of expression, association and assembly. Consequently, while noting that existing supranational norms – especially the GDPR and the LED – already provide relevant and initial guarantees, the Commission emphasized the importance of launching «a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards (..) in order to address possible societal concerns relating to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market»[72].

2.2. From Data to Technology. Navigating the Artificial Intelligence Act and AI-Powered Biometric Systems: Between Prohibitions and Exemptions

Within the described scenario and in response to the urgent and far-reaching calls for regulatory intervention, the EU Institutions introduced the pioneering AI Act in 2024. This Regulation directly and innovatively disciplines the «development, the placing on the market, the putting into service and the use of artificial intelligence systems» (Recital 1).
Adopting a risk-based approach[73], the AI Act classifies AI technologies into different risk-levels according to their potential impact on health, safety and fundamental rights. Under this structure, biometric systems receive considerable attention and are addressed across multiple provisions. As part of its effort to comprehensively and systematically regulate biometric technologies for the first time, the EU legislators began by tackling a key gap: the lack of legal definitions for technologies previously unrecognized within the existing regulatory instruments.

(the latter is a security process that relies on the unique biological characteristics of an individual to verify that he/she is who he/she says he/she is). Remote biometric identification is when the identities of multiple persons are established with the help of biometric identifiers (fingerprints, facial image, iris, vascular patterns, etc.) at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database», 18.

[72] *Ibidem*, 22.

[73] P. Dunn, *The Artificial Intelligence Act*, cit. For a comprehensive analysis of the AI Act, see, among the others, C.N. Pehlivan *et al.* (eds.), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, 2024; A. Bensoussan *et al.*, *The European AI Act. Summary, Key Points and Article-by-Article Analysis*, Louvain-la-Neuve, 2025; D.U. Galetta-L. Hueso Cotino (eds.), *The European Union Artificial Intelligence Act*, Naples, 2025; G. Malgieri *et al.* (eds.), *The EU Artificial Intelligence Act. A Thematic Commentary*, London, 2025; A. Mantelero *et al.* (eds.), *Intelligenza Artificiale. Commentario*, Milan, 2025.

To this end, art. 3(No. 34) provides a definition of biometric data[74] that echoes the GDPR but, crucially, does not reaffirm the debated and criticized limitation to identification purposes (as noted in Section 2.1 of this work). This specific choice reflects the need to encompass systems designed for a variety of functions beyond identification. As a result, the definition of biometric data in the AI Act is more extensive than those found in both the GDPR and the LED[75].

While the AI Act reintroduces the much-debated and partly criticized distinction between identification and verification (art. 3(No. 35) and (No. 36))[76], it also offers other unprecedented definitions, such as those relating to "emotion recognition system", and "biometric categorization system". The former is described as «an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data» (art. 3(No. 39))[77]; the latter is termed as a system aimed at «assigning natural persons to specific categories», based on their biometric data (art. 3(No. 40))[78].

Another notable novelty includes the distinction between real-time (art. 3(No. 42)) and post (art. 3(No. 43)) remote biometric identification sy-

[74] «'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data».

[75] E.J. Kindt-C. Jasserand, *Prohibited AI Practices*, in C.N. Pehlivan *et al.* (eds.), *The EU Artificial Intelligence (AI) Act*, cit., 168.

[76] Verification is defined as an «automated one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data»; see also Recital 15 on this point. Some scholars expressed some doubts and concerns with regards to the "biometric identification" definition, that refers to «automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database». In particular, «the mention of psychological characteristics in the definition (..) seems contradictory, especially since the term 'biometric data' does not refer to psychological characteristics», L. Feiler-B. Konig, *Article 3*, in C.N. Pehlivan *et al.* (eds.), *The EU Artificial Intelligence (AI) Act*, cit., 70. On this point, see also A.C. Nazzaro, *The Protection of Biometric Data Between the GDPR and the AI Act*, in *European Journal of Privacy Law & Technologies*, 2, 2024, 37.

[77] Recital 18 explains that the definition of emotion recognition systems «does not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents. This does also not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions». Other useful interpretation and examples are provided by the European Commission, *Guidelines on Prohibited AI Practices*, C(2025)884 final, 4 February 2025, in particular Para. 249.

[78] Systems that are used as «ancillary to another commercial service and strictly necessary for objective technical reasons» do not fall into the definition. Recital 16 provides interesting examples of such exemptions.

stems. While both are systems designed to identify natural persons «without their active involvement, typically at a distance», through the comparison of biometric data with those stored in a database (so called one-to-many identification), real-time systems are characterized by capture, comparison and identification occurring «without a significant delay», thus including «not only instant identification, but also limited short delays» (art. 3(No. 42))[79].

This definitional effort marks a significant starting point for analysis: by introducing new legal definitions and distinctions related to the functioning of AI-based biometric systems, the AI Act immediately highlights varying levels of perceived risks and intrusion into the private sphere. These differentiations are directly reflected in the admissibility, legitimacy and applicable safeguards required by such technologies. Indeed, the AI Act assigns these different systems to distinct categories, each corresponding to specific risk levels.

Of particular relevance here is the fact that most of the practices described above qualifies and falls under the category of "unacceptable risk". Alongside subliminal, manipulative and deceptive techniques (a), exploitation of vulnerabilities (b), social scoring (c) and crime prediction and predictive policing (d)[80], art. 5 of the AI Act prohibits a significant number of biometric systems – although, as will be discussed in this Section, certain conditions and several exceptions apply. The prohibited biometric practices include: untargeted scraping of facial images (art. 5(1)(e)); systems to infer emotions (f); biometric categorization systems (g) and real-time remote biometric identification systems (art. 5(1)(h) and art. 5(2) to (8)).

Looking at this list, the approach taken by the EU legislator is, in many respects, quite unprecedented and even courageous, aligning with longstanding demands from civil society organisations and institutions, concerned with the impact of AI and biometrics on fundamental rights. By classifying a wide range of AI-based biometric systems as posing unacceptable risks, the AI Act acknowledges that «these are AI systems that present a risk deemed unacceptable due to their potential to cause such high danger that it becomes incompatible with the shared values and principles at the

[79] Recital 17 states that «'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data has already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned». On the sociological effects concerning remote biometric identification systems, see K. Kieslich-M. Lunich, *Regulating AI-Based Remote Biometric Identification*, Conference Paper FAccT, 2024, 173.

[80] Respectively art. 5(1)(a), (b), (c) and (d).

European level»[81].

While a detailed examination of every single provision lies beyond the scope of this paper, an overview of these groundbreaking rules is essential for a critical assessment of the EU's approach to AI-powered biometric systems.

Staring with the ban on untargeted scraping, it is evident that the controversial use – also by law enforcement authorities – of systems such as the previously mentioned Clearview AI significantly influenced the regulatory stance. The AI Act, in fact, explicitly prohibits the placing on the market, the putting into service for this specific purpose or the use of AI systems operating through untargeted scraping of facial images from the Internet or CCTV footage, where the goal is to build or expand facial recognition databases. As expressly clarified by the European Commission's *Guidelines on Prohibited AI Practices*[82], the prohibition applies where all the specified conditions are cumulatively and simultaneously satisfied[83].

---

[81] W. Gasparri-F. Tesi, *Artificial Intelligence and AI Act: From the Individual to the Algorithm?*, in *Zbornik Radova*, 59, 2025, 297. As recalled by Mazur, the category of unacceptable risk represents a novelty, which was not included in the European Commission *White Paper* (see *supra* note 70); that document «proposes to create a category of high-risk uses of AI which would be subject to requirements regarding, for example, the representativeness of data used for training the algorithms, or documentation of the programming», J. Mazur, *Artificial Intelligence vs Data Protection: How the GDPR Can Help to Develop a Precautionary Regulatory Approach to AI?*, in A. Kornilakis *et al.* (eds.), *Artificial Intelligence and Normative Challenges. International and Comparative Legal Perspectives*, Cham, 2023, 218. Looking at the regulatory approach adopted in the final version of the AI Act, as underlined by Majado, «the European legislators are making a presumption *juris et de jure* with this point, understanding that certain practices (..) are not, at present, susceptible to a legally beneficial use in current European democratic systems, or at least a use that is not detrimental to individuals' fundamental rights», P. Garcia Majado, *Prohibited AI Practices under the EU AI Act*, in B. Raue *et al.* (eds.), *Artificial Intelligence and Fundamental Rights: The AI Act of the European Union and Its Implications for Global Technology Regulation*, Trier, 2025, 40.

[82] As explained in Paras. 3, 4 and 5 of the abovementioned *Guidelines*, «Pursuant to Art. 96(1) (b) AI Act, the Commission is to adopt guidelines on the practical implementation of the practices prohibited under Art. 5 AI Act. (..) These Guidelines aim to increase legal clarity and to provide insights into the Commission's interpretation of the prohibitions in Art. 5 AI Act with a view to ensuring their consistent, effective and uniform application. (..) These Guidelines are non-binding».

[83] Specifically, the prohibition exclusively applies when all four conditions are fulfilled, namely «i) the practice must constitute the 'placing on the market', 'the putting into service for this specific purpose' or the 'use' of an AI system; ii) for the purpose of creating or expanding facial recognition databases; iii) the means to populate the database are through AI tools for untargeted scraping; and iv) the sources of the images are either from the internet or CCTV footage», Para. 224-225. While "scraping" has been interpreted in the European Commission's *Guidelines on Prohibited AI Practices* as «web crawlers, bots or other means to extract data or content from different sources, including CCTV, websites or social media, automatically. These tools are software programmed to sift through databases and extract information and

Another banned practice is the placing on the market, the putting into service for this specific purpose, or the use of categorization systems based on biometric data and aimed at deducting or inferring sensitive information about race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientations. Given the risks to individuals' rights, particularly regarding discrimination practices based on sensitive characteristics and traits, these systems are deemed unbearably intrusive and unacceptable[84]. Nonetheless, similarly to other prohibited practices, the ban is not to be considered as absolute: art. 5(1)(g) establishes that the interdiction does not cover «any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement»[85]. In addition, biometric categorization systems that do not fall under this strict prohibition are classified as high-risk, according to Annex III, provision 1(b), that will be examined later.

The EU legislators have also decided to prohibit, in certain contexts, AI systems used to infer emotions. Specifically, this emerging technology, based on affective computing[86], is banned in the workplace and education institutions, «except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons» (art. 5(1)(f)). This provision raises several interpretative issues. First, the terminology employed appears to diverge from the definition provided in art. 3(No. 39), which describes "emotion recognition systems" as those capable of both identifying and inferring emotions. From a literal reading, the provision in art. 5 «does not deploy the concept of emotion recognition system but 'AI systems to infer emotions'»[87]. Nonetheless, as several scholars pointed out,

to make use of that information for another purpose», the term "untargeted" «relates to technique that operates like a 'vacuum cleaner', absorbing as much data and information as possible», Paras. 227-228. The rationale behind this classification, is clearly stated in Recital 43: «because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy».

[84] Recital 16.

[85] The use of the expression "in the area of law enforcement", rather than "for law enforcement purposes" – as employed in other prohibited practices – has been criticised for being «unprecise and would, most probably, be subject to divergent interpretations by various EU and national instances», U. Cemalovic, *Prohibited Artificial Intelligence Practices According to Article 5 of the European Union's Regulation on AI – Between the 'Too Late' and the 'Not Enough'*, in *International Journal of Law and Information Technology*, 32, 2024, 12.

[86] For a technical analysis, H. Al-Samarraie *et al.*, *Emotional Intelligence and Individuals' Viewing Behaviour of Human Faces: A Predictive Approach*, in *User Modeling and User-Adapted Interaction*, 33, 2023, 889; A.-L. Cirneanu *et al.*, *New Trends in Emotion Recognition Using Image Analysis by Neural Networks. A Systematic Review*, in *Sensors*, 23, 2023, 1.

[87] E.J. Kind-C. Jasserand, *Prohibited AI Practices*, cit., 162.

«while it remains unsure if the legislator has on purpose deviated from the concept of emotion recognition systems in art. 5, one could defend that the broadest protection should prevail, based on the argument that the AI Act aims to protect against harmful AI practices and a broad interpretation fits the legislator's intention. It would imply that the ban does not only cover inferences but also identification of emotions and intentions»[88].
Further definitional ambiguities arise from the lack of clarity surrounding the terms "workplaces" and "education institutions". The broad and vague contours of these concepts also characterize the undefined medical or safety purposes, which could potentially lead to wide exclusions[89]. All the other uses of emotion recognition systems – including those falling under the mentioned exceptions[90] – are categorized as high-risk systems, as also stated in Annex III[91]. In such cases, these systems are permitted but are subject to obligations and safeguards set out in Section II and III of Chapter III of the AI Act[92].
Finally, another biometric system classified as posing an unacceptable risk is the real-time remote identification in publicly accessible spaces[93] for

[88] *Ibidem*. This interpretation has been also confirmed by the European Commission's *Guidelines*, where it is pointed out that «inferring generally encompasses identifying as a prerequisite, so that the prohibition should be understood as including both AI systems identifying and inferring emotions or intentions (..). The definition in Art. 3(39) AI Act of emotion recognition systems should therefore be considered relevant in relation to Art.5(1)(f) AI Act», Para. 245. The rationale behind the legislators' decision not to directly and expressly use the term "emotion recognition systems" in art. 5 remains unclear.

[89] I. Barkane-L. Buka, *Prohibited AI Surveillance Practices in the Artificial Intelligence Act*, cit., 116. See also the European Commission's *Guidelines*, Paras. 254-255.

[90] E.J. Kindt-C. Jasserand, *Prohibited AI Practices*, cit., 165.

[91] Based on art. 6(2) and Annex III, Para. 1(c). Moreover, Annex III contains other references to AI systems – potentially biometric ones – employed in the field of education: «AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels» (Para. 3(d)) and «AI systems intended to be used to (..) monitor and evaluate the performance and behaviour of persons in such relationship» (Para. 4(b)) are to be considered as high-risk systems. In the first category it is possible to include «proctoring systems using FRT», while «monitoring or surveillance systems using FRT in workplace environments» could be considered part of the second category (on this point, see N. Menendez Gonzalez-G.. Mobilio, *Between Prohibited Risks and High Risk*, cit., 174).

[92] For an in-depth analysis, see, *ex multis*, T. Rodriguez de las Heras Ballell, *High-Risk AI Systems in the European AI Act*, in O. Pollicino *et al.* (eds.), *La disciplina dell'Intelligenza Artificiale*, cit., 227; see also the contributions devoted to Chapter III in the AI Act Commentaries *supra* note 73.

[93] Definition in art. 3(No. 44); the European Commission's *Guidelines* provide some useful examples at Para. 316.

the purpose of law enforcement[94]. This categorization was the subject of intense political contention during the legislative process. While the European Parliament – supported by the European Data Protection Supervisor and the European Data Protection Board[95] – advocated for a more restrictive approach, calling for far-reaching bans, the European Commission and the Council supported a partial ban, limited to real-time technologies, and a flexible framework allowing such systems under certain conditions[96]. As a result of the negotiations between the EU legislators, the definitive version of the ban included in art. 5(1)(h) uniquely targets remote identification systems employed in publicly accessible spaces for the purpose of law enforcement and exclusively those with a real-time capturing, comparison and identification, thus proposing a relevant differentiation from the *post* (retrospective) systems. This distinction is based on their – supposedly – differing risks and impacts on fundamental rights. As explained in Recital 31, in fact, real-time identification «is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities.» As will be further discussed in Section 3, this differentiation and the consequently diverse discipline applied is considered one of the most controversial aspects of the AI Act[97] and still continues to provoke a lively debate.

---

[94] Art. 3(No. 45).

[95] EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (AI Act)*, 2021.

[96] «The Parliament's negotiating position version of text from June 2023 was the strictest with RBIs [Remote Biometric Identification] and FRT. It prohibited the use of both real-time and *ex post* RBIs in the EU», N. Menendez Gonzalez-G. Mobilio, *Between Prohibited Risks and High Risk*, cit., 165. For a comprehensive analysis of the evolution of the legislative discourse from the initial draft to the final version of the AI Act, with particular reference to prohibited practices, see R.J. Neuwirth, *Prohibited Artificial Intelligence Practices Revisited*, in V.L. Raposo (ed.), *The European Artificial Intelligence Act. Promises and Perils?*, Cham, 2025, 131.

[97] L. Bertuzzi, *European Union Squares the Circle on the World's First AI Rulebook*, in *Euractiv*, 9 December 2023.

Although real-time systems for law enforcement purposes are generally prohibited, the legislation provides for a significant number of broad exceptions, which permit the use of such instruments when strictly necessary for: «i) targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for mission persons; ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack; iii) the localization or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or a prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least 4 years» (art. 5(1)(h))[98].

In these exceptional cases, the provision strictly limits the use of real-time identification for the confirmation of the identity of a «specifically targeted individual» (art. 5(2)): this formulation seems to exclude the implementation of such systems for indiscriminate and bulk searches[99], also called «fishing expeditions which could lead to generalized and indiscriminate surveillance»[100]. Additionally, due to the exceptional nature of real-time systems, art. 5(2) also mandates a careful assessment of «the nature of the situation giving rise to the possible use»[101], as well as of the potential consequences for rights and freedoms.

Necessity and proportionality safeguards should also be fulfilled, in accordance with applicable national laws that may authorize such use. Moreover, a fundamental rights impact assessment (FRIA), as mandated by art. 27 AI Act, must be conducted as a mandatory precondition for the authorisation and the employment of the system, which must also be registered in a dedicated database (except in cases of urgency)[102].

According to art. 5(3), a prior authorization from a judicial or independent

---

[98] As pointed out in Recital 33 of the AI Act, «the list of criminal offences provided in an Annex to this Regulation is based on the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA».

[99] As reported by *EDRi*, «Emeritus Professor of International Law, Douwe Korff, supports this interpretation on the basis of case law of the Court of Justice of the EU, specifically the PNR (Passenger Name Records) case», in *edri.org*, accessed 20 January 2026.

[100] N. Menendez Gonzalez-G. Mobilio, *Between Prohibited Risks and High Risk*, cit., 169.

[101] «In particular the seriousness, probability and scale of the harm that would be caused if the system were not used», art. 5(2).

[102] Art. 5(2).

administrative national authority is required[103]. It should be granted only when, «on the basis of objective evidence or clear indications», the use of the system is both necessary and proportionate to achieving the objectives specified in exceptions discussed above. Furthermore, the use must be limited to what strictly necessary in terms of duration, geographic and personal scope.

Once authorized, the deployment of the system must be notified to the relevant market surveillance authority and national data protection authority, in accordance with national rules (art. 5(4)). Importantly, to allow the described procedure to take place, Member States shall adopt national rules governing the process for requesting, issuing, exercising, supervising and reporting the authorization, as well as for determining the list of relevant criminal offences referred to in the exemption determined in art. 5(1)(h)(iii). Also in this context, national legislators may choose to adopt stricter provisions than those provided in the AI Act[104]. As underlined by the European Commission in its *Guidelines on prohibited AI practices*, «only a domestic Member State law that fulfils, in particular, the requirements in art. 5(2-7) AI Act, can allow the use of real-time remote biometric identification, as provided by Art. 5(2)» (Para. 326): in the absence of such national provisions, the use of the systems under analysis must be considered prohibited as of 2 February 2025[105].

While an overall critical assessment of the analysed rules on real-time systems will be reserved for the concluding Section of this work, it is already evident that, on the one hand, the prohibition on real-time identification systems exclusively covers the law enforcement purpose and, on the other

[103] «For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5», art. 5(3).

[104] Finally, annual reports shall be submitted to the European Commission by the national market surveillance authorities and the national Data Protection Authorities, and published by the Commission itself, using aggregated data (art. 5(6) and (7)).

[105] «According to Article 113 AI Act, Article 5 AI Act applies as from 2 February 2025. The prohibitions in that provision will apply in principle to all AI system regardless of whether they were placed on the market or put into service before or after that date. At the same time, the chapters on governance, enforcement and penalties will become applicable on 2 August 2025. Consequently, the provisions on penalties for noncompliance with the prohibitions in Article 5 AI Act will not apply before 2 August 2025. In this interim period, there will also be no market surveillance authorities to monitor whether the prohibitions are being properly complied with», European Commission's *Guidelines*, Paras. 430-431. See also Recital 179, explaining the reason why it has been considered necessary to anticipate the application of prohibitions.

hand, the scope of the exemptions is broad, despite the safeguards and requirements laid down to accompany them.

Beyond the prohibited practices outlined in art. 5, it is essential to recall – as previously noted – that certain biometric surveillance systems are qualified as high-risk. This follows art. 6, which also refers to the practices listed in Annex III. According to Recital 54, the potential for inaccuracies, bias and discriminatory effects in biometric systems could pose significant threats to fundamental rights, thus justifying the classification as high-risks and the consequent need for strict safeguards, rigorous requirements and compliance obligations. Among the AI systems outlined in Annex III (Para. 1(a), (b), (c)), are: remote biometric identification systems, including *ex post* identification[106], biometric categorization "according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics", as well as AI systems intended to be used for emotion recognition where used in contexts permitted by the AI Act[107].

When high-risk systems are involved, several conditions must be met, as laid out in Chapter III, Section 2 and 3 of the AI Act. These provisions (from art. 8 to 27) include the establishment of a risk management system, quality criteria for datasets employed to train AI models, the elaboration of technical documentation, record-keeping obligations, transparency measures, human oversight guarantee and specific duties for providers, importers, distributors and deployers. With regard to the latter, art. 26 explicitly sets out rules concerning the use of high-risk AI systems for post-remote biometric identification by law enforcement authorities. Specifically, in light of «the intrusive nature» of such systems, their use «shall be subject to safeguards», without prejudice to applicable EU law, in particular LED provisions (Recital 95). Consequently, post-remote identification systems should always be «used in a way that is proportionate, legitimate and strictly necessary, and thus targeted» in terms of individuals, location and scope. Recital 95 also emphasizes that such systems should not be used by law enforcement authorities to implement indiscriminate surveillance mechanisms. When employed «in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence», the deployer is required to obtain an *ex ante* authorization – and, in any case, without delay and within 48 hours – from a judicial or administrative authority. However, this requirement does not apply when the remote identification system is implemented for

[106] As explicitly stated in Annex III, Para. 1(a), «AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be» are not included in the category of high-risk systems.

[107] Annex III, para. 1 nonetheless specifies that such systems are considered as high-risk, in so far as their use is permitted under relevant Union or national law.

«the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence» (art. 26(10))[108]. Importantly, the legislators clarify, in Recital 95, that «in no case shall such high-risk AI system for post-remote biometric identification be used for law enforcement purposes in an untargeted way, without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person». Also with regards to the procedural rules disciplining *ex post* remote biometric identification systems, Member States retain the discretion to introduce more restrictive national laws, provided these are in line with EU law. From this rapid overview of the provisions regulating biometric systems in the AI Act, it becomes clear that, while some biometric applications fall outside both the high-risk and the prohibited practices[109], a significant number are covered by the regulation and are subject to different classifications, each with a detailed set of safeguards and specific conditions. These provisions, distinctions and categorizations have sparked considerable debate and criticism, which merits closer examination, as they will play a crucial role in shaping the future deployment and governance of AI-based biometric technologies under the AI Act.

3. The Constitutional Governance of AI-Powered Biometric Systems: From Dystopia to Dignity

3.1. Assessing the AI Act Approach to Biometric Identification Systems: Regulatory Ambition and Legal Uncertainties

The AI Act undoubtably marks a regulatory milestone, representing the first systematic legislative effort to comprehensively address AI-biometric

[108] Other requirements necessitate that «Regardless of the purpose or deployer, each use of such high-risk AI systems shall be documented in the relevant police file and shall be made available to the relevant market surveillance authority and the national data protection authority upon request, excluding the disclosure of sensitive operational data related to law enforcement. This subparagraph shall be without prejudice to the powers conferred by Directive (EU) 2016/680 on supervisory authorities. Deployers shall submit annual reports to the relevant market surveillance and national data protection authorities on their use of post-remote biometric identification systems, excluding the disclosure of sensitive operational data related to law enforcement. The reports may be aggregated to cover more than one deployment», art. 26(10).

[109] Such as verification systems, including authentication (Annex III, Para. 1), but also «biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures should not be considered to be high-risk AI systems», Recital 54.

systems by directly focusing on the technologies themselves.
While regulating such practices has been one of the most complex and heavily debated aspects of the legislative process[110], the AI Act deserves credit for recognizing a crucial issue: AI systems – and in particular AI-powered biometric systems – often involve trade-offs between the protection of fundamental rights and other competing interests, such as security, efficiency or promotion of innovation and free circulation of goods and services. Consequently, the Act proposes a range of solutions aimed at striking a balance, distinguishing between practices that constitute unacceptable surveillance and those that may be implemented as necessary and proportionate recognition tools[111].
The AI Act should also be acknowledged for anticipating the risks posed by technologies and biometric systems that are not yet fully implemented or deployed in the EU, such as predictive policing, social scoring or emotion recognition[112]. In this respect, the AI Act's forward-looking approach adds significant value, especially given the rapidly evolving scenario of AI adoption.
However, despite these courageous steps, several provisions of the AI Act concerning biometric systems remain vague, leaving room for varied interpretations. This ambiguity grants national legislators substantial discretion, principally in areas where security interests are invoked.
Upon closer examination, while it is true that the list of prohibited practices was expanded in the final version compared to the initial Commission proposal[113], some of the total bans adopted in the Act, as some scholars pointed out, appear more like restrictions on certain uses rather than outright prohibitions[114]. This consideration largely stems from the extensive use of conditions to be fulfilled for the prohibition to apply as well as of exceptions, particularly concerning real-time biometric remote identification systems employed by law enforcement authorities[115]. These exceptions

[110] R.J. Neuwirth, *Prohibited Artificial Intelligence Practices Revisited*, cit.

[111] E. Haber, *Racial Recognition*, cit., 119.

[112] Some scholars refer to them as "second generation of biometric technologies", using physiological processes or behavioural biometrics to ensure more developed, sophisticated and widespread systems (see M. Smith-S. Miller, *Biometric Identification*,cit.).

[113] F.P. Levantino-I. Neroni Razende, *Rischio inaccettabile: usi proibiti*, in O. Pollicino *et al.* (eds.), *La disciplina dell'Intelligenza Artificiale*, cit., 159.

[114] *Ibidem.* Similarly, see also C. Jasserand, *Facial Recognition in Public Spaces and the Principle of Necessity*, cit.; I. Barkane, *Questioning the EU Proposal for an Intelligence Act*, cit.; P. Garcia Majado, *Prohibited AI Practices under the EU AI Act*, cit.

[115] The appropriateness of referring to Council Framework Decision 2002/584/JHA62 (n. iii) has been called into question, especially with regard to the fixed nature of the list: several scholars have emphasized the importance to ensure flexibility and adaptability in a rapidly evolving landscape of criminal activity (G Villafuerte-Guerrero, *Facial Recognition Systems under*

«represent a point of criticism, as they, if interpreted broadly, may end up neutralizing and nullifying the effectiveness of the established bans. Moreover, the absolute nature of the bans in the regulation is somewhat diminished in relation to other cases, given the specific characteristics of the banned AI practices, as the prohibitions are very thoroughly constructed, effectively widening the scope of AI systems that falls outside the ban»[116]. Additionally, it may be considered difficult to understand or to justify the decision (and the underlying rationale) to prohibit certain uses of AI systems, while permitting others. With regards to emotion recognition tools, for instance, it remains unclear why their acknowledged limited reliability – as stated in Recital 44[117] – constitutes a valid ground for prohibition only in the context of employment and education: «if they are not scientifically

the European Union's Artificial Intelligence Act, in *RFJ*, 15, 2024, especially 179).

[116] W. Gasparri-F. Tesi, *Artificial Intelligence and AI Act*, cit., 299. Similarly, Nikolinakos affirmed that «The proposed prohibition of remote biometric recognition technologies contains too many exceptions, so that it becomes de facto not a real prohibition», N.Th. Nikolinakos, *EU Policy and Legal Frameworks for Artificial Intelligence, Robotics and Related Technologies – The AI Act*, Cham, 2023, 388; Lynch affirmed on this point: «there is still considerable uncertainty around how the exceptions will be implemented (..). The parameters, particularly around the broader spread of available offence types, will allow significant room for the use of these technologies. (..) An obvious risk is that technologies such as FRT will be seen as more acceptable or even as "approved" due to the wording of the AI Act», N. Lynch, *Facial Recognition Technology in Policing and Security*, cit., 12. See also N. Menendez Gonzalez-G. Mobilio, *Between Prohibited Risks and High Risk*, cit., 169; R.J. Neuwirth, *Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)*, in *Computer Law and Security Review*, 48, 2023, 1. According to Barkane and Buka, «The EU legislator has considerably extended the list of prohibited AI practices during the negotiation process in comparison with the initial proposal, however it has failed to introduce clear prohibitions on AI-based mass surveillance and other unacceptable AI practices. The AI Act sets only partial prohibitions on the use of real-time remote biometric identification, predictive policing, emotion recognition and biometric categorisation systems, severely limiting their scope and allowing for a large number of exceptions. Consequently, the use of remote biometric identification and predictive policing systems for law enforcement purposes, although permitted in exceptional cases, could almost always be justified», I. Barkane-L. Buka, *Prohibited AI Surveillance Practices in the Artificial Intelligence Act: Promises and Pitfalls in Protecting Fundamental Rights* 127.

[117] «There are serious concerns about the scientific basis of AI systems aiming to identify or infer emotions, particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such systems are the limited reliability, the lack of specificity and the limited generalisability. Therefore, AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data may lead to discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons. Considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof. Therefore, the placing on the market, the putting into service, or the use of AI systems intended to be used to detect the emotional state of individuals in situations related to the workplace and education should be prohibited».

reliable or highly inaccurate, they may produce harmful results in other contexts as well»[118].

This, combined with the "implementing" rules assigned to Member States legislators for specific and fundamental regulatory aspects[119], may «not only lead to fragmentation in the implementation of the regulation in the EU but also result in a broad and dangerous expansion of their deployment»[120].

Notably, certain Member States have expressed concerns as well: Austria for example highlighted in an official Statement that the exceptions outlined in art. 5(1)(h) with regards to real-time biometric identification in publicly accessible spaces for law enforcement purposes are «too far-reaching and are not in keeping with Austria's understanding of proportionate interference with citizens' fundamental rights»[121].

Another significant limitation to the bans established by the AI Act lies in the national security exemption (art. 2(3))[122]. Although this exclusion reflects the division of competences between the EU and Member States – where national security remains a national prerogative –, it nonetheless raises critical concerns, similar to controversial provisions in other regulatory areas involving data protection and security[123]. Indeed, as some have observed, «the significant implementation challenge is that the line between national security and law enforcement is blurred in many contexts, particularly around terrorism, cybercrime, financial crimes, money

---

[118] P. Garcia Majado, *Prohibited AI Practices under the EU AI Act*, cit., 40. According to the Author, the power imbalance referred to in Recital 44 may also arise in other context, such as migration and law enforcement. Similar considerations may be extended to real-time remote biometric identification systems, which are not prohibited outside law enforcement use, thereby excluding their deployment by private actors from the ban. Similarly, on this point, G.M. Diaz Gonzalez, *Prohibited Artificial Intelligence Practices*, in A.J. Huergo Lora (ed.), *The EU Regulation on Artificial Intelligence*, cit., 60 and U. Cemalovic, *Prohibited Artificial Intelligence Practices According to Article 5 of the European Union's Regulation on AI*, cit., 13.

[119] Such as the authorisation process concerning the employment of real-time remote identification systems, and the determination of the competent authority.

[120] A. Giannini-S. Tas, *Much Ado About Nothing? AI Act and the Prohibition of Real-Time Biometric Identification*, in *Verfassungsblog*, 10 December 2024. Similarly, European Parliamentary Research Service (Authors: G. González Fuster and M. Nadolna Peeters), *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence* (2021), analysing the regulatory trends at the time of the AI Act Proposal.

[121] Statement Interinstitutional File 2021/0106, 9645/24 of 15 May 2024.

[122] «This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences».

[123] See *supra* notes 27 and 64.

laundering, and cross-border-organised crime»[124].

Alongside the sensitive and ambiguously defined exceptions for prohibited AI-based biometric practices, the distinction between real-time and *ex post* remote identification systems – and the corresponding differentiation in terms of risks evaluation – has also been the subject of intense debate, with criticisms raised since the initial Commission proposal[125]. Some scholars have questioned the rationale behind this distinction, arguing that the level of intrusiveness does not necessarily depend on the timing of biometric data processing[126]. In particular, they challenged the assumption that the delay between data capture and identification reduces the potential harm to fundamental rights. For example, *ex post* remote biometric identification in the context of a political protest could still have a chilling effect on the freedom of assembly[127].

Similar criticisms have been directed at the distinction between identification and verification – a concept already introduced in the GDPR – and at the resulting exclusion of verification systems from the scope of high- and unacceptable risk regimes. Scholars have argued that «the current binary distinction is reductionist and might fall short of addressing the potential consequences in the current landscape»[128].

Concerns about vague and unclear provisions are not limited to the definitions, conditions or exceptions for prohibited practices; they also extend to the requirements and conditions for high-risk systems. For instance, art. 26(10), which allows the use of post-remote biometric identification for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence, is notably unclear; the (practical) definitions of targeted versus untargeted investigations, as well as the

---

[124] N. Lynch, *Facial Recognition Technology in Policing and Security*, cit., 13; N. Menendez Gonzalez-G. Mobilio, *Between Prohibited Risks and High Risk*, cit., 175. It is worth recalling that art. 111 AI Act states that «Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030».

[125] *The European Data Protection Supervisor (EDPS), Wojciech Wiewiorowski, affirmed in a press release in 2021* that «the EDPS regrets to see that our earlier calls for a moratorium on the use of remote biometric identification systems – including facial recognition – in publicly accessible spaces have not been addressed by the Commission» in *edps.europa.eu*, accessed 20 January 2026. See also G. Gultekin-Varkonyi, *Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation*, in *Internet Policy Review*, 13, 2024, 1, in particular 18.

[126] N. Menendez Gonzalez-G. Mobilio, *Between Prohibited Risks and High Risk*, cit., 174.

[127] A. Ribera Martinez, *The Debiasing Paradox*, cit. 144-145. The Author also criticizes the lack of attention to the bias-related matters and concerns.

[128] B. Sumer, *The AI Act's Exclusion of Biometric Verification*, cit., 151.

concept of bulk surveillance, are indeed highly contested within the EU, even in relation to other technologies and law enforcement practices, such as data retention.

Significantly, also the Commission's *Guidelines* on prohibited AI practices refer to the interpretation provided by the CJEU in the data retention and Passenger Name Records cases (Para. 347) to help clarify the conditions established by the AI Act in situations where the balance between security and fundamental rights is at stake. It can be argued that this reference represents a weakness. Notably, both the data retention saga and the discipline on data transfers remain highly contentious, with the principles and conditions established by the Judges of Luxembourg's case law continuing to provoke controversy. It is no coincidence that numerous preliminary rulings have been requested, in recent years, in these areas, reflecting not only the persistent need for clear interpretation of multiple criteria but also the difficulties faced by national lawmakers to fully implement what are often conceived as too restrictive requisites established in the CJEU decisions. In fact, public authorities and security forces continue to debate whether it is realistically and concretely possible to comply with the requirements determined by the supranational landmark judgments without rendering the technology (i.e. the data retention) ineffective for its intended purpose[129].

From this analysis, it is therefore evident that reference to such supranational jurisprudence, rather than providing clarity, highlights the uncertainties regarding legal interpretations as well as the unresolved questions surrounding the use and discipline of surveillance instruments for law enforcement and security purposes[130].

Another aspect that is still contested is the strict necessity requirement, also recalled in art. 26(10) of the AI Act. This criterion is particularly difficult to assess and is often insufficiently evaluated due to technological solutionism drifts and the quasi-automatic reliance on the technology and the limited consideration of alternative, less intrusive systems[131].

A further point of complexity concerns the discipline of targeted searches. It can be argued that such delicate measures should be accompanied by diverse and numerous safeguards – not entirely specified in art. 26(10)

---

[129] On this point, with regards to both data retention and data transfer, see E. Tuchtfeld *et al.* (eds.), *Eyes Everywhere. Surveillance and Data Retention under the EU Charter*, Berlin, 2025; T. Naef, *Data Protection without Data Protectionism*, Cham, 2023; S. Yakovleva, *Governing Cross-Border Data Flows: Reconciling EU Data Protection and International Trade Law*, Oxford, 2024.

[130] E. Celeste-G. Formici, *Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia*, in *German Law Journal*, 25, 2024, 427.

[131] On this point, with regards to the data retention case as well as to the data transfer and PNR instruments, see G. Formici, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali*, cit.

AI Act –. This requires careful (national) legislative choices. For instance, when a FRT system is used for real-time or post identification purposes, a key consideration is the watchlist – the set of images against which one-to-many matches are conducted. The manner in which this watchlist is determined is highly sensitive: the larger the watchlist, the more expansive the control on civil society. This is analogous to the use of DNA for investigative purposes, using systems based on matching genetic samples against specific profiles included in DNA databases. These databases – which have been at the centre of landmarks decisions by national and supranational Courts[132] – raise(d) significant issues: rules must govern what genetic data are retained in the database (only convicted individuals? And for all crimes or exclusively for certain specific types of crimes – maybe the most serious ones? Or also data concerning suspected or investigated persons, not yet convicted?), who can access the database, the scope of that access and the necessary data security measures. Similar challenges may arise for facial images and the regulatory framework that should discipline the creation of watchlists for FRTs: for example, could a watchlist include images from social media to identify a suspect? What safeguards and conditions must lawmakers establish to prevent fishing expeditions or overreach?

All these legislative decisions and interventions, as clearly emerges, are crucial to determine the real dimension and impact of such surveillance mechanisms on fundamental rights as well as to properly evaluate the concrete targeted nature of "technological" searches.

Beyond these concerns and the potential interpretative and practical challenges[133], another sensitive issue lies in the interplay between the AI Act and existing legislative frameworks, particularly the GDPR and the LED. Although the AI Act includes provisions intended to clarify and coordinate its application with different legislations[134], challenges may still arise in cases where definitions differ or where overlaps create uncertainty[135].

---

[132] On this vast case-law, see L. Scaffardi (ed.), *La banca dei dati italiana del DNA. Limiti e prospettive della genetica forense*, Bologna, 2020; G. Formici, *From "Familial Searching" to "Forensic Genetic Genealogy": New Frontiers – and Challenges – of DNA Analysis in Criminal Investigations*, in *BioLaw Journal*, 1S, 2021, 305.

[133] Other critiques regard, for instance, the definition of emotion recognition systems: on this point, see J. Czarnocki, *Will New Definitions of Emotion Recognition and Biometric Data Hamper the Objectives of the Proposed AI Act?*, in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2021, 1; M. Durovic-T. Corno, *The Privacy of Emotions*, cit.

[134] For example, art. 10(5).

[135] With regards to real-time remote biometric identification systems, Recitals 38 and 39 provides some clarifications on the applicability of the LED provisions. In particular, Recital 39 specifies that «Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of real-

As suggested in the already recalled Commission's *Guidelines*, «where some practices would not fall within the scope of a prohibition of the AI Act or would be mentioned as an exception, same practices may still be prohibited based on other primary or secondary Union or national law»[136]. Determining the applicability of EU digital legislations, however, remains a complex task. Difference in key definitions are not merely formal issues: the divergence between the definition of biometric data in GDPR and in the AI Act, already highlighted in Section 2.2.[137], may create a difficult interplay between the two frameworks. This raises questions as to what should be considered "biometric data" and when the GDPR should apply "in the background" for data processing, considering that some data classified as biometric under the AI Act do not align with the GDPR definition and may, for this reason, fall outside the stricter data protection regime applicable to special categories of data.

Moreover, inconsistencies can be identified with regard to the legal basis for processing such data. The AI Act allows, under art. 10(5), the processing of special categories of data for bias monitoring, detection and correction in high-risk systems; however, this possibility is not clearly reflected in the exemptions provided under art. 9 GDPR.

In this context, the work of Data Protection Authorities could continue to represent a solution to gaps or doubts, by providing with guidelines on the use of GDPR provisions in cases of AI-systems, as was done in the past. Nevertheless the incoherence and applicative concerns could be posed at the basis of a perceived need for redesigning the existing legislative

time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, should continue to comply with all requirements resulting from Article 10 of Directive (EU) 2016/680. For purposes other than law enforcement, Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data subject to limited exceptions as provided in those Articles. In the application of Article 9(1) of Regulation (EU) 2016/679, the use of remote biometric identification for purposes other than law enforcement has already been subject to prohibition decisions by national data protection authorities». This reference recalls the relevant decisions adopted by DPAs, as underlined in Section 2.1. of this paper. Also art. 5(1) states that «Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement».

[136] With regards to real-time remote biometric identification systems, «the AI Act applies as ex *specialis* to Article 10 LED, thus regulating such use and the processing of biometric data involved in an exhaustive manner (..). All other provisions of that Directive apply in addition to the conditions set out in the AI Act, in particular for the use of real-time systems for law enforcement purposes when permitted, subject to the limited exceptions in Art. 5(1)(h) AI Act», Paras. 15-16.

[137] See *supra* note 75. See also B. Sumer, *The AI Act's Exclusion of Biometric Verification*, cit., 151.

landscape[138]. Interestingly, this option has already emerged in the debate surrounding the so-called Digital Omnibus Package, that will be discussed in Section 3.2.; it is not surprising, in fact, that this proposal for reform places particular emphasis on provisions concerning sensitive data.
This recent development immediately suggests that the relationship between the AI Act and the GDPR is widely considered as a point of weakness requiring legislative intervention, thereby limiting the strength and effectiveness of the AI Act from the outset.

3.2. Present and Future of Biometric Systems in the EU: Mastering the Genie of the Lamp for Good?

Taking into account all the complex aspects and open issues illustrated in the previous Section 3.1, some concluding (and more general) reflections can be drawn.
The unprecedented prohibitions introduced by the AI Act represent a «major step forward for regulating the use in the EU of biometric data systems in general and facial recognition technologies also for law enforcement purposes. (..) The Proposal [and subsequently the Act] may be seen as a source of inspiration for other countries and jurisdictions to enact comprehensive legislation which would allow (albeit in a restrictive way) the use of automated facial recognition technologies by law enforcement authorities and its inclusion in the criminal justice system»[139].
EU lawmakers have thus demonstrated a strong legislative activism and an innovative approach, informed by past regulatory shortcomings and aimed at governing not just a single instrument but the broader ecosystem of AI-based biometric technologies. The EU Institutions have also shown an ability to reach political and legal compromises necessary to achieve a unified regulatory outcome[140] as well as to determine a balance point

[138] Policy Department for Transformation, Innovation and Health, Directorate-General for Economy, Transformation and Industry, *Interplay between the AI Act and the EU Digital Legislative Framework*, European Parliament, 2025.

[139] R. Soares Pereira, *Remarks on the Use of Biometric Data Systems (and Facial Recognition Technologies) for Law Enforcement Purposes: Security Implications of the Proposal for an EU Regulation on Artificial Intelligence*, in D. Moura Vicente *et al.* (eds.), *The Legal Challenges of the Fourth Industrial Revolution. The European Union's Digital Strategy*, Cham, 2023, 208.

[140] For a comparative analysis between the US and the EU approach towards AI governance, C. Sbailò, *Governing Artificial Intelligence: Technological Leadership and Regulatory Challenges in an Era of Exponential Growth*, in *DPCE Online*, 67(SP 3), 2024, 275; V. Lubello, *From Biden to Trump: Divergent and Convergent Policies in the Artificial Intelligence (AI) Summer*, in *DPCE Online*, 1, 2025, 49; C. Novelli-A. Gaur-L. Floridi, *Two Futures of AI Regulation under the Trump Administration*, in *ssrn.com,* 31 March 2025, accessed 20 January 2025; see also G. Formici, *Transatlantic Debate*

between fundamental rights and competing interests[141]: the expanded list of prohibitions, driven in part by pressure from civil society, stands in contrast with security needs, addressed in several exceptions.

Despite these important efforts, it is clear that the debate around AI-powered biometric systems in the EU remains far from settled.

The concrete effectiveness of such a far-reaching legislative initiative – and of the prohibitions it establishes – will, in practical terms, depend on the breadth with which the exceptions will be interpreted and applied, the degree of compliance by relevant actors (including providers and deployers) with the prescribed safeguards and requirements, as well as the manner in which Member States will regulate the sensitive aspects left to national intervention by the AI Act[142]. These include, in particular, the procedural requirements and the designation of national authorities responsible for authorizing the use of real-time and post remote biometric identification systems for law enforcement purposes[143].

In other words, the innovative nature of this EU legislative framework must ultimately be assessed through its practical implementation and enforcement. In this context, national Data Protection Authorities, competent judicial bodies and other institutions designated for the authorization process will play a central role in interpreting and enforcing the relevant provisions[144].

Member States legislators also bear significant responsibility in shaping national frameworks consistent with the AI Act. Notably, different approaches have emerged in the past years.

Taking Italy as an example, it is worth noting that, alongside various in-

on AI-Powered Facial Recognition Technologies: EU and US Regulatory Models, in *Comparative Law Review*, 1, 2026, 60.

[141] We also have to consider that according to art. 112(1) AI Act, the European Commission «shall assess the need for amendment of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5, once a year following the entry into force of this Regulation, and until the end of the period of the delegation of power laid down in Article 97. The Commission shall submit the findings of that assessment to the European Parliament and the Council».

[142] «It is our understanding that while the AIA should theoretically be directly applicable, including the exclusion provided for in Article 5(1)(h), it is only through national law that Member States will be able to benefit from the exclusion of the ban», A. Giannini-S. Tas, *Much Ado About Nothing?*, cit.

[143] On this very delicate implementation point, see F. Paolucci, *Enhancing Oversight and Addressing Gaps: Assessing the Impact of the AI Act on Biometric Identification Systems*, cit.

[144] 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*, 4, 2021, 101.

terventions by the national Data Protection Authority[145], the legislators adopted Law Decree (*Decreto legge*) No. 139 of 8 October 2021 –, later converted into Law No. 205 of 3 December 2021 –. This measure introduced a moratorium on the installation and use of video surveillance systems incorporating FRTs in public spaces or areas open and accessible to public. The suspension applied to both private and public entities, albeit with specific exceptions for security purposes (namely, the prevention and prosecution of crimes), subject to a prior favourable opinion of the *Garante*[146]. The moratorium was subsequently extended until 31 December 2025 by art. 8-ter, Law No. 87 of 3 July 2023.

More recently, as the extended deadline approached, the Italian legislators were once again required to assess whether and how to intervene in the field of FRTs. Through an amendment introduced in Law No. 26 of 27 February 2026, converting Law Decree No. 200 of 31 December 2025 (the so-called *Decreto Milleproroghe*)[147], the Parliament decided to renew the existing moratorium until 31 December 2027.

The effects of this measure may vary depending on the category of technology considered. With regard to real-time remote biometric identification systems (of which FRTs are a key example) used for law enforcement purposes in publicly accessible spaces, it should be recalled that art. 5(5) of the AI Act already imposes Member States to adopt domestic legislation fulfilling the conditions set out in art. 5(2-7), in order to permit the exceptional use of these instruments. Since the Italian legislature has not yet adopted such measures, the implementation and exploitation of the aforementioned systems must be regarded as prohibited as of February 2025, when the supranational rules on unacceptable risk entered into force[148].

While the Italian moratorium could therefore have limited practical implications on real-time systems for law enforcement purposes, it plays a significant role with respect to post remote biometric identification technologies based on FRTs. In fact, for these technologies, the rules on high-risk AI systems, under which they are classified, have not yet entered into for-

[145] On this point, see Section 2.1 of this work.

[146] The list of relevant offences and the procedural requirements for obtaining the approval of the *Garante* are set out in Legislative Decree (*Decreto legislativo*) No. 51 of 18 May 2018, implementing the LED in Italy. The moratorium applies exclusively to video surveillance systems using FRTs. A prior favourable opinion of the Data Protection Authority, as disciplined by art. 24(1) of Legislative Decree (*Decreto legislativo*) No. 51 of 18 May 2018, is not required in cases where such systems are used by judicial authorities or by the public prosecutor (*Pubblico Ministero*) (art. 9(12), Law Decree No. 139 of 8 October 2021).

[147] The amendment, proposed by Deputee Riccardo Magi, thus modified once again art. 9(9) of Law Decree No. 139 of 8 October 2021.

[148] As analysed in Section 2.2 of the present paper.

ce, leaving the matter primarily governed by the GDPR. The decision by the Italian Parliament to extend the moratorium consequently appears to respond to a perceived need for compliance of such technologies with both data protection requirements and the broader framework of fundamental rights reflected in the AI Act approach. From this perspective, the suspension may be considered a strongly protective solution, capable of avoiding regulatory gaps and a potential weakening of safeguards pending the full application of the AI Act.

In this context, the debate remains largely open, with the extension of the moratorium providing additional time for legislators to determine the next steps. First, the Italian lawmakers will be required to decide whether to adopt specific legislation on real-time systems in order to permit their exceptional use, or to refrain from doing so. In fact, as guaranteed by the AI Act, Member States may also choose to introduce stricter rules in this field (art. 5(5) AI Act). Although it is difficult to predict if such a framework will be adopted, any decision in this regard would require careful consideration of the procedural safeguards to be put in place, as well as the authorities responsible for prior authorisation.

Secondly, as regards post systems, the extension of the moratorium may be seen as acknowledging the necessity for a comprehensive and carefully designed legislative intervention capable of addressing risks to a wide range of fundamental rights, not limited to data protection. Such an intervention should take into account not only the guarantees established by the AI Act – once fully applicable, and subject to possible delays, as will be discussed later in relation to the Digital Omnibus Package –, but also the need for detailed rules on issues such as data retention, the composition of the watchlist and potential differentiations depending on the private or public nature of the actors involved. Alternatively, the legislature could follow the approach advocated by several NGOs, among which *Rete Diritti Umani Digitali*, consisting in maintaining a general ban on the use of these technologies, both real-time and post.

The key choices and regulatory approaches that the Italian legislators will be required to adopt with regard to FRTs and biometric systems also form part of a broader ongoing legislative process, primarily reflected in Law No. 132 of 23 September 2025, entitled "Provisions and delegation to the Government in the field of AI" (*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*). Among its various provisions[149], art. 24 grants broad

[149] This legislative intervention reaffirms several key principles of AI governance adopted at the supranational level, including the anthropocentric dimension, respect for fundamental rights, the guarantee of transparent, reliable and accurate AI systems. Alongside these general principles and without introducing additional obligations beyond those already introduced by the AI Act, the law also addresses specific sectors such as healthcare, education, economic development, public and national security, workplace

delegated powers to the Government, authorising it to adopt a significant number of legislative decrees (*decreti legislativi*) aimed at aligning and adapting national legislation to the supranational framework. Since these powers also extend to the security sector, including law enforcement, it will be particularly important to assess if and how specific rules, also governing biometric systems, will be introduced in compliance with the AI Act.

Given the space left by the AI Act to Member States' intervention, its actual impact remains difficult to assess at this stage. This uncertainty is further compounded by recent developments associated with the so-called EU Digital Omnibus Package. It includes both the Digital Omnibus[150], primarily concerning the reform of data protection rules, and the Digital Omnibus on AI[151], which directly affects the AI Act. Aimed at increasing efficiency, reducing the costs of compliance and, consequently, enhancing competitiveness, as well as ensuring a simplified and proportionate implementation of certain AI Act measures[152], these proposals have already sparked considerable controversy[153].

AI, public administration. The law further designates the national authorities for AI, namely the *Agenzia per l'Italia digitale* (AgID) and the *Agenzia per la cybersicurezza nazionale* (ACN). On the Italian legislation on AI, see F. Paolucci, *La legge italiana sull'intelligenza artificiale: attuazione nazionale dell'AI Act e primi nodi applicativi*, in *Quaderni Costituzionali*, 4, 2025, 965; O. Pollicino, G Muto, *La legislazione delegata in materia di intelligenza artificiale: la costruzione di una disciplina organica al confine tra scelte governative, controllo parlamentare e vincoli europei*, in this Journal, 2, 2025, 393.

[150] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM/2025/837.

[151] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM/2025/836.

[152] *As stated by the Commission*, the proposal on Digital Omnibus «includes a set of technical amendments to a large corpus of digital legislation, selected to bring immediate relief to businesses, public administrations, and citizens alike, and to stimulate competitiveness. It is a first step to optimise the application of the digital rulebook. The immediate objective is to ensure that compliance with the rules comes at a lower cost, delivers on the same objectives, and brings in itself a competitive advantage to responsible businesses» (in *digital-strategy.ec.europa.eu*, accessed 20 January 2026). *With regards to the Digital Omnibus on AI*, it is intended to introduce «targeted simplification measures to ensure timely, smooth and proportionate implementation of certain of the AI Act's provisions» (*ibid.*, accessed 20 January 2026).

[153] It is worth noting that some scholars and NGOs expressed concerns about the potential impact of the Omnibus Package on fundamental rights and about the risk of increased legal uncertainty – something that companies are also keen to avoid –, while

Although a comprehensive analysis of these initiatives falls beyond the scope of this contribution, it is important to note that some of the proposed amendments are likely to have implications for biometric identification systems.

First, with regard to the Commission's proposals[154], several provisions are expected to affect the processing of biometric data. In particular, the Digital Omnibus seeks to address the legal basis for processing special categories of personal data used in AI training and development, when such data are accidentally included in datasets due to the technical difficulty of removing them. It also introduces an exception to the already mentioned general prohibition on processing biometric data in cases of biometric verification.

Similarly, the Omnibus on AI includes changes that may directly influence the deployment and implementation of biometric systems and the processing of biometric data. In particular, it proposes to broaden the legal basis for providers and deployers of AI systems to process special categories of personal data – including biometric data – for purposes of bias detection and correction. This expansion would no longer be limited to high-risk systems, as is currently the case, but would also apply to other categories of AI systems. This development may be understood as an instrument to

others consider simplification measures both necessary and overdue (for first comments, see R. Mahieu, *The Ominous Omnibus: Dismantling the Right of Access to Personal Data*, in *Verfassungsblog*, 3 December 2025; B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite*, in *MediaLaws – Symposium*, 19 December 2025; H. Hofmann, *This Is Not Simplification: How to Simplify the Digital Acquis Without Undermining Rights*, in *Verfassungsblog,* 3 January 2026). See also the study published by the Policy Department for Economy and Growth, Directorate-General for Economy, Transformation and Industry, *A Digital Omnibus: Identifying Interlinks and Possible Overlaps Between Different Legal Acts in the Field of Digital Legislation to Streamline Tech Rules*, European Parliament, 2026; EDPB-EDPS *Joint Opinion 1/2026 on the Proposal for a Regulation as Regards the Simplification of the Implementation of Harmonised Rules on AI (Digital Omnibus on AI)*, 21 January 2026; EDPB-EDPS *Joint opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, 11 February 2026. In these documents, while recalling that joint guidelines with the Commission on the delicate interplay between the GDPR and the AI Act are expected later this year, the EDPB and EDPS stress the need of «A careful balance to be kept between reducing administrative burden where possible, without undermining the protection of fundamental rights in the context of AI». They expressed concerns about the potential impact on the protection of fundamental rights of the proposed moveable deadline of the high-risks AI systems rules, also underlining the dangers in terms of legal certainty. The EDPB and EDPS also warned of the importance of establishing clear limits and conditions on the possible extension of the use of sensitive data, as proposed in the Digital Omnibus on AI.

[154] The European Parliament on 26 March 2026 adopted its position on the proposal with numerous amendments. This very recent development marks the beginning of the negotiations with the Council on the final text. See the Press Release of the European Parliament, *Artificial Intelligence Act: Delayed Application, Ban on Nudifier Apps*, 26 March 2026.

facilitate compliance with the data protection framework, which, as noted in the previous Section of this paper, has been identified as a critical issue. In addition, a possible "stop-the-clock" mechanism may be introduced with regard to the implementation timeline for rules on high-risk AI systems. In particular, under art. 113 of the AI Act, the provisions concerning high-risk AI systems listed in Annex III – including certain non-prohibited biometric systems, as discussed in Section 2.2. of this paper – are scheduled to apply from 2 August 2026. The Commission's proposal would postpone the application of these rules, in any event no later than 2 December 2027 for Annex III high-risk AI systems, while providing in the meantime for the adoption of appropriate supporting measures, such as harmonised standards, guidance and compliance tools for high-risk AI requirements[155].

While it is true that the Omnibus on AI is not intended to immediately affect prohibited practices – among which the most controversial biometric systems –, the potential delay in the application of rules on high-risks systems translates into a prolonged absence of the vaster and more comprehensive safeguards established by the AI Act. The deferral thus raises questions as to the resilience of the fundamental rights protection enshrined in the AI Act in the face of other priorities, such as competitiveness and efficiency, particularly in a context shaped by increasing geopolitical tensions[156].

At the same time, the intention to facilitate the use of biometric data for AI training and bias detection could undoubtedly prove useful for providers and deployers. Nonetheless, it also risks normalising the processing of sensitive data and diluting both the necessity test and existing prohibitions.

More broadly, the objective of simplification is both legitimate and understandable: it can contribute to enhancing the attractiveness and correct functioning of the EU internal market, while also improving consistency across a complex legislative framework. The main concern, however, is that of missing the forest for the trees: further modifying the regulatory landscape may create uncertainty and blur one of the fundamental purposes of legislative intervention in this field. Namely, to ensure that technologies are embedded within the "constitutional" framework of rights, freedoms and values established at the EU level through digital legislation and the case-law of the CJEU, thereby preserving a unique and distinctive model in the global arena[157].

---

[155] For an in-depth analysis of the described provisions, see E. Aldibs *et al.*, *White Paper on the Digital Omnibus Proposal and the AI Omnibus Proposal*, Leuven, 2026.

[156] E. Celeste, *Digital Omnibus: Quo Vadis?*, in ***docu.ie***, , accessed 20 January 2026.

[157] We can recall the concept of the *Brussels Effect*, valid also in the digital law sphere (A.

Considering this scenario and with specific regard to AI-powered biometric systems, the main effort to be ensured, therefore, is the maintenance of a high level of fundamental rights protection throughout the reform process initiated by the Omnibus Package. As the analysis presented in this paper suggests, this can only be achieved by continuing to take into account the peculiar nature and intrinsic – and unique – risks related to biometric data and biometric systems, and by limiting their use to what is strictly necessary, within a framework of rules capable of delimiting practices that might otherwise lead to indiscriminate processing of sensitive data for the sake of simplifying AI-related operations.

As a consequence, the future discussion on the adoption of such reformed rules must be carefully monitored throughout the legislative debate, as it will shape the trajectory of the digital regulatory ecosystem the EU is currently attempting to (re)define. How EU Institutions will address this ambition will be of crucial importance.

This ongoing legislative discussion clearly illustrates how regulatory efforts in the field of AI, data protection and, most notably for present purposes, biometric data and AI-based biometric systems remain in constant evolution.

In conclusion, in this context of constant regulatory developments, it is essential to situate both the existing discipline and the discussed reforms concerning biometric systems within the broader constitutional framework. The real and profound challenge lies in guaranteeing that legislative interventions remain oriented towards the "constitutionalisation"[158] of AI-based biometric technologies, understood as their interpretation in the light of constitutional principles and fundamental rights.

This also requires moving beyond an oversimplified «AI-as-existential threat narrative»[159]. At present, it seems unlikely that AI-powered biometric systems can be entirely halted or banned. Once the genie is out of the lamp, it is difficult to put it back and renounce to its powers, especially when its ability to fulfil desires makes it so appealing. Yet, despite this reality, the aim should be, as in the story of Aladdin, to maintain conscious and responsible control over the genie, so as to prevent its misuse for

Bradford, *The Brussels effect*, in *Northwestern University Law Review*, 1, 2012, 1; F. Fabbrini-E. Celeste-J. Quinn (eds.), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignity*, London, 2021.

[158] More generally, on the concept of "constitutionalisation" of mass surveillance practices see E. Celeste-G. Formici, *Constitutionalizing Mass Surveillance in the EU*, cit.

[159] R.J. Neuwirth, *Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)*, cit.; on the simplified dichotomy between "adoption" or "ban", see O. Lobel, *The Law of AI for Good*, in *Florida Law Review*, 75, 2023, 1073.

harmful purposes[160].
Regulatory decisions should therefore avoid simplistic solutions and instead pursue nuanced, forward-looking and innovative responses, capable of identifying a careful balance between overly restrictive provisions and insufficient safeguards.
A first step in this direction is the development of clearer, more precise and stringent rules capable of assessing whether a given AI-powered practice using biometric data is genuinely necessary[161]. This assessment should form part be part of careful scrutiny by authorities, private actors and courts. Society should not be categorically deprived of the benefits of biometric systems, but it is essential first to determine whether these systems are truly and concretely useful for achieving a specific purpose. In this respect, the debate on necessity criterion, as noted in this paper, remains far from sufficiently explored[162].
If the necessity test is satisfied, the next step should be that of evaluating if and how the technology can be aligned with constitutional values.
Drawing on the metaphor of the lamp, the law should prevent certain desires – and uses – from being expressed. In this regard, the AI Act appears to adopt a coherent approach, assessing *ex ante* when AI-based biometric systems have the potential to unacceptably jeopardise or erode other constitutional rights or freedoms.
Even when no such risk exists, there remains a need to establish rules that ensure the responsible, acceptable and proper use of the genie. Doing so allows Aladdin – and all the other potential users – to harness the potential "good" of these technologies while preventing misuse and dangerous effects.
The development, interpretation and implementation of these rules must

[160] We refer to the original story in the well-known *Arabian Nights*. Although Aladdin initially used the genie for personal gain, his clever and strategic use ultimately produced positive outcomes. Similarly, AI-powered biometric systems, once unleashed, should be guided and regulated in ways that maximize their benefits while minimizing harm.

[161] N. Menendez Gonzalez, *Technical Solutions for a Proportional Use of FRT*, in N. Menendez Gonzalez-G. Mobilio (eds.), *Next Democratic Frontiers for Facial Recognition Technology (FRT)*, cit., 33.

[162] The necessity of such systems remains an often underexplored dimension of analysis and evaluation; in fact, several scholars «consider that much of the discussion has taken for granted the existence of such technologies as a necessary means for securing public safety», C. Jasserand, *Facial Recognition in Public Spaces and the Principle of Necessity*, cit., 68; also Murray critically affirmed that the focus of multiple legislative efforts related to FRT and biometric systems have «been on limiting use, and establishing safeguards, rather than really questioning what the impact of FRT might be (..) and whether certain applications of this technology should be used at all», D. Murray, *Facial Recognition and the End of Humal Rights as We Know Them?*, cit., 146. As already underlined, this aspect remains critical also with regards to other technologies, such as data retention schemes (see *supra* note 131).

be guided by a fundamental principle: shielding human identity and emotions from interferences enabled by AI. This also entails averting dystopian futures characterized by pervasive biometric surveillance, resisting the commodification of our bodies and unique traits and preserving intimacy as an essential component of human dignity[163]. The ability of resisting the weaponization of sensitive data and surveillance mechanisms based on the exploitation of our "identity/ies" is crucial to avoid control instruments by both public authorities and private actors.
Addressing this enormous and rapidly evolving challenge represents a key factor in determining whether the EU can realize its ambition of fostering a human-centered and trustworthy AI[164].

Abstract

Automated biometric systems are increasingly deployed across public and private sectors, raising urgent concerns for the protection of fundamental rights. After outlining the main legal challenges posed by the implementation of these technologies, the paper examines EU regulatory response, focusing on the recent innovations introduced by the AI Act. Particular attention is therefore attributed to the "prohibited AI practices" set out in Article 5, AI Act. The analysis explores how EU lawmakers seek to balance innovation, efficiency and security with the need to safeguard fundamental freedoms. The concluding Section identifies unresolved issues and persistent concerns, highlighting the difficulty of regulating pervasive technologies that are increasingly embedded in contemporary societies. Future regulatory efforts in this domain will be crucial to promoting human-centric and trustworthy AI systems and preventing surveillance practices.

Keywords

AI-based biometric systems - AI Act - fundamental rights protection - biometric data - biometric surveillance

---

163 Y. Wen *et al.*, *Face De-Indentification: Safeguarding Identities in the Digital Era*, Cham, 2024; see also A. Pin, *Artificial Intelligence, the Public Space, and the Right to Be Ignored*, in J. Temperman-A. Quintavalla (eds.), *Artificial Intelligence and Human Rights*, Oxford, 2023, 177.

164 On this broad topic, *ex multis*, G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022; G. De Gregorio *et al.* (eds.), *The Oxford Handbook of Digital Constitutionalism*, Oxford, 2024; M. Fasan, *Intelligenza artificiale e costituzionalismo contemporaneo*, Naples, 2024; W. Barfield-U. Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence. Current and Future Directions*, Cheltenham, 2025; P.K. Dutta *et al.* (eds.), *Artificial Intelligence and Human Rights, Democracy, and the Rule of Law*, Boca Raton, 2026.

L'ecosistema digitale europeo tra proclamazione assiologica ed effettività normativa*

Raffaele Torino

Sommario

1. L'ecosistema digitale europeo online come arena regolatoria – 2. La Dichiarazione del 2022 come cornice assiologica – 3. Il principio antropocentrico – 4. La promozione della solidarietà e dell'inclusione nell'ecosistema digitale europeo – 5. La libertà di scelta sostanziale – 6. La partecipazione allo spazio pubblico digitale – 7. La sicurezza e la protezione delle persone – 8. La sostenibilità ambientale e intergenerazionale – 9. Conclusioni: un antropocentrismo prevalentemente reattivo

1. L'ecosistema digitale europeo online come arena regolatoria

L'ecosistema digitale europeo può essere ricostruito, nella sua dimensione economica essenziale, come il mercato dei servizi prestati in rete (online) a favore di utenti stabiliti nel territorio dell'Unione[1]. Nel volgere di poco più di un decennio tale mercato ha cessato di essere un comparto specialistico per divenire l'infrastruttura ordinaria dell'esistenza quotidiana di centinaia

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

[1] Sebbene il termine "ecosistema digitale" indichi, in senso proprio, la totalità dei processi, delle infrastrutture e degli ambienti che operano in formato binario (includendo contesti anche del tutto estranei alla connessione in rete, come i sistemi embedded, l'automazione industriale o l'archiviazione locale), lo impiegherò in un'accezione deliberatamente più ristretta. Con "ecosistema digitale" designerò esclusivamente lo spazio online: l'insieme delle piattaforme, dei servizi intermediari, dei sistemi algoritmici e delle infrastrutture di connessione che operano in rete e che il corpus regolatorio europeo esaminato disciplina. Tale restrizione riflette il perimetro applicativo dei regolamenti che saranno oggetto del presente studio, ciascuno dei quali costruisce le proprie figure soggettive (l'interessato, il destinatario del servizio, l'utente finale, la persona esposta a sistemi di IA) in relazione a relazioni che si svolgono, per definizione, in rete, ossia online. In maniera analoga, quando utilizzerò il termine "digitale" mi riferirò alla manifestazione online di tutto ciò che è digitale.

di milioni di persone[2]. Lo spazio digitale è insieme, da una parte, il luogo in cui ci si informa, si formano e si manifestano le opinioni, si intrattengono relazioni sociali, si partecipa al dibattito pubblico e, dall'altra parte, il teatro di un'intensa attività economica, dove il commercio elettronico di beni fisici coesiste con la distribuzione di servizi integralmente smaterializzati. La distinzione tra spazio digitale e spazio analogico, già teoricamente problematica, si è progressivamente attenuata fino a risultare, nella pratica quotidiana, difficilmente percepibile: il digitale online non è più uno strumento tra gli altri, ma la forma prevalente attraverso cui si esercitano le pratiche fondamentali dell'esistenza.

Le dimensioni quantitative di questo ecosistema rendono manifesta la sua rilevanza[3]. L'analisi per segmenti rivela, in quasi tutte le categorie rilevanti, una concentrazione di potere economico di carattere oligopolistico[4], finanche antagonista del potere regolatorio pubblico[5].

I servizi che si svolgono nell'ecosistema digitale sono classificabili in alcune macrocategorie e in ciascuna di esse la struttura del mercato europeo è caratterizzata dalla presenza di uno o pochissimi operatori dominanti, pressoché tutti di origine statunitense. Questi operatori detengono quote di mercato tali da configurare una posizione di *gatekeeper*: controllano l'accesso degli utenti ai servizi e l'accesso dei fornitori terzi agli utenti, definendo unilateralmente le condizioni di un ecosistema che formalmente appartiene al mercato interno europeo, ma che è strutturalmente governato da soggetti che operano secondo logiche e valori radicalmente diversi e che faticano (o semplicemente non vogliono) adeguarsi alle regole europee. Il dato è tanto più significativo se si considera che, come ha sottolineato il Rapporto Draghi del settembre 2024, solo quattro delle prime

---

[2] L. Floridi (a cura di), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, 2015.

[3] Secondo i dati Eurostat (Eurostat, *Digitalisation in Europe*, ed. 2025, in *ec.europa.eu*, nel 2024 il 93% della popolazione europea ha utilizzato internet; tra gli usi principali figurano la ricerca di informazioni su prodotti e servizi (81%), le comunicazioni vocali e video (79%), l'home banking (72%) e l'accesso a contenuti informativi e social network (circa il 70%). Il 77% degli europei ha effettuato acquisti online e il fatturato generato dalle vendite in rete ha rappresentato il 19% del fatturato totale delle imprese europee.

[4] K. Kowalski - C. Volpin - Z. Zombori, *Competition in Generative AI and Virtual Worlds,* Competition Policy Brief, 3, September 2024, J. Crémer - Y.A. de Montjoye - H. Schweitzer, *Competition Policy for the Digital Era*, rapporto per la Commissione europea, DG Competition, Lussemburgo, 2019, in *ec.europa.eu*. Per un'analisi sistematica della struttura di mercato delle piattaforme digitali e dei suoi effetti sul benessere degli utenti, v. anche J. Furman et al., *Unlocking Digital Competition. Report of the Digital Competition Expert Panel*, Londra, 2019, Stigler Committee on Digital Platforms, *Final Report*, Chicago, 2019, L.M. Khan, *Amazon's Antitrust Paradox*, *Yale Law Journal,* 126, 2017, 710.

[5] In argomento, v. O. Pollicino, *Potere digitale*, in M. Cartabia – M. Ruotolo (dir.), *Enciclopedia del diritto*, I Tematici, V-2023, *Potere e Costituzione*, Milano, 2003.

cinquanta imprese tecnologiche mondiali sono europee[6].
L'asimmetria geopolitica costituita da un mercato da quasi un trilione di euro governato da regole europee[7], ma servito quasi esclusivamente da imprese statunitensi, costituisce un elemento strutturale di primaria rilevanza al quale l'Unione ha risposto secondo un approccio che si può definire precipuamente europeo: da un lato, disciplinando il fenomeno in conformità ai propri valori e ai propri obiettivi regolatòri[8]; dall'altro, cercando di sostenere, nel contesto del mercato interno, le imprese europee del settore e di salvaguardare la risorsa strategica fondamentale di tale mercato, ossia i dati che vengono incessantemente prodotti nell'ecosistema digitale europeo.
Il presente contributo si propone di indagare il primo profilo, ricostruendo e valutando criticamente i valori in base ai quali l'Unione ha disciplinato l'ecosistema digitale online. L'indagine si organizza attorno a due interrogativi che ne guidano lo sviluppo. Il primo riguarda la misura in cui il corpus normativo europeo adottato nell'ultimo decennio ha tradotto i valori proclamati dalla Dichiarazione europea sui diritti e i principi digitali per il decennio digitale del 2022in posizioni giuridiche soggettive azionabili e standard giurisprudenziali effettivi. Il secondo investe la qualità di questa traduzione e, specificamente, se la risposta regolatoria dell'Unione abbia saputo costruire condizioni positive di autonomia della persona allorché agisce online o si sia limitata a contenere i rischi della tecnologia. La risposta alle due domande, qui anticipata e argomentata nei paragrafi che seguono, è che la giurisdizionalizzazione procede in modo asimmetrico tra i sei valori della Dichiarazione del 2022 e che, sul piano qualitativo, il modello europeo ha sviluppato una postura prevalentemente difensiva che si può definire di *antropocentrismo reattivo*.
L'ipotesi che guida l'analisi è, infatti, che il modello europeo abbia sviluppato una regolamentazione più efficace nel limitare i rischi tecnologici che nel costruire condizioni positive di autonomia della persona e partecipazione democratica.

---

[6] M. Draghi, *The Future of European Competitiveness. A Competitiveness Strategy for Europe*, rapporto alla Commissione europea, settembre 2024, 5.

[7] Per tutti, v. O. Pollicino, *Regolazione e innovazione tecnologica nell'"ordinamento della rete"*, in *Rivista AIC*, 2, 2025, 8 aprile 2025, S. Calzolaio - A. Iannuzzi - E. Longo - M. Orofino - F. Pizzetti, *La regolazione europea della società digitale*, Torino, 2024.

[8] Esula dal presente contributo l'analisi della capacità regolatoria dell'Unione di proiettare i propri standard al di là dei propri confini, definita come *Brussels Effect*, ossia il meccanismo di esportazione involontaria di regole attraverso cui l'Unione eserciterebbe una forma di sovranità regolatoria globale che prescinde dalla giurisdizione formale. In argomento, ovviamente, A. Bradford, *The Brussels Effect. How the European Union Rules the World*, Oxford, 2020, A. Bradford, *Digital Empires. The Global Battle to Regulate Technology*, Oxford, 2023.

Il presente contributo assume i valori proclamati nella Dichiarazione del 2022 non come meri enunciati programmatici, ma come categorie ordinanti utili a testare la coerenza materiale del diritto derivato. L'oggetto dell'analisi non è dunque la validità formale degli atti, bensì la loro capacità di tradurre i valori proclamati in posizioni giuridiche soggettive, obblighi regolatori e standard giurisprudenziali effettivi: il passaggio dalla proclamazione alla giurisdizionalizzazione è il banco di prova su cui si misura la tenuta del modello europeo. L'analisi non si concentrerà sulla struttura delle basi giuridiche degli atti (primariamente l'art. 114 TFUE per il mercato interno e l'art. 16 TFUE per la protezione dei dati) la cui scelta da parte del legislatore dell'Unione pone questioni rilevanti sul piano della competenza e del riparto di poteri, che esulano però dall'obiettivo del presente contributo.
L'esame prende avvio dalla Dichiarazione del 2022, assunta come chiave di lettura dell'architettura normativa (par. 2), per verificare poi la declinazione dei suoi valori nei principali strumenti regolatori. Saranno oggetto di indagine il principio antropocentrico (par. 3), la promozione della solidarietà e dell'inclusione nell'ambito dell'ecosistema digitale europeo (par. 4), la libertà di scelta sostanziale (par. 5), la partecipazione allo spazio pubblico digitale (par. 6), la sicurezza e la protezione delle persone (par. 7), la sostenibilità ambientale e intergenerazionale (par. 8). Il paragrafo conclusivo (par. 9) offre alla discussione un bilancio complessivo del modello regolatorio europeo, individuandone i limiti strutturali e le prospettive evolutive.

2. La Dichiarazione del 2022 come cornice assiologica

Nel dicembre del 2022 il Parlamento europeo, il Consiglio e la Commissione hanno congiuntamente proclamato, in forma interistituzionale, la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale[9].
La Dichiarazione del 2022 si inserisce nel percorso di costruzione di una politica digitale europea dotata di una propria identità valoriale[10], come

[9] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, 2022/C 23/01. V., in argomento, P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *DUE*, 2022, 163; E. Quinn, *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *VBlog*, 22 dicembre 2022; P. Passaglia, *La Dichiarazione per la sovranità digitale europea e l'utilità (trascurata) del ricorso alla geopolitica*, in *MediaLaws. Rivista di Diritto dei Media*, 11 febbraio 2026, 3, 2025, 348.

[10] Tale percorso prende avvio con la Comunicazione della Commissione "Plasmare il futuro digitale dell'Europa" del febbraio 2020 (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final), che ha individuato

complemento assiologico della Bussola per il digitale 2030[11], che ha tradotto le priorità strategiche in obiettivi misurabili. La Bussola per il 2020 definisce cosa l'Unione vuole raggiungere, mentre la Dichiarazione del 2022 stabilisce entro quali vincoli valoriali il raggiungimento è da ritenersi legittimo.

La Dichiarazione del 2022 si colloca nella categoria degli strumenti di soft law e non produce obblighi giuridicamente vincolanti per gli Stati membri e per gli operatori privati, né attribuisce diritti soggettivi direttamente azionabili dai singoli. Sarebbe tuttavia superficiale sottovalutarne la portata giuridica, poiché sul piano funzionale essa orienta il legislatore dell'Unione nella definizione delle scelte normative in materia digitale, offre il parametro valoriale rispetto al quale misurare la compatibilità degli atti di diritto derivato, e funge da criterio orientativo ed ermeneutico per l'interprete chiamato a ricostruire la ratio degli obblighi imposti dalla normativa vincolante. Quest'ultima funzione trova conferma esplicita nel sistema delle fonti: l'AI Act stabilisce che le regole armonizzate sui sistemi di intelligenza artificiale «dovrebbero tenere conto della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale» (considerando 7). La Dichiarazione del 2022 opera come meccanismo di vincolo istituzionale del legislatore europeo, ossia una forma di *pre-commitment* valoriale che restringe lo spazio delle scelte normative legittime non sul piano della validità formale, ma su quello della coerenza assiologica[12].

Sebbene non sia invalido, un atto di diritto digitale che si ponga in contrasto con i principi della Dichiarazione del 2022 tradisce la coerenza interna del modello europeo, che ha assunto i valori della Dichiarazione del 2022 come propria identità regolatoria. Sul piano ermeneutico, la Dichiarazione del 2022 ha creato un ambiente interpretativo nel quale quegli stessi valori operano come canoni di lettura degli atti successivi: il giudice chiamato a interpretare una norma in tensione con essi dispone di uno strumento argomentativo per orientarne il significato in senso conforme; l'avvocato generale può farne uso nelle proprie conclusioni; la Commissione può valorizzarli in sede di *enforcement*. Ne deriva una pressione argomentativa crescente sul legislatore, che non è evidentemente una sanzione, ma una forma di *accountability* discorsiva che si esercita negli spazi dell'interpretazione giudiziale, del controllo parlamentare e del dibattito dottrinale. La

nella transizione digitale una delle due priorità strategiche del mandato 2019-2024.

[11] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final.

[12] E. Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Oxon, 2023, G. De Gregorio, *The Declaration on European Digital Rights and Principles: A First Analysis from Digital Constitutionalism*, in *The Digital Constitutionalist*, 2 February 2022.

misura in cui questa pressione produca effetti giuridici reali dipende, in ultima analisi, dalla disponibilità della Corte di giustizia a recepire la Dichiarazione del 2022 come criterio ermeneutico rilevante: un passaggio che – come si vedrà - la giurisprudenza non ha ancora compiuto, ma che la logica del sistema valoriale dell'Unione non esclude.
Sul piano testuale, la Dichiarazione del 2022 si articola in sei capitoli corrispondenti ad altrettante aree tematiche: la centralità della persona nella trasformazione digitale; la solidarietà e l'inclusione; la libertà di scelta; la partecipazione allo spazio pubblico digitale; la sicurezza, la protezione e il conferimento di maggiore autonomia e responsabilità; la sostenibilità. L'intero documento è permeato da una centrale ed essenziale concezione antropocentrica secondo la quale la tecnologia deve essere concepita come strumento al servizio dell'essere umano, non come fine in sé, né come variabile indipendente rispetto alla quale il diritto debba soltanto adattarsi. Questa impostazione introduce nella regolazione dell'ecosistema digitale europeo una discontinuità rispetto al paradigma tradizionale del mercato interno, nel quale la liberalizzazione dei servizi è il fine e la tutela dei diritti il suo limite esterno. Tale discontinuità, come si vedrà, non è sempre coerentemente tradotta negli atti di diritto derivato adottati in un arco temporale di circa un decennio.

3. Il principio antropocentrico

Il principio antropocentrico è attuato nell'architettura regolatoria europea in forma prevalentemente difensiva, poiché la persona appare essere tutelata dai rischi della tecnologia più di quanto sia messa nelle condizioni di appropriarsi dei suoi benefici. Questa tensione attraversa il primo capitolo della Dichiarazione del 2022 ("Mettere le persone al centro della trasformazione digitale"), che enuncia il principio fondativo dell'intero sistema valoriale: la tecnologia deve essere al servizio delle persone e andare a loro beneficio[13], mettendole nelle condizioni di perseguire le proprie aspirazioni «in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali» (art. 1 della Dichiarazione del 2022).
La formulazione del Capitolo I esprime una scelta di metodo prima ancora che di contenuto: il soggetto giuridico di riferimento dell'intero sistema regolatorio non è il mercato, l'innovazione o la tecnologia in sé, ma la persona. Questa impostazione risponde a una precisa opzione teorica che può definirsi di "antropocentrismo regolatorio", contrapposta tanto al tecno-centrismo (che assume il progresso tecnologico come valore autono-

[13] L. Floridi et al., *AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 689.

mo rispetto al quale il diritto deve adattarsi) quanto al mercato-centrismo (che subordina gli obiettivi e i contenuti della regolazione alle esigenze di efficienza allocativa delle risorse in un libero mercato).
Va sottolineato che il Capitolo I individua nel principio di equivalenza online/offline uno dei pilastri del modello europeo: ciò che è illegale offline è illegale online, e i diritti riconosciuti nell'ambiente fisico devono essere garantiti nell'ambiente digitale senza regressione. Questo principio funziona da clausola generale di estensione dell'intera Carta dei diritti fondamentali dell'Unione europea all'ecosistema digitale online.
In questo contesto, il riferimento più diretto ed esplicito all'antropocentrismo è nell'AI Act[14], che nel considerando 6 enuncia che l'intelligenza artificiale «dovrebbe essere una tecnologia antropocentrica» e «fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani», richiamando esplicitamente la Dichiarazione del 2022 quale riferimento orientativo (considerando 7), e all'art. 1, par. 1, enuncia come scopo del regolamento «promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile»[15]. La struttura normativa dell'AI Act incarna questo principio in un sistema a gradazione di rischio: i sistemi di IA che comportano rischi inaccettabili per la dignità, la libertà e i diritti fondamentali sono vietati[16]; quelli ad alto rischio sono soggetti a obblighi stringenti di trasparenza, documentazione tecnica e supervisione umana.
Pur se precedente alla Dichiarazione del 2022, il GDPR costituisce per molti aspetti l'anticipazione normativa più compiuta dell'antropocentrismo regolatorio e sua componente fondamentale[17]. Il considerando 4

[14] 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).

[15] Nell'AI Act il termine ricorre con una frequenza che non ha precedenti nel diritto digitale europeo. Oltre a comparire nell'oggetto del regolamento (art. 1, par. 1) e nel considerando 6, il termine si ritrova anche nel considerando 8, che richiama «l'approccio antropocentrico europeo all'IA», nel considerando 27, che riprende il lessico degli orientamenti etici dell'AI HLEG per un'IA «affidabile ed antropocentrica» e infine nel considerando 176, che replica la formula dell'art. 1 nella clausola di sussidiarietà.

[16] In argomento v. N. Zorzi Galgano, *Il regolamento (UE) 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contratto e Impresa*, 1, 2025, 45.

[17] 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 atti e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
In realtà, la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati

enuncia con nettezza che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo», mentre il considerando 1 e l'art. 1 del medesimo qualificano la protezione dei dati personali come diritto fondamentale. Fondando la disciplina del trattamento sui diritti azionabili dell'interessato (accesso, rettifica, cancellazione, portabilità, opposizione al trattamento automatizzato), il GDPR ha introdotto nel diritto dell'Unione una concezione personalistica del dato che il Capitolo I della Dichiarazione assume e generalizza[18].

L'ulteriore diritto derivato declina l'antropocentrismo in modo asimmetrico, ciascuno strumento incarnandone una variante distinta. Il DSA[19] lo costruisce come tutela rafforzata del soggetto vulnerabile, vietando la pubblicità profilata nei confronti dei minori e imponendo alle piattaforme di dimensioni molto grandi valutazioni di impatto che riconducono esplicitamente la dignità umana sancita dall'art. 1 della Carta tra i diritti fondamentali da preservare[20]. Il DMA[21], di vocazione formalmente concorrenziale, opera sul piano della tutela del contraente debole: la garanzia di mercati equi e contendibili «a vantaggio degli utenti commerciali e degli utenti finali» è il presidio indiretto della centralità della persona contro gli «squilibri gravi in termini di potere contrattuale» imposti dai *gatekeeper*[22]. Il

personali, nonché alla libera circolazione di tali dati (abrogata dal GDPR con effetto dal 25 maggio 2018) già affermava (considerando 2) che i sistemi di trattamento dei dati «sono al servizio dell'uomo» e che essi «devono, qualunque sia la nazionalità o la residenza delle persone fisiche, rispettare le libertà e i diritti fondamentali delle persone fisiche». L'antropocentrismo del GDPR non è dunque un'innovazione valoriale introdotta nel 2016, ma il consolidamento e l'estensione sistematica di un principio già inscritto nel fondamento genetico del diritto europeo della protezione dei dati. In questa prospettiva, la direttiva 95/46/CE — e non il GDPR — è il vero atto fondativo dell'antropocentrismo regolatorio digitale europeo e la continuità tra i due strumenti sul piano assiologico è più rilevante della discontinuità sul piano tecnico.

[18] Sulla concezione personalistica del dato rimangono fondamentali le riflessioni di S. Rodotà, *Il diritto ad avere diritti*, Bari, 2021, in specie il cap. 12.

[19] 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).

[20] L'art. 28 DSA vieta la pubblicità profilata nei confronti dei minori e impone a tutte le piattaforme misure adeguate e proporzionate a garanzia della loro protezione online; l'art. 34, par. 1, lett. b), obbliga le piattaforme di dimensioni molto grandi a valutare i rischi sistemici per i diritti fondamentali, con riferimento esplicito alla dignità umana sancita dall'art. 1 della Carta dei diritti fondamentali dell'Unione europea.

[21] 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).

[22] L'obiettivo è enunciato dall'art. 1, par. 1 DMA; la descrizione delle pratiche dei gatekeeper come fonte di squilibri contrattuali è del considerando 4.

DGA[23] radica il principio sul piano lessicale: insieme all'AI Act, è l'unico atto in cui il termine "antropocentrico" compare in via testuale (considerando 3), segnando una progressiva sedimentazione del principio nel diritto derivato. L'EMFA[24], infine, sposta il baricentro dalla persona-utente alla persona-cittadino: la fruizione di contenuti mediatici pluralistici come «fondamentale per promuovere il dibattito pubblico e la partecipazione civica» trasforma l'antropocentrismo in funzione civica, completando in dimensione partecipativa la tutela individuale prevalente negli altri strumenti.

Sul piano giurisprudenziale, il termine "antropocentrico" non compare in alcuna pronuncia della Corte di giustizia. Eppure la logica antropocentrica percorre in maniera sotterranea le decisioni più rilevanti della corte di Lussemburgo in materia digitale: nelle sentenze relative al diritto all'oblio e al controllo della persona sulla propria sfera informativa online (C-131/12, *Google Spain* (2014)[25]), ai limiti invalicabili che i diritti fondamentali oppongono alle ragioni di sicurezza nazionale (C-362/14, *Schrems I* (2015); C-311/18, *Schrems II* (2020)[26]), all'incompatibilità della conservazione generalizzata dei dati con i diritti fondamentali anche in nome della sicurezza nazionale (C-511/18, C-512/18 e C-520/18, *La Quadrature du Net* (2020)[27]), all'abuso di posizione dominante delle piattaforme nel trattamento dei dati personali a fini pubblicitari (C-252/21, *Meta Platforms* (2023)[28]), al trattamento massivo di dati dei passeggeri e al principio di pro-

[23] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

[24] Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media).

[25] Su questa pronuncia v. P. de Hert - V. Papakonstantinou, *Google Spain: Addressing Critiques and Misunderstandings One Year Later*, in *Maastricht Journal of European and Comparative Law*, 2015, 624, A. Viglianisi Ferraro, *La Sentenza Google Spain ed il diritto all'oblio nello spazio giuridico* europeo, in *Contratto e Impresa. Europa*, 2015, 159, I. Spiecker genannt Döhmann, *A New Framework for Information Markets: Google Spain*, in *Common Market Law Review*, 2015, 1033, G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. Inf.*, 2014, 591.

[26] Sulle pronunce *Schrems* v., per tutti, C. Gentile, *La saga Schrems e la tutela dei diritti fondamentali*, in *federalismi.it*, 13 gennaio 2021.

[27] Su questa pronuncia v. C. Waldron, *French family welfare scoring algorithm challenged by La Quadrature du Net*, in *medialaws.eu,* 4 dicembre 2024.

[28] Su questa pronuncia v. P. Manzini, *La nuova anima costituzionale del diritto antitrust europeo*, in *rivista.eurojus.it*, 2025, 440, N. Guggenberger, *Consent as Friction*, in *Boston College Law Rev.*, 66, 2025, 353.

porzionalità (C-817/19, *Ligue des droits humains* (2022)[29]), e alla tutela contro le decisioni automatizzate (C-203/22, *Dun & Bradstreet* (2025)[30]), i giudici dell'Unione ragionano sistematicamente sulla centralità della persona come titolare di diritti azionabili nei confronti di soggetti privati dotati di potere strutturale. Ne risulta che il principio è proclamato dal legislatore e praticato dal giudice, ma non ancora formalmente giurisdizionalizzato come tale: un fondamento valoriale in via di consolidamento normativo, ma che non si è ancora tradotto in uno standard interpretativo stabilizzato.

4. La promozione della solidarietà e dell'inclusione nell'ecosistema digitale europeo

La solidarietà digitale emerge nel corpus normativo dell'Unione come valore frammentato, presidiato da strumenti eterogenei che operano con logiche diverse, senza che nessuno di essi costruisca una posizione giuridica individuale pienamente azionabile. La Dichiarazione del 2022 ne definisce il contenuto nel secondo capitolo ("Solidarietà e inclusione"), enunciando il principio secondo cui la tecnologia dovrebbe essere utilizzata per unire le persone, non per dividerle, contribuendo a una società e a un'economia eque e inclusive nell'Unione.

Il nodo concettuale del capitolo è la relazione tra digitalizzazione e disuguaglianza. La Dichiarazione del 2022 prende atto che la trasformazione digitale, abbandonata alla propria logica, tende a riprodurre e amplificare le disuguaglianze preesistenti[31]: chi ha competenze, connettività e risorse trae beneficio dal digitale; chi ne è privo ne resta escluso, subendo al contempo i costi della digitalizzazione dei servizi pubblici e del lavoro. Il principio di solidarietà digitale è, dunque, una risposta normativa a questa tendenza centrifuga, e la sua effettività dipende dalla capacità degli strumenti regolatori di tradurre un impegno politico generale in obblighi concreti e azionabili.

La traduzione normativa del principio è frammentaria, poiché siamo di fronte a tre strumenti, con logiche distinte e nessun raccordo sistemico.

---

[29] Su questa pronuncia v. E. Mendos Kuşkonmaz, *The Grand Gala of PNR Litigations: Case C-817/19, Ligue des droits humains v Conseil des ministers*, in *European Constitutional Law Review*, 19, 2023, 294, J. Gerards, *Machine learning and profiling in the PNR system*, in *VerfBlog*, 8 maggio 2023.

[30] Su questa pronuncia v. E. Pandolfi, *Il diritto alla spiegazione nei processi decisionali automatizzati e nei sistemi di intelligenza artificiale: riflessioni a margine della sentenza* Dun & Bradstreet Austria, in *rivista.eurojus.it*, 1, 2026, 269.

[31] J. van Dijk, *The Digital Divide*, Polity Press, 2020 (2a ed.), N. Couldry - U.A. Meijas, *The Costs of Connection. How Data is Colonizing Human Life and Appropriating It for Capitalism*, Stanford, 2019, J. van Dijck - T. Poell - M. de Waal, *The Platform Society*, New York, 2018.

Sul versante della connettività, il Codice europeo delle comunicazioni elettroniche ha incluso l'accesso a banda larga ad alta velocità nel servizio universale[32], integrato dal principio di neutralità della rete sancito dal regolamento (UE) 2015/2120[33] che vieta agli operatori di bloccare o degradare il traffico. Tuttavia, la piena attuazione della Bussola per il digitale 2030 resta largamente incompiuta e il divario di connettività tra aree urbane e rurali persiste come fattore strutturale di esclusione digitale. Sul versante del lavoro, la direttiva (UE) 2024/2831 sul lavoro mediante piattaforme digitali[34] ha costruito un minimo statuto protettivo (presunzione legale di subordinazione in presenza di direzione e controllo, trasparenza algoritmica, diritto di contestazione delle decisioni automatizzate, divieto di sorveglianza delle comunicazioni tra lavoratori) la cui ambizione iniziale è stata però significativamente ridotta nel corso dell'iter negoziale, particolarmente sul meccanismo della presunzione. Sul versante dei servizi pubblici digitali, il regolamento (UE) 2024/1183 (eIDAS 2.0[35]) ha istituito il Portafoglio europeo di identità digitale (EUDI Wallet), che gli Stati membri sono tenuti a rendere disponibile a tutti i cittadini e residenti dell'Unione entro la fine del 2026, garantendo il controllo esclusivo dell'individuo sulla propria identità digitale. La giustapposizione di questi tre dispositivi (connettività universale, statuto del lavoratore di piattaforma, identità digitale) non costruisce un sistema: ciascuno opera su un piano normativo proprio, con destinatari, autorità competenti e meccanismi di tutela disgiunti.

Le dimensioni più trasversali del Capitolo II, ossia la protezione delle persone vulnerabili, la lotta ai bias algoritmici, il contrasto alle discriminazioni digitali, sono trattate da più strumenti contemporaneamente. Tre strumenti convergono nella tutela dei soggetti più esposti. Il GDPR rafforza la disciplina per le categorie particolari di dati ritenute più sensibili dal considerando 51 (art. 9). Il DSA combina la valutazione dei rischi sistemici per gli utenti vulnerabili e i minori con il divieto, valevole per tutte le piattaforme, di pubblicità profilata rivolta a destinatari riconosciuti come minori. Sul

[32] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche.

[33] Regolamento (UE) 2015/2120 del parlamento europeo e del Consiglio del 25 novembre 2015 che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione.

[34] Direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali.

[35] Regolamento (UE) 2024/1183 del parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

versante della discriminazione algoritmica, l'AI Act impone ai sistemi ad alto rischio pratiche di governance dei dati che individuino e mitighino le distorsioni in grado di produrre discriminazioni vietate[36].
Il quadro complessivo presenta due limiti strutturali. Il primo è l'assenza di attuazione del principio del "*fair share*"[37]: l'impegno affinché chi trae vantaggio economico dalla trasformazione digitale contribuisca equamente ai costi delle infrastrutture che la rendono possibile è rimasto privo di effetti normativi vincolanti, risolvendosi in un cantiere politico aperto. Il secondo è la frammentazione degli strumenti, poiché la solidarietà digitale è presidiata da regolamenti e direttive che operano con logiche e finalità diverse, senza un coordinamento sistematico che garantisca la coerenza degli esiti verso i soggetti che il Capitolo II intendeva proteggere prioritariamente.
La giurisprudenza della Corte di giustizia ha affrontato la logica dell'inclusione senza nominarla come tale. I giudici hanno imposto salvaguardie specifiche contro il rischio di discriminazione indiretta nei sistemi di profilazione algoritmica, riconoscendo che la combinazione di categorie di dati apparentemente neutre può produrre effetti escludenti su gruppi protetti (C-817/19, *Ligue des droits humains* (2022)). In altre pronunce la Corte di Lussemburgo ha rafforzato la tutela individuale contro l'esclusione algoritmica dall'accesso a servizi (C-634/21, *Schufa* (2023)[38] e C-203/22, *Dun & Bradstreet* (2025)). Anche in questo ambito, dunque, il principio enunciato dalla Dichiarazione del 2022 attende di essere giurisdizionalizzato come categoria autonoma.

5. La libertà di scelta sostanziale

Nel sistema della Dichiarazione del 2022 la libertà di scelta non designa la mera assenza di coercizione formale, ma la capacità effettiva dell'utente di orientare le proprie decisioni in un ambiente online strutturalmente asimmetrico. Essa è costruita nell'ordinamento digitale europeo attraverso tecniche regolatorie eterogenee: obblighi di trasparenza, divieti di manipo-

[36] Si vedano, rispettivamente, l'art. 9 GDPR e il considerando 51 del medesimo regolamento; gli artt. 28, par. 2, 34 e 35 DSA; l'art. 10, parr. 2-3, AI Act, che richiede ai set di dati di addestramento, convalida e prova proprietà statistiche appropriate rispetto ai gruppi di persone cui il sistema è destinato.

[37] In argomento v. Z. Warso, *The Limits of The Fair Share Debate*, Open_Future, 6 aprile 2023.

[38] Su questa pronuncia v. F. Mattasoglio, *La Corte di giustizia europea, algoritmi e credit scoring. L'apertura del vaso di Pandora delle società che si "limitano" a elaborare gli scoring*, in *Dialoghi di Diritto dell'Economia*, gennaio 2025, F. D'Orazio, *Il credit scoring e l'art. 22 del GDPR al vaglio della Corte di giustizia*, in *Nuova Giur. Comm.*, 2, 2024, 416, A.G. Grasso, *Decisioni automatizzate e merito creditizio: la Corte di giustizia sulcredit-scoring*, in *BBTC*, 2024, 715.

lazione, diritti di portabilità, requisiti strutturali di contendibilità. Il nodo concettuale del terzo capitolo della Dichiarazione ("Libertà di scelta") è la distinzione tra libertà di scelta formale e libertà di scelta sostanziale. Che ogni utente sia formalmente libero di scegliere quale servizio utilizzare è una verità superficiale nell'ambiente online, ma resta il problema è che questa libertà formale è sistematicamente svuotata dalla struttura stessa dell'ambiente digitale, da architetture di interfacce progettate per condizionare le decisioni, da sistemi di raccomandazione che orientano le scelte senza che l'utente ne sia consapevole, da effetti di lock-in che rendono il cambio di servizio costoso o impraticabile, da asimmetrie informative che rendono impossibile un confronto genuino tra alternative[39].

La libertà di scelta sostanziale è costruita dal diritto dell'Unione per sottrazione, non per addizione, attraverso divieti di manipolazione, obblighi di trasparenza, diritti di portabilità, ma non strutture positive che garantiscano l'esistenza di alternative effettivamente praticabili. Cinque atti convergono in questa logica con modalità complementari ma con un baricentro comune.

Il GDPR presidia la dimensione consensuale, esigendo che il consenso al trattamento sia libero, specifico, informato e inequivocabile (art. 4, n. 11)[40] e ritenendolo viziato quando intervenga un significativo squilibrio di potere tra l'interessato e il titolare del trattamento (considerando 43). La portata pratica di questa garanzia è tuttavia ridimensionata dalla circostanza, ormai strutturale, che il consenso al trattamento dei dati personali costituisce frequentemente il presupposto per accedere a servizi o beni digitali[41]; consenso che gli utenti pressoché mai negano. Sempre il GDPR, sul versante positivo, riconosce il diritto alla portabilità dei dati (art. 20), che risulta essere strumento concorrenziale tra i pochi a logica abilitante, poiché trasferisce i dati da un titolare all'altro in formato interoperabile, abbassando le barriere al cambio di servizio.

DSA e DMA operano sulle architetture di scelta. L'art. 25 DSA introduce nel diritto dell'Unione il divieto esplicito di dark patterns, prescrivendo che le interfacce online non siano progettate o gestite in modo da «materialmente falsare o compromettere la capacità dei destinatari del servizio

[39] In argomento v. D. Susser - B. Roessler - H.F. Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, in *Georgetown Law Technology Review*, 4(1), 2019.

[40] Da ultimo, sulle caratteristiche del valido consenso v. S. Thobani, *Il consenso nella regolazione della circolazione dei dati*, in *Persona e Mercato*, 2, 2025, 469, A.S. D'Amico, *Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be* Freely Given?*,* in *European Papers*, 8(2), 2023, 611.

[41] In argomento v. European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platform*, 17 aprile 2024, P. Gallo, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. Dir. Civ.*, 6, 2022, 1054.

di prendere decisioni libere e informate[42]». Il DMA estende il divieto ai mercati dominati dai gatekeeper (art. 13, par. 6) e ne completa il presidio con strumenti strutturali (portabilità in tempo reale e interoperabilità (artt. 6 e 7)) che abbattono direttamente le barriere al cambio di servizio. Per i sistemi di raccomandazione, il DSA impone alle piattaforme di dimensioni molto grandi di offrire almeno un'opzione non basata sulla profilazione (art. 38).

Sul piano infrastrutturale, il Data Act[43] estende la logica della portabilità ai dati industriali e ai servizi cloud, disciplinando il processo di passaggio tra fornitori in modo tale da neutralizzare gli effetti di lock-in[44]. Infine, l'AI Act presidia la libertà di scelta sul versante delle tecniche manipolative: vieta i sistemi che alterano il comportamento delle persone tramite tecniche subliminali (art. 5)[45] e impone obblighi di trasparenza nei confronti di chi interagisce direttamente con un sistema di IA (art. 50)[46].

Il filo che attraversa l'intero capitolo è già visibile nella geometria delle disposizioni richiamate: la libertà di scelta è tutelata prevalentemente per via negativa, attraverso divieti e trasparenza, piuttosto che per via positiva, attraverso costruzione di alternative reali.

La Corte di giustizia ha affrontato i temi della libertà di scelta con crescente nitidezza, senza tuttavia mai elevarla a categoria autonoma. In *Meta Platforms* (C-252/21, 2023), i giudici europei hanno affermato che l'estensione e la pervasività del trattamento dei dati a fini pubblicitari operato da Meta eccede la ragionevole aspettativa degli utenti e non può essere giustificata da un legittimo interesse. In *Schufa* (C-634/21, 2023) e *Dun & Bradstreet* (C-203/22, 2025) i giudici europei hanno riconosciuto che una persona il cui accesso a servizi sia negato sulla base di una valutazione algoritmica

---

[42] A. Scaffidi - V. Forte, *Dai* dark Patterns *agli* Hyper-Engaging Dark Patterns*: per un'applicazione moderna del divieto ex art. 25 DSA, in* questa *Rivista*, 2, 2025, 431, O. Salvatore, *A proposito dei* deceptive design (*già* dark) patterns, in G. Grisi – S. Tommasi (a cura di), *Mercato digitale e tutela dei consumatori. Prove di futuro*, Torino, 2024, 63, G. Guerra, *Redesigning Protection for Consumer Autonomy. The case-study of* dark patterns *in European private law*, Milano, 2023.

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

[44] Il diritto al passaggio è garantito dall'art. 25 Data Act, che impone ai fornitori di assicurare l'equivalenza funzionale e la disponibilità dei dati esportabili; l'art. 29 dispone l'abolizione progressiva delle tariffe di passaggio, con eliminazione completa a decorrere dal 2027.

[45] In argomento v. C. Solinas, *Sistemi di IA e tecniche subliminali, manipolative o ingannevoli. Il perimetro del divieto dell'*AI ACT, in *Contratto e impresa*, 4, 2025, 1018.

[46] In argomento A. Amidei, *La tutela del consumatore "profilato": obblighi informativi e asimmetrie negoziali*, in *Giur. it.*, febbraio 2025, 461.

opaca non è in condizione di esercitare una scelta informata, né di contestare efficacemente la decisione, e ha imposto ai titolari del trattamento di fornire spiegazioni significative sulla logica dell'automatismo decisionale in forma concisa e intellegibile.
Il quadro che emerge presenta una caratteristica rilevante: la libertà di scelta è tutelata dalla regolazione dell'ecosistema digitale europeo prevalentemente attraverso obblighi di trasparenza e divieti di manipolazione, piuttosto che attraverso diritti positivi di accesso a alternative effettivamente praticabili. Questo approccio rischia di rivelarsi insufficiente in mercati in cui l'alternativa al servizio dominante non esiste o non è accessibile: la trasparenza su come funziona un algoritmo non restituisce libertà di scelta a chi non ha alternative reali. La tensione tra libertà di scelta come diritto individuale e libertà di scelta come condizione strutturale di mercato è il limite che attraversa l'intero Capitolo III della Dichiarazione del 2022.

6. La partecipazione allo spazio pubblico digitale

La partecipazione digitale può a buon titolo collocarsi fra i luoghi di massimo conflitto tra diritti nell'intero corpus normativo europeo: libertà di espressione, tutela del pluralismo e contrasto alla disinformazione si fronteggiano senza che nessuno dei tre valori possa prevalere senza condizionare gli altri. Il quarto capitolo della Dichiarazione ("Partecipazione allo spazio pubblico digitale") ne affronta la dimensione più schiettamente democratica, affermando che ogni persona dovrebbe avere accesso a un ambiente digitale affidabile, diversificato e multilingue; ogni persona ha diritto alla libertà di espressione e di informazione nell'ambiente digitale; le piattaforme online di dimensioni molto grandi dovrebbero sostenere il libero dibattito democratico, attenuare i rischi di disinformazione e tutelare la libertà di espressione.
Il DSA è lo strumento che più direttamente configura gli impegni del quarto capitolo. La sua impostazione normativa riflette consapevolmente la tensione fondamentale, poichè vieta obblighi generali di sorveglianza dei contenuti (art. 8) e tutela la libertà di espressione, garantendo che le decisioni di moderazione siano motivate e contestabili (artt. 16 e 20). Al tempo stesso, impone alle piattaforme di dimensioni molto grandi obblighi stringenti di valutazione e mitigazione dei rischi sistemici per i diritti fondamentali (artt. 34-35), articolati lungo quattro direttrici: contenuti illegali, diritti fondamentali, integrità del dibattito civico e dei processi elettorali, salute pubblica e benessere dei minori[47]. La logica è quella di responsabi-

[47] L'art. 34, par. 1, DSA individua quattro categorie di rischi sistemici che le piattaforme di dimensioni molto grandi devono valutare: diffusione di contenuti illegali (lett. a); effetti

lizzare le piattaforme per gli effetti sistemici dei loro servizi senza imporre censure preventive sui singoli contenuti.
Sul versante specifico della trasparenza dei sistemi di raccomandazione, il DSA impone a tutte le piattaforme online che vi ricorrono di pubblicare nelle proprie condizioni generali i parametri principali che determinano l'ordine di presentazione dei contenuti e le ragioni della loro importanza relativa (art. 27). Le piattaforme di dimensioni molto grandi sono inoltre tenute a offrire agli utenti almeno un'opzione di sistema non basata sulla profilazione (art. 38). Sullo sfondo di questa architettura normativa emerge una trasformazione qualitativa che il diritto fatica ancora a qualificare e regolare con precisione: le piattaforme di dimensioni molto grandi hanno cessato di essere meri intermediari privati per diventare infrastrutture quasi-pubbliche del discorso democratico[48]. Esse definiscono le condizioni di visibilità dell'informazione, le regole di accesso allo spazio pubblico digitale, i criteri di moderazione del dibattito collettivo, ossia funzioni che nell'ambiente analogico erano proprie delle istituzioni pubbliche o dei media soggetti a obblighi di servizio pubblico. Questa trasformazione è il presupposto implicito del DSA e dell'EMFA, venendo a costituire il fondamento teorico su cui poggia l'intera architettura regolatoria della partecipazione digitale.
Va preso atto che l'accesso alle condizioni di visibilità dell'informazione sono definite unilateralmente da soggetti privati attraverso sistemi algoritmici opachi e incide direttamente sulla qualità dell'appartenenza democratica all'Unione. Chi non raggiunge visibilità nello spazio pubblico digitale è di fatto marginalizzato da quella sfera di partecipazione che le democrazie contemporanee non possono più distinguere dallo spazio pubblico tout court. È su questo piano che la regolazione delle piattaforme cessa di essere materia di diritto del mercato interno e diviene, irrimediabilmente, materia avente un rilievo costituzionale.
L'EMFA interviene nella dimensione istituzionale del quarto capitolo: la libertà e il pluralismo dei media come condizioni costitutive di una democrazia funzionante. Il considerando 2 qualifica la tutela di questi valori come «aspetto essenziale per il buon funzionamento del mercato interno dei servizi di media», riconoscendo in essi pilastri della democrazia e dello Stato di diritto. Il regolamento agisce su tre piani principali: protegge l'indipendenza editoriale dei fornitori di servizi di media da pressioni esterne e governative (artt. 4 e 6); impone la trasparenza sulla struttura proprieta-

negativi sull'esercizio dei diritti fondamentali, inclusi libertà di espressione e pluralismo dei media (lett. b); effetti negativi sul dibattito civico e sui processi elettorali (lett. c); rischi per la salute pubblica, la protezione dei minori e il benessere fisico e mentale della persona (lett. d).

[48] V. J.M. Balkin, *Free Speech is a Triangle*, in *Columbia Law Review*, 118(7), 2018, 2011.

ria (art. 6, par. 2); disciplina le concentrazioni con impatto significativo sul pluralismo (art. 22).

La relazione tra l'EMFA e il DSA è di complementarità funzionale, poiché il DSA regola le condizioni di distribuzione dei contenuti nelle piattaforme, mentre l'EMFA garantisce le condizioni di produzione e indipendenza dei contenuti giornalistici. Il rischio di lacune normative si colloca nell'intersezione tra i due regolamenti, dove i fornitori di servizi di media accedono agli utenti prevalentemente attraverso le piattaforme soggette al DSA, esponendosi agli effetti dei loro sistemi algoritmici di distribuzione senza che nessuno dei due strumenti affronti compiutamente questa dipendenza di fatto.

La Corte di giustizia ha costruito nel corso di un decennio un corpus coerente in materia di partecipazione al discorso pubblico digitale, articolato attorno al bilanciamento tra libertà di espressione e protezione dei diritti fondamentali. Il filone inaugurato da *Google Spain* (C-131/12 (2014)) ha affermato il diritto alla deindicizzazione come espressione del diritto alla protezione dei dati personali, avviando una giurisprudenza sul bilanciamento tra diritto all'oblio e diritto del pubblico all'informazione che si è consolidata in *Google v. CNIL* (C-507/17 (2019)[49]) e *Google (de-referencing of allegedly inaccurate content*) (C-460/20 (2022)[50]). Sul versante della moderazione dei contenuti, *Glawischnig-Piesczek v. Facebook Ireland* (C-18/18 (2019)[51]) ha stabilito che un giudice nazionale può ordinare la rimozione non solo del contenuto dichiarato illecito, ma anche di contenuti identici ed equivalenti, aprendo un problema di compatibilità con il divieto di obbligo generale di sorveglianza che il DSA ha poi tentato di comporre sul piano legislativo. In *Schrems v. Meta Platforms Ireland* (C-446/21 (2024)[52]), i giudici della Corte di giustizia hanno affermato che il consenso non giustifica il trattamento illimitato di dati personali a fini pubblicitari, incidendo direttamente sulla struttura economica delle piattaforme che finanziano il

---

[49] Su questa pronuncia v. F. Balducci Romano, *La Corte di giustizia 'resetta' il diritto all'oblio*, in *federalismi.it*, 5 febbraio 2020.

[50] Su questa pronuncia v. E. Falletti, *La proiezione della personalità online: quale rapporto tra diritto all'oblio e diffamazione?*, in *Foro it.*, 4, 2023, 188, E. Grillo, *Effettività del diritto alla deindicizzazione: informazioni inesatte e valore informativo delle immagini "*thumbnails*"*, in *NGCC*, 3, 2023, 546.

[51] Su questa pronuncia v. A. Ricci, *Contenuti illeciti e obblighi «di reazione» del prestatore di servizi di* hosting. *La Corte di Giustizia interpreta la direttiva 2000/31/CE alla luce del principio di effettività*, in *Giur. comm.*, II, 2020, 1018.

[52] Su questa pronuncia v. J.A. Cruz, *Schrems v. facebook: Limitations on the Use of Off-Platform Data and Sensitive Personal Data*, in *medialaws.eu,* 28 novembre 2024, O. Pollicino - M. Bassini, *Bridge is Down, Data Truck Can't Get Through…A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, in *The Global Community. Yearbook of International Law and Jurisprudence 2016*, 2017, 254.

discorso pubblico digitale attraverso la profilazione pubblicitaria.
Dalla tensione che attraversa l'intero Capitolo IV appare che il modello europeo ha scelto di affrontare i rischi per la democrazia digitale attraverso la responsabilizzazione delle piattaforme e la trasparenza algoritmica, piuttosto che attraverso la regolazione diretta dei contenuti. Questa scelta preserva la libertà di espressione e il divieto di censura preventiva, ma la sua effettività dipende dalla capacità delle piattaforme di valutare genuinamente i rischi sistemici e di mitigarli senza che la mitigazione si traduca a propria volta in forme di controllo privatizzato del discorso pubblico.

7. La sicurezza e la protezione delle persone

La sicurezza è il valore più giurisdizionalizzato dell'intero sistema: nessun altro capitolo della Dichiarazione del 2022 può contare su un corpus giurisprudenziale della Corte di giustizia altrettanto consolidato nel tempo, né su strumenti normativi altrettanto verificati nella prassi applicativa. Il quinto capitolo della Dichiarazione ("Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità") si articola in tre sottosezioni: la sicurezza tecnica di prodotti e infrastrutture; la vita privata e il controllo individuale sui dati; la protezione di bambini e giovani.
Il nodo concettuale del capitolo è la tensione tra sicurezza come valore collettivo (che può giustificare limitazioni alla vita privata in nome della protezione pubblica) e sicurezza come difesa della sfera individuale contro le intrusioni tanto degli attori privati quanto degli Stati. Questa tensione, già presente nella tradizione giuridica europea, si manifesta nel contesto digitale in forme nuove e più acute: la raccolta massiva di dati da parte delle piattaforme[53], la sorveglianza di massa da parte dei governi[54], il tracciamento pervasivo a fini commerciali[55], l'utilizzo dell'intelligenza artificiale per identificare, classificare e valutare le persone[56], sono tutti fenomeni che il Capitolo V intende presidiare.
A differenza degli altri valori, la sicurezza è tutelata nel modello europeo in chiave eminentemente infrastrutturale: non per via di diritti soggettivi

[53] Su questo tema restano centrali le riflessioni di S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019, S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, S. Rodotà, *Tecnologie e diritti*, Bologna, 1995.

[54] V. D. Lyon, *Surveillance After Snowden*, Cambridge, 2015.

[55] V. D. Lyon, *Surveillance Society: Monitoring Everyday Life*, Buckingham, 2001.

[56] O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constiutionalism?*, Oxford, 2022, F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (MA), 2015.

azionabili, ma per via di requisiti tecnici imposti a chi progetta sistemi e prodotti. Il GDPR ne è la matrice, con il principio di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25) e con l'obbligo generale di sicurezza del trattamento (art. 32, che impone misure adeguate a garantire riservatezza, integrità, disponibilità e resilienza dei sistemi). Su questo asse si innestano due strumenti di portata più ampia: la Direttiva NIS2 (direttiva (UE) 2022/2555)[57], che eleva i requisiti di cybersicurezza per le infrastrutture critiche e i servizi essenziali, estendendo l'ambito di applicazione a diciotto settori, e il Cyber Resilience Act (regolamento (UE) 2024/2847)[58], che trasferisce la responsabilità della sicurezza dal consumatore al fabbricante, imponendo requisiti obbligatori per tutti i prodotti con elementi digitali immessi sul mercato dell'Unione. Con coerenza logica la sicurezza è protetta non tanto attribuendo poteri agli utenti, quanto vincolando ex ante chi produce e gestisce le infrastrutture su cui gli utenti operano. È una scelta regolatoria che attribuisce al valore una densità giuridica peculiare, fatta di obblighi tecnici verificabili più che di posizioni soggettive azionabili.

Se, sul generale versante della vita privata, il GDPR costituisce l'asse portante della tutela, il diritto alla riservatezza delle comunicazioni elettroniche trova disciplina specifica nella Direttiva ePrivacy (direttiva 2002/58/CE[59]), che protegge la riservatezza delle comunicazioni e dei relativi metadati[60], vieta il tracciamento non autorizzato e subordina l'accesso alle informazioni archiviate sui dispositivi terminali degli utenti al consenso dell'interessato, fondamento giuridico che governa, tra l'altro, la disciplina dei cookie. La riforma di questo strumento è da anni bloccata in sede legislativa: la proposta della Commissione del 2017 prevedeva la sostituzione della direttiva con un regolamento direttamente applicabile, che

[57] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2).

[58] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).

[59] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[60] V. M. Orofino, *La tutela dei dati personali nelle comunicazioni elettroniche: dalla direttiva e-Privacy alla crisi del modello e-Privacy*, in G. De Minico – M. Orofino (a cura di), *Regole telecomunicazioni dati nell'Europa* digitale, Napoli, 2025, 31, F.J. Zuiderveen Borgesius - W. Steenbruggen, *The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust*, in *Theoretical Inquiries in Law*, 19, 2019, 291.

avrebbe garantito uniformità applicativa e piena coerenza sistematica con il GDPR[61]. Tuttavia, il negoziato interistituzionale non ha ancora prodotto un testo definitivo. Sul piano delle fonti, la tutela della confidenzialità delle comunicazioni elettroniche che si fonda sulla Direttiva ePrivacy è oggi destinata a operare come *lex specialis* rispetto al GDPR, secondo una logica espressamente confermata dalla proposta di regolamento ePrivacy del 2017 (che ribadisce che tale disciplina «*particularise and complement*» il GDPR in materia di comunicazioni elettroniche). Si può osservare che la protezione della segretezza delle comunicazioni non tutela soltanto la sfera individuale della privacy, ma anche valori collettivi quali la libertà di espressione e, soprattutto, la *trust in communication services*, ossia la possibilità per individui e organizzazioni di affidare in sicurezza le proprie interazioni ai fornitori di servizi digitali. In questa prospettiva, la disciplina ePrivacy assume una funzione di rilievo costituzionale ulteriore rispetto al GDPR: non solo protezione del dato personale, ma presidio della fiducia infrastrutturale che rende possibile l'esercizio dei diritti della persona nello spazio comunicativo europeo.

Sul fronte dell'eredità digitale[62], ossia il diritto di determinare cosa accada ai propri account e alle proprie informazioni dopo la morte, enunciato al punto 19 del Capitolo V, l'Unione non dispone ancora di uno strumento normativo armonizzato.

Per quanto concerne la protezione di bambini e giovani, l'AI Act vieta i sistemi di IA che sfruttano le vulnerabilità di una persona fisica dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il suo comportamento in modo da provocarle un danno significativo (art. 5, par. 1, lett. b)). Il DSA, come già visto, vieta alle piattaforme online di presentare inserzioni pubblicitarie basate sulla profilazione quando siano ragionevolmente consapevoli che il destinatario è minore (art. 28, par. 2) e impone loro di adottare misure adeguate e proporzionate per proteggere i minori, anche progettando le interfacce con il massimo livello di privacy e sicurezza per

[61] La proposta (COM(2017) 10 final) è stata presentata dalla Commissione europea il 10 gennaio 2017, con il titolo "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)". Sulla proposta v. F.J. Zuiderveen Borgesius - J. van Hoboken - R. Fahy - K. Irion - M. Rozendaal, *An assessment of the Commision's Proposal on Privacy and Electronic Communications*, Study for the LOBE Committee, 2017.

[62] In argomento v. V. Confortini, *Persona e patrimonio nella successione digitale*, Torino, 2023, F. Bartolini - F.P. Patti, *Digital Inheritance and* Post Mortem*Data Protection: The Italian Reform*, in *European Review of Private Law*, 27(5), 2019, 118, E. Harbinja, *Does the Eu data protection regime protect post-mortem privacy and what could be the potential alternatives?*, in *Scripted*, 10, 1, aprile 2013.

impostazione predefinita (art. 28, par. 1, e considerando 71).
Come accennato, il corpus giurisprudenziale della Corte di giustizia in materia di sicurezza è il più ricco e consolidato tra tutti i capitoli della Dichiarazione. Il filone sulla riservatezza delle comunicazioni e il divieto di sorveglianza di massa si sviluppa da *Digital Rights Ireland* (C-293/12 e C-594/12 (2014)), in cui la Corte ha invalidato la Direttiva sulla conservazione dei dati, a *Tele2 Sverige e Watson* (C-203/15 e C-698/15 (2016)), dove i giudici hanno affermato che la conservazione generalizzata e indifferenziata dei dati di traffico è incompatibile con il diritto dell'Unione. *La Quadrature du Net* (C-511/18, C-512/18 e C-520/18 (2020)) ha segnato un passaggio ulteriore, estendendo l'applicabilità della direttiva 2002/58/CE alle misure nazionali adottate per finalità di sicurezza nazionale e respingendo in tal modo l'argomento degli Stati membri secondo cui tali misure esulerebbero dall'ambito del diritto dell'Unione. La Corte ha confermato il divieto di conservazione generalizzata e indifferenziata dei dati di traffico e localizzazione, ammettendo tuttavia che una minaccia grave, reale e attuale o prevedibile alla sicurezza nazionale possa giustificare un obbligo temporaneo di conservazione generale, purché sottoposto a controllo effettivo da parte di un giudice o di un'autorità amministrativa indipendente. La pronuncia ha inoltre fissato garanzie specifiche per l'analisi automatizzata dei dati, anticipando sul piano giurisprudenziale la logica di sorveglianza algoritmica controllata che il legislatore avrebbe successivamente codificato nell'AI Act. In *H.K. c. Prokuratuur* (C-746/18 (2021)) la Corte ha poi ribadito che l'accesso alle comunicazioni elettroniche da parte delle autorità pubbliche deve essere limitato, nel rispetto del principio di proporzionalità, alla lotta contro forme gravi di criminalità. Il filone sui trasferimenti internazionali dei dati è ben presidiato da Schrems I (C-362/14 (2015)) e Schrems II (C-311/18 (2020)), in cui la Corte di giustizia hanno rispettivamente invalidato il Safe Harbor e il Privacy Shield[63]. Elaborata progressivamente lungo entrambi i filoni appare oramai consolidata la valutazione che una normativa che consenta alle autorità pubbliche di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche compromette l'essenza stessa del diritto garantito dall'art. 7 della Carta dei diritti fondamentali dell'Unione e costituisce oggi il riferimento costituzionale per la valutazione di qualsiasi regime di sorveglianza.
Il limite principale del Capitolo V rimane la tenuta dell'equilibrio tra sicurezza collettiva e libertà individuale. Le pressioni degli Stati membri per ampliare le capacità di accesso ai dati in nome della sicurezza pubblica

[63] In argomento, da ultimo, G. Proietti, *Tutela e valorizzazione dei dati nei mercati digitali. Il contratto, la concorrenza e i nuovi soggetti* tutelati, Milano, 2025, spec. cap. II, 89 e ss., A. Busacca, *Trasferimento dei dati personali UE-USA novità e criticità del* data primacy framework, in *federalismi.it*, 18 dicembre 2024.

(accentuate dal mutato contesto geopolitico successivo al febbraio 2022) continuano a mettere sotto tensione i confini tracciati dalla Corte di giustizia. Il caso più emblematico è il travagliato iter del regolamento sulla prevenzione degli abusi sessuali su minori online (noto come "Chat Control"[64]). L'EDPB e l'EDPS hanno congiuntamente segnalato che l'obbligo generalizzato di scansione delle comunicazioni private avrebbe configurato una forma di sorveglianza di massa incompatibile con la giurisprudenza della Corte[65]. Il Consiglio ha adottato nel novembre 2025 una posizione negoziale che eliminava l'obbligo generalizzato di scansione, mantenendo però un regime favorevole alla sorveglianza volontaria, siché il trilogo è infine fallito nel marzo 2026 e il Parlamento europeo ha respinto anche la proroga del regime transitorio. Ne consegue che le piattaforme non possono più effettuare scansioni di massa dei messaggi privati, mentre i negoziati per un regolamento permanente restano aperti.

8. La sostenibilità ambientale e intergenerazionale

La sostenibilità ambientale e intergenerazionale resta il valore meno sviluppato e più programmatico dell'intera Dichiarazione del 2022: nessun altro capitolo presenta uno scarto altrettanto ampio tra l'ambizione valoriale proclamata e la densità giuridica degli strumenti che ne assicurano l'effettività. Il sesto capitolo della Dichiarazione ("Sostenibilità") si articola in due enunciati fondamentali: i prodotti e i servizi digitali dovrebbero essere progettati, prodotti, utilizzati, riparati, riciclati e smaltiti in modo da attenuare il loro impatto negativo sull'ambiente. Vieppiù, ogni persona ha diritto ad accedere a informazioni precise sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, «in modo da essere in grado di compiere scelte responsabili». Quest'ultimo enunciato incorpora implicitamente una dimensione intergenerazionale: il diritto all'informazione responsabile non tutela soltanto il consumatore presente, ma opera come argine contro il trasferimento sistematico dei costi ecologici della trasformazione digitale sulle generazioni future, alle quali verrebbero altrimenti consegnate le esternalità ambientali di scelte compiute oggi in condizioni di opacità informativa.

[64] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori, COM(2022) 209 final, 11 maggio 2022. Sulla proposta di regolamento v. EPRS, *Proposal for a regulation laying down rules to prevent and combat child sexual abuse. Complementary impact assessment*, April 2023. In argomento v. R. Anderson, *Chat Control or Child Protection?*, 2022.

[65] EDPB e EDPS, *Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, 28 luglio 2022.

La contraddizione strutturale tra transizione digitale e transizione verde non è all'evidenza risolvibile per via normativa in tempi brevi. La digitalizzazione dell'economia è stata presentata come leva della decarbonizzazione, ma richiede essa stessa infrastrutture ad alto consumo energetico (data center, reti 5G, sistemi di addestramento per l'intelligenza artificiale generativa) la cui impronta ambientale è in rapida crescita[66], in una maniera difficilmente compatibile con gli obiettivi climatici dell'Unione per come definiti dal regolamento (UE) 2021/1119[67]. A questa tensione se ne sovrappone una seconda, di natura geopolitica: la sovranità digitale europea passa in misura crescente per la capacità computazionale autonoma, che richiede infrastrutture energivore localizzate nel territorio dell'Unione. Il perseguimento dell'autonomia strategica nel settore dell'IA e del cloud rischia così di entrare in conflitto diretto con gli impegni climatici, esponendo il modello europeo a una contraddizione interna che gli strumenti normativi adottati non hanno ancora affrontato in modo sistematico.
Il Regolamento Ecodesign per Prodotti Sostenibili (regolamento (UE) 2024/1781[68]) è lo strumento che più direttamente risponde agli impegni del Capitolo VI: estende i requisiti di progettazione ecocompatibile a quasi tutti i prodotti immessi sul mercato europeo e introduce il passaporto digitale di prodotto, uno strumento elettronico che rende accessibili le informazioni sulla sostenibilità ambientale del prodotto lungo l'intero ciclo di vita, inclusa la sua impronta di carbonio, le capacità di riparazione e le modalità di smaltimento. Il Data Act concorre su un piano diverso, in quanto il suo considerando 15 riconosce espressamente che i dati provenienti da prodotti connessi sono strumento per «tutelare l'ambiente, la salute e l'economia circolare, anche agevolando la manutenzione e la riparazione dei prodotti connessi», orientando in chiave ambientale la ratio dell'accesso ai dati disciplinato dal Capo II. L'AI Act affronta la dimensione energetica dell'intelligenza artificiale imponendo ai fornitori di modelli per finalità generali di includere nella documentazione tecnica «il consumo energetico noto o stimato del modello»[69], introducendo una misura di trasparenza che, per la prima volta, rende visibile su scala sistemica

[66] V. OECD, *Measuring the environmental impacts of artificial intelligence compute and applications*, OECD Digital economy papers, n. 341, November 2022.

[67] Regolamento (UE) 2021/1119 del Parlamento europeo e del Consiglio del 30 giugno2021 che istituisce il quadro per il conseguimento della neutralità climatica e che modifica il regolamento (CE) n. 401/2009 e il regolamento (UE) 2018/1999 ("Normativa europea sul clima").

[68] Regolamento (UE) 2024/1781 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili, modifica la direttiva (UE) 2020/1828 e il regolamento (UE) 2023/1542 e abroga la direttiva 2009/125/CE.

[69] Allegato XI, punto 2, lett. e), richiamato dall'art. 53, par. 1, lett. a.

l'impronta ambientale dei sistemi di IA. La Direttiva *Empowering Consumers for the Green Transition* (direttiva (UE) 2024/825[70]) chiude il quadro introducendo nel regime delle pratiche commerciali sleali un divieto esplicito delle asserzioni ambientali ingannevoli: il collegamento con il Capitolo VI della Dichiarazione è diretto, poiché il diritto a informazioni precise sull'impatto ambientale dei prodotti digitali perde sostanza se le comunicazioni commerciali che veicolano tali informazioni possono essere costruite su affermazioni non verificate.
La Corte di giustizia non ha ancora sviluppato un corpus di pronunce specificamente dedicato alla sostenibilità dell'ecosistema digitale.
Il Capitolo VI della Dichiarazione è quello che misura con maggiore nitidezza la tenuta del modello europeo. Non si tratta di accertare la semplice coerenza tra valori proclamati e norme adottate, ma di verificare la compatibilità tra le ambizioni regolatorie sulla sostenibilità digitale e le scelte di governance tecnologica compiute in nome dell'autonomia strategica, che si muovono in direzioni opposte. La crescita dei consumi energetici legati all'IA generativa, al cloud computing e ai data center procede a ritmo nettamente superiore agli incrementi di efficienza prodotti dagli strumenti normativi vigenti. Colmare questo scarto è la condizione minima perché i valori del Capitolo VI non restino enunciazione programmatica.

9. Conclusioni: un antropocentrismo prevalentemente reattivo

Tutto quanto sopra illustrato, quale prima conclusione si può ragionevolmente ritenere che il modello europeo di regolazione dell'ecosistema digitale online abbia raggiunto una maturità sufficiente per essere valutato non più soltanto nei suoi strumenti, ma nella sua capacità di tradurre in obblighi concretamente esigibili e giurisdizionalmente effettivi i principi enunciati dalla Dichiarazione del 2022.
Tale valutazione risulta in un bilancio differenziato, poiché l'architettura regolatoria europea non ha tradotto con uguale intensità i valori della Dichiarazione del 2022.
La giurisdizionalizzazione procede in modo asimmetrico: è densa e consolidata per la sicurezza e la vita privata, mentre si assottiglia progressivamente per la libertà di scelta, la solidarietà e l'inclusione, la partecipazione al discorso pubblico, fino al limite estremo della sostenibilità ambientale,

[70] Direttiva (UE) 2024/825 del Parlamento europeo e del Consiglio, del 28 febbraio 2024, che modifica le direttive 2005/29/CE e 2011/83/UE per quanto riguarda la responsabilizzazione dei consumatori per la transizione verde mediante il miglioramento della tutela dalle pratiche sleali e dell'informazione.

per la quale la giurisprudenza della Corte è ancora del tutto embrionale. Questa asimmetria non è casuale, ma riflette la sequenza storica con cui i valori sono stati incorporati nel diritto dell'Unione. Il diritto alla vita privata e alla protezione dei dati aveva già trovato costituzionalizzazione negli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (su un fondamento normativo che affondava le radici nella direttiva 95/46/CE) quando la regolazione digitale online specifica ha cominciato a prendere forma come corpus autonomo. La sostenibilità ambientale dell'ecosistema digitale online, viceversa, è una categoria costruita *ex novo* dalla Dichiarazione del 2022, senza retroterra giurisprudenziale su cui fare leva. Il deficit più rilevante è tuttavia di ordine qualitativo. Il modello europeo appare aver privilegiato una declinazione prevalentemente difensiva dei valori proclamati, tutelando la persona dai rischi della tecnologia più di quanto la metta nelle condizioni di appropriarsi dei suoi benefici: un antropocentrismo reattivo più che promozionale, capace di proteggere, ma non ancora di emancipare. La Dichiarazione del 2022 parla di persone «nelle condizioni di perseguire le loro aspirazioni»: questa formulazione presuppone non solo l'assenza di ostacoli, ma la presenza attiva di risorse. Le competenze digitali, le interfacce accessibili, la distribuzione equa del potere informativo sono state garantite in modo disomogeneo, lasciando aperta la dimensione positiva dell'antropocentrismo: quella che non si esaurisce nella protezione, ma richiede abilitazione.

Un secondo piano di analisi riguarda il rapporto tra la Dichiarazione del 2022 e la giurisprudenza della Corte di giustizia. La logica dei valori della Dichiarazione del 2022 percorre sotterraneamente le pronunce della Corte, ma essa non compare come canone interpretativo esplicito in alcuna pronuncia: i suoi valori sono applicati senza essere nominati. Lo spazio tra il diritto proclamato e il diritto giurisdizionalizzato è ancora aperto, ed è su questo spazio che si misura la portata del costituzionalismo digitale europeo, inteso anzitutto come tentativo di estendere i vincoli valoriali del diritto costituzionale anche ai poteri privati che governano l'ecosistema digitale[71]. La Dichiarazione del 2022 si candida a divenire centrale documento assiologico del costituzionalismo digitale europeo, poiché ne esprime i valori fondativi, può orientare la produzione normativa e ne offre il parametro di coerenza interna. Il passaggio dalla candidatura alla piena operatività giuridica dipende da una condizione ancora non avverata: che la Corte di giustizia la incorpori come canone ermeneutico esplicito, com-

[71] Sul costituzionalismo digitale europeo v. G. De Gregorio - O. Pollicino - P. Valcke (eds.), *The Oxford Handbook of Digital Constitutionalism*, Oxford, 2024; G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road towards Digital Constitutionalism?*, Oxford, 2021; E. Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, in *International Review of Law, Computer and Technology*, 33, 2019, 79.

piendo per la Dichiarazione del 2022 percorso analogo a quello che la giurisprudenza europea (ma anche nazionale) ha già compiuto per la Carta dei diritti fondamentali dell'Unione europea. Quel percorso ha una storia nota: in *Mangold* (C-144/04 (2005)) la Corte ha ricavato per la prima volta un principio generale (il divieto di discriminazione in ragione dell'età) dalle tradizioni costituzionali comuni e da strumenti di diritto derivato non ancora in vigore, affermandone l'efficacia orizzontale diretta in assenza di un esplicito fondamento nei Trattati. In *Kücükdeveci* (C-555/07 (2010)) quella costruzione è stata consolidata e ancorata esplicitamente all'art. 21 della Carta dei diritti fondamentali dell'Unione europea, convertendo un principio giurisprudenzialmente elaborato in diritto primario vincolante. È lo stesso meccanismo (dall'enunciazione valoriale all'operatività giuridica attraverso la mediazione giurisprudenziale) che *Google Spain* (C-131/12 (2014)) ha attivato nel dominio digitale per il diritto all'oblio: un diritto non scritto nei testi, ricavato per via interpretativa dalla Corte di giustizia e poi recepito dal legislatore nel GDPR. Il percorso è tracciato ed è stato già seguito con successo. La Dichiarazione del 2022 può ambire a farlo proprio.

A complicare il quadro interviene la pressione geopolitica. Il modello europeo è esposto a tensioni che provengono da due direzioni opposte: la spinta alla deregolazione in nome della competitività tecnologica e la tentazione, opposta, di rispondere alla dipendenza tecnologica con misure di controllo digitale che rischiano di erodere dall'interno i valori proclamati, di cui i dubbi e le incertezze sul regolamento Chat Control sono l'esempio più eloquente[72].

La prima spinta trova nel Digital Omnibus l'espressione più rilevante e recente. Le due proposte gemelle presentate dalla Commissione il 19 novembre 2025 riaprono il cuore stesso dell'apparato regolatorio europeo a meno di tre anni dalla sua piena operatività, in nome della semplificazione e della competitività[73].

---

[72] L. Carrer, *La strana alleanza tra big tech, Trump e l'estrema destra contro i diritti digitali in Europa*, in *Wired*, 5 febbraio 2026; A. Puliafito, *La retromarcia dell'AI Act si chiama digital omnibus*, in *Internazionale*, 3 dicembre 2025.

[73] Commissione UE, Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 19 novembre 2025; Proposal for a Regulation amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final, 19 novembre 2025. Per prime riflessioni v. G. Gonzàlez Fuster*, Caught Between AI and the AI Hype: How the Right to personal Data Protection was Ambushed*, in *Rivista di Diritti Comparati*, Spec. Issue VIII, 2026, 107; B. Carotti, *Contro il Digital Omnibus*, in *IRPA*, 18 novembre 2025;

Per quanto concerne la disciplina dei sistemi di intelligenza artificiale, si conferma la portata sistemica dell'intervento, poiché il testo di compromesso licenziato dal Coreper il 13 maggio 2026, in vista dell'adozione in prima lettura, ridefinisce alcuni snodi strutturali dell'AI Act[74]. Sul piano dell'entrata in applicazione, le sezioni 1, 2 e 3 del Capo III, originariamente operative dal 2 agosto 2026, sono rinviate al 2 dicembre 2027 per i sistemi ad alto rischio dell'Allegato III e al 2 agosto 2028 per quelli dell'Allegato I, in ragione del ritardo nella predisposizione delle norme tecniche armonizzate e dell'assetto di governance nazionale. Sul piano sostanziale, viene introdotto un meccanismo orizzontale di limitazione degli obblighi del Capo III, Sezione 2, allorché la legislazione di armonizzazione settoriale elencata nella Sezione A dell'Allegato I garantisca un livello di protezione equivalente o superiore (nuovo art. 2, par. 13). L'elenco delle pratiche vietate viene esteso ai sistemi che generano o manipolano materiale intimo non consensuale e materiale di abuso sessuale su minori (nuovo art. 5, par. 1, lett. ba e bb), in una direzione che rafforza, anziché ridurre, la protezione di posizioni soggettive fondamentali. Specularmente, però, l'obbligo di alfabetizzazione dei fornitori e dei deployers (art. 4) è ricondotto da obbligo di risultato a obbligo di mezzi, e la competenza esclusiva dell'AI Office è ampliata ai sistemi costruiti su modelli per finalità generali sviluppati dalla medesima impresa e a quelli integrati in piattaforme e motori di ricerca *very large* ai sensi del DSA, con un articolato apparato di poteri ispettivi e sanzionatori (nuovi artt. 75-75e). L'insieme di queste modifiche, intervenendo simultaneamente sul perimetro applicativo, sulla tassonomia delle pratiche vietate, sull'architettura di vigilanza e sul cronoprogramma dell'entrata in vigore, appaiono eccedere la categoria della mera semplificazione e configurare piuttosto una rivisitazione di non poco momento.
La proposta sulla disciplina dei dati, viceversa, resta in negoziato e divide i co-legislatori in particolare sulla ridefinizione soggettiva e relativa della nozione di dato personale, su cui EDPB ed EDPS hanno espresso nel febbraio del 2026 un parere congiunto problematico[75]. È sottolineato come la riforma trascenda la dichiarata finalità di codificazione della giurisprudenza della Corte di giustizia (di cui isola selettivamente un solo elemento,

E. Tripodi - G. Cassano, *Il «Digital Omnibus»: semplificazione (o deregolamentazione) del contesto digitale europeo?*, in *Rivista dell'Internet*, 1, 2026.

[74] L'orientamento generale del Consiglio del 13 marzo 2026 (doc. 7322/26) e la posizione del Parlamento europeo adottata il 26 marzo 2026, hanno condotto all'accordo provvisorio del 6 maggio 2026, confermato dal Coreper il 13 maggio 2026 (doc. 9247/26).

[75] V. EDPB-EDPS, *Joint Opinion 02/2026 on the proposal for a Regulation as regards the simplification of the digital legislative framework* (*Digital Omnibus*), 10 febbraio 2026, in *edpb.europa.eu*.

dilatandolo oltre il perimetro tracciato in *EDPS c. SRB*[76]) e introduca una definizione costruita per via negativa, generatrice di incertezza applicativa. Viene ritenuto che essa restringa in modo strutturale l'ambito materiale del GDPR, con effetti diretti sul livello di protezione dei dati personali quale diritto fondamentale ex art. 8 della Carta dei diritti fondamentali. Criticata è anche la delega alla Commissione, per via di atto di esecuzione, scelte che attengono ai confini stessi della tutela.

Letto attraverso la lente dell'antropocentrismo reattivo, il Digital Omnibus è qualcosa di più di un intervento di manutenzione. È il test che misura la stabilità stessa del modello regolatorio europeo. Se la costituzionalizzazione difensiva consolidata nel decennio scorso fosse stata radicata in un baricentro valoriale stabilizzato, una riapertura di tale ampiezza, a tale distanza dall'entrata in vigore degli atti modificati, non sarebbe stata politicamente concepibile. La rapidità con cui le difese costruite intorno alla persona possono essere rinegoziate, quando lo richiede l'argomento della competitività, conferma che l'antropocentrismo europeo non ha ancora trovato l'ancoraggio strutturale che la Dichiarazione del 2022 prometteva. Ne resta, per ora, la dimensione reattiva, esposta come ogni postura difensiva alla pressione delle congiunture.

Le due spinte, deregolatoria e securitaria, convergono in un unico effetto: restringere lo spazio entro cui il modello europeo può sviluppare la sua vocazione promozionale, riducendolo a una funzione difensiva che esso ha già dimostrato di saper esercitare, ma che non esaurisce l'ambizione valoriale della Dichiarazione del 2022.

Colmare il divario fra un diritto della protezione e un diritto dell'emancipazione digitale, passare dalla tutela reattiva all'abilitazione positiva dell'autonomia individuale e collettiva nell'ambiente digitale, è la sfida che la prossima stagione regolatoria dell'Unione ha davanti per dare completezza al modello valoriale europeo. Non si tratta di abbandonare la logica della protezione, ma di arricchirla: costruire le condizioni materiali (competenze, infrastrutture, distribuzione del potere informativo) senza le quali i diritti proclamati restano asimmetrici rispetto alle dinamiche di potere che governano l'ecosistema digitale online. È in questo passaggio dalla protezione alla emancipazione ed *emporwement* che si gioca la maturazione del costituzionalismo digitale europeo: non più soltanto limite al potere tecnologico, ma costruzione giuridica delle condizioni materiali dell'autonomia informazionale della persona nello spazio digitale dell'Unione. Dare a questo statuto digitale europeo della persona una forma giuridica compiuta, definirne il contenuto, i titolari, le condizioni di esercizio e i meccanismi di tutela, è il compito teorico che la stagione regolatoria descritta lascia aperto.

[76] CGUEC-413/23 P, *EDPS c. SRB* (2025).

Abstract

Viene analizzato il modello europeo di regolazione dell'ecosistema digitale europeo online attraverso la lente assiologica della Dichiarazione europea sui diritti e i principi digitali del 2022, assunta come cornice valoriale dell'intero corpus normativo dell'Unione. Il metodo adottato assume i valori proclamati dalla Dichiarazione del 2022 come categorie ordinanti per testare la coerenza materiale del diritto derivato: oggetto dell'analisi è la capacità degli atti normativi adottati nell'ultimo decennio dalle istituzioni europee di tradurre i principi in obblighi giuridicamente esigibili e standard giurisprudenziali effettivi. La tesi centrale è che il modello europeo abbia sviluppato una costituzionalizzazione prevalentemente difensiva dell'ecosistema digitale: più efficace nel limitare i rischi tecnologici che nel costruire condizioni positive di autonomia informazionale. Questa postura viene definita "antropocentrismo reattivo", capace di proteggere, ma non ancora di emancipare l'individuo dai bisogni digitali. Il saggio esamina in successione i sei valori della Dichiarazione del 2022 (centralità della persona, solidarietà e inclusione, libertà di scelta, partecipazione democratica, sicurezza e protezione, sostenibilità ambientale e intergenerazionale), misurando per ciascuno lo scarto tra proclamazione e giurisdizionalizzazione. Il bilancio complessivo individua nel passaggio dalla tutela reattiva all'abilitazione positiva dell'autonomia individuale e collettiva la sfida aperta della prossima stagione regolatoria europea.

This article analyses the European model for regulating the online digital ecosystem through the axiological lens of the 2022 European Declaration on Digital Rights and Principles, taken as the value framework of the Union's entire normative corpus. The methodology treats the values proclaimed by the 2022 Declaration as organising categories against which to test the substantive coherence of secondary law: the inquiry focuses on the capacity of the legislative acts adopted over the past decade by the European institutions to translate principles into legally enforceable obligations and effective judicial standards. The central thesis is that the European model has developed a predominantly defensive constitutionalisation of the digital ecosystem, more effective in containing technological risks than in constructing positive conditions for informational autonomy. This posture is defined as "reactive anthropocentrism": capable of protecting, but not yet of emancipating, the individual from digital dependencies. The article examines in turn the six values of the 2022 Declaration (centrality of the person, solidarity and inclusion, freedom of choice, democratic participation, safety and protection, environmental and intergenerational sustainability), measuring for each the gap between proclamation and justiciability. The overall assessment identifies the transition from reactive

protection to the positive enablement of individual and collective autonomy as the open challenge of the next European regulatory season.

Keywords
European digital ecosystem – European values – digital rights – digital constitutionalism – 2022 European Declaration on Digital Rights and Principles

I giganti digitali alla prova del pluralismo informativo e della tutela del *copyright*[*]

Anna Chimenti, Elena Maioli Castriota Scanderbech

Sommario

1. Introduzione. - 2. Tutela del pluralismo informativo ai sensi della Direttiva Copyright: il diritto a un equo compenso degli editori. - 3. La trasposizione dell'art. 15 della Direttiva Copyright nell'ordinamento italiano e la questione di pregiudizialità dinanzi alla Corte di giustizia UE. - 4. Conclusioni.

1. Introduzione

Non esiste un settore industriale in cui la rivoluzione tecnologica abbia avuto conseguenze così dirompenti sul prodotto e sulla sua diffusione come quello dell'informazione. Qualcuno obietterà che il sistema dell'informazione non può essere considerato tout-court un semplice settore industriale, considerata l'influenza che esercita sulla democrazia e sulle istituzioni. Ed è vero. Ma se nel giro di trent'anni, a un ritmo sempre più rapido, notizie inventate e notizie controllate vengono messe sullo stesso piano, e se la distribuzione delle stesse avviene senza segnalare le differenze, o addirittura prendendo pezzi di qua e pezzi di là, «è l'intera società che, giorno dopo giorno, si scopre completamente mutata. E con essa cambiano di senso diritto e linguaggi, i modi stessi della costruzione della personalità»[1]. Stefano Rodotà, uno dei primi giuristi a studiare la tecnologia applicata all'informazione e più in dettaglio alla comunicazione politica, già nel 1997 si poneva alcune domande che oggi, a distanza di quasi trent'anni, sembrano profetiche.

Parliamo di un'epoca in cui i "social" non erano ancora entrati nell'universo mediatico, impadronendosi dell'informazione fondata su regole e principi e stravolgendola. Eppure, già allora, Rodotà denunciava i muta-

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

[1] S. Rodotà, *Tecnopolitica. La Democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997, 4-5.

menti dei sistemi politici e legati alla diffusione delle nuove tecnologie. In particolare, quella che Rodotà definiva[2] la "teledemocrazia", la "videocrazia" e la "sondocrazia", cioè l'irrompere di una politica non più fondata sul confronto delle idee e dei progetti, ma sulle regole di marketing. E trasformata in una sorta di campagna elettorale permanente in cui i cittadini sono continuamente inseguiti nelle loro tendenze, e non guidati da una classe dirigente secondo le proprie convinzioni e i propri programmi. Che poi via via questo meccanismo "populista", legato cioè all'illusione di compiacere il popolo e di qui ricavare il consenso, abbia portato a una disaffezione al voto che sfiora ormai la metà degli elettori è qualcosa che preoccupa fino a un certo punto i partiti attuali. Essendo importante, appunto, volta per volta, assicurarsi fette di mercato elettorale, e non convincere i cittadini attraverso un'adesione più solida alle proprie proposte.

La velocità con cui si muovono i mutamenti d'opinione dei cittadini sui grandi temi, un tempo oggetto di grandi battaglie civili, come ad esempio divorzio, aborto, nucleare, guerra e pace, in quella che oggi viene definita "speed democracy" fa sì che chi riesce a impadronirsi delle tecnologie e dei grandi gruppi che le governano, controlla in realtà il consenso. Ed è in grado di intervenire anche al di fuori del proprio Paese. Questo ha reso stringente il problema dei "giganti digitali", "*Giant tech*", cioè delle aziende multinazionali che guidano - e trasformano, sempre più spesso, anche attraverso la novità dell'Intelligenza Artificiale - sulla Rete la diffusione delle informazioni. E mentre fino a trent'anni fa la questione era solo di una regolamentazione più severa dell'uso delle televisioni nei singoli Paesi, oggi la dimensione transnazionale delle aziende che controllano la comunicazione è tale da rendere sempre più difficile la ricerca di soluzioni adeguate.

Secondo Enzo Cheli, costituzionalista e primo presidente dell'Autorità per le garanzie nelle comunicazioni ("AGCom"), «i giganti dell'intelligenza artificiale hanno ormai cambiato pelle. Sono nati come soggetti privati, ma si sono tramutati in soggetti pubblici. Oggi hanno un potere paragonabile a quello degli Stati»[3]. Uso spregiudicato dei contenuti, senza riferimento ad autori ed editori, trasformazione degli stessi in miscellanea di notizie vere, controllate e inventate. Difficoltà economiche per l'attività editoriale, privata del tutto o parzialmente dell'esclusiva sui propri prodotti e dei ricavi provenienti dalla pubblicità. Violazioni del diritto d'autore. Sono solo alcune, le più evidenti, delle conseguenze della trasformazione e della prevalenza del mondo digitale che agisce senza regole. Oltre a una forma di colonialismo digitale che è in grado di condizionare in modo transnazionale le campagne elettorali, attraversando gli oceani e modificando i

[2] *Ibid.*

[3] E. Cheli, *I Giganti digitali paghino editori e redazioni ora regole per gli algoritmi*, *Intervista*, in *La Repubblica*, 27 luglio 2024, 25.

confini politici dei territori.
Di fronte a questo fenomeno in così rapida espansione, l'Unione europea ha avvertito la necessità di regolamentare questo cambiamento, definito dalla Commissione europea "il decennio digitale". Così, all'inizio del 2020, con la comunicazione "Plasmare il futuro digitale dell'Europa" ha formalizzato l'intenzione di ridisegnare le norme del mercato interno dei servizi digitali e le "*Giant-tech*".
In considerazione della rapida espansione dell'innovazione tecnologica e dell'incessante evoluzione del mercato, l'Unione europea, da diversi anni, è ormai impegnata a rivendicare una propria "sovranità digitale"[4] attraverso un costante processo di riforme del quadro normativo unionale applicabile all'ecosistema digitale.
Dinanzi alle nuove sfide imposte dallo sviluppo tecnologico nella nuova agorà digitale, il legislatore europeo, rispetto all'emersione del potere digitale, ha inteso, difatti, riappropriarsi del proprio ruolo di *policy maker*, per molto tempo lasciato prevalentemente nelle mani della giurisprudenza della Corte di giustizia dell'Unione europea, attraverso un'impostazione non solo assiologico-sostanziale di matrice legislativa, ma anche procedurale, volta a rimediare alla frequente opacità e mancata trasparenza dei meccanismi algoritmici, superando la logica di un intervento *ex post*, tipico della disciplina della concorrenza, in favore di uno strumentario costituzionale da rimodulare – ma non stravolgere – nel nuovo contesto digitale.[5]
La necessità di preparare l'Unione europea all'era digitale è stata dichiarata dalla Commissione europea già a partire dal 2015, sotto la presidenza di

[4] Per una riflessione sul concetto di "sovranità digitale" cfr. L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philisophy & Technology*, 33, 2020, 369 ss.; M. Santaniello, *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics*, 3, 2021, 579 ss.; V. Bertola, *La sovranità digitale e il futuro di Internet,* in *Rivista Italiana di Informatica e Diritto*, 1, 2022, 39 ss.; M. Merler, *Il ruolo della Commissione europea nella realizzazione dello spazio digitale europeo,* in *Rivista trimestrale di diritto pubblico*, 4, 2024, 1121; B. Marchetti, *L'esecuzione della regolazione digitale dell'Unione europea e il ruolo della Commissione*, ivi, 1096; E. Falletti, *Sovranità digitale, tutela della sicurezza nazionale e libertà di manifestazione del pensiero: i faticosi equilibri della sentenza Tiktok v. Garland*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2025, 81. Avverso l'idea di una sovranità tecnologica europea si v. M. Bauer - F. Erixon, *Sovranità tecnologica? I rischi prima delle opportunità*, in *Aspenia online*, 19 novembre 2020. Bauer ed Erixon ritengono, in particolare, che «[p]er essere più "sovrani" in un'economia globalizzata, gli europei devono puntare a divenire leader mondiali nell'innovazione tecnologica, non solo nella dimensione burocratico-normativa». Ad avviso degli autori, una sovranità tecnologica potrebbe rivelarsi utile ai cittadini europei soltanto se ancorata al concetto di apertura e cooperazione con i partner più stretti, in particolare, con gli Stati Uniti. A favore di un "ponte transatlantico" solido, «cruciale per un effettivo contenimento, da parte del costituzionalismo moderno, dell'ormai consolidato potere digitale di natura privata», cfr. anche O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, 584.

[5] Cfr. O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, cit., 579 ss.

Jean-Claude Juncker, con la presentazione di una "Strategia per il mercato unico digitale in Europa", avente l'obiettivo di garantire a consumatori e imprese i massimi vantaggi derivanti dalla trasformazione digitale all'interno dell'Unione.[6]

Il 25 maggio del 2016, con una comunicazione dal titolo "Piattaforme online e mercato unico digitale. Opportunità e sfide per l'Europa", la Commissione europea ha poi messo in evidenza come le piattaforme online svolgano un ruolo sempre più rilevante, che comporta maggiori responsabilità rispetto ad un apparato normativo, quale quello di cui alla direttiva 2000/31/CE sul commercio elettronico, nota anche come "Direttiva *e-commerce*",[7] concepito quando le piattaforme online non avevano le caratteristiche e la portata attuali.[8]

Tali atti programmatici dell'esecutivo unionale hanno posto le basi per l'adozione di importanti interventi legislativi, quali: la direttiva (UE) 2018/1808 sui servizi di media audiovisivi (c.d. "Direttiva SMAV"),[9] recepita in Italia con d.lgs. 208/2021,[10] volta ad attenuare l'asimmetria regolamentare tra i cd. *broadcaster* tradizionali del settore audiovisivo e coloro che distribuiscono contenuti online, per raggiungere un nuovo equilibrio fra l'esigenza, da un lato, di promuovere lo sviluppo del mercato e, dall'altro, di tutelare gli utenti;[11] il regolamento (UE) 2019/1150, noto anche come

[6] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Strategia per il mercato unico digitale in Europa", COM (2015) 192 final, Bruxelles, 6 maggio 2015.

[7] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico").

[8] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa", COM (2016) 288 final, Bruxelles, 25 maggio 2016.

[9] Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.

[10] Recante il "Testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato".

[11] Per un approfondimento sui principali profili giuridici della direttiva (UE) 2018/1808 e sul suo recepimento nell'ordinamento italiano si v., tra gli altri, G. Abbamonte - E. Apa - O. Pollicino (a cura di), *La Riforma del mercato audiovisivo europeo*, Torino, 2019; G. E. Vigevani - O. Pollicino - C. Melzi d'Eril - M. Cuniberti - M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2022; R. Razzante, *Manuale di diritto dell'informazione e della comunicazione*, Milano, 2022; S. Sica - V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazione*, Milano, 2022; C. Contessa - P. Del Vecchio, *Testo Unico Servizi Media e Audiovisivi. Annotato*

Regolamento *Platform to Business* ("P2B"),[12] che ha introdotto un insieme di norme armonizzate a livello europeo a tutela degli utenti commerciali che si servono dei fornitori di servizi di intermediazione online e dei motori di ricerca online per offrire beni e servizi ai consumatori; la direttiva (UE) 2018/1972 che istituisce il nuovo Codice europeo delle comunicazioni elettroniche,[13] recepita nell'ordinamento italiano con d.lgs. 207/2021;[14] la direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale, nota anche come "Direttiva Copyright", [15] recepita in Italia con d.lgs. 177/2021.[16]

In seguito, sotto il primo mandato di Ursula von der Leyen, all'inizio del 2020, la Commissione europea, con la comunicazione "Plasmare il futu-

con dottrina e giurisprudenza D. lgs. 8 novembre 2021 n. 208, Napoli, 2023; E. Albanesi - A. Valastro - R. Zaccaria, *Diritto dell'informazione e della comunicazione*, Milano, 2023; P. Caretti - A. Cardone, *Il diritto dell'informazione e della comunicazione nell'era dell'intelligenza artificiale*, Bologna, 2024; M. Bassini - R. Mastroianni - O. Pollicino (a cura di), *Il T.U. dei servizi di media audiovisivi*, Milano, 2024.

[12] Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.
Cfr. F. Foltran, *Professionisti, consumatori e piattaforme online: la tutela delle parti deboli nei nuovi equilibri negoziali*, in questa *Rivista,* 3, 2019, 162 ss.; F. Ruggeri, *Regole di trasparenza e rapporti tra imprese nei mercati digitali: il regolamento (UE) 2019/1150 sull'intermediazione online e i motori di ricerca*, in *Diritto dell'Informazione e dell'Informatica,* 2, 2021, 397 ss.

[13] Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il Codice europeo delle comunicazioni elettroniche.

[14] Sulla direttiva (UE) 2018/1972 e sul suo recepimento ad opera del d. lgs. 207/2021 cfr., tra gli altri, F. Dalle Nogare, *Regolazione e mercato delle comunicazioni elettroniche. La storia, la governance delle regole e il nuovo Codice europeo*, Torino, 2019; R. Razzante, *Manuale di diritto dell'informazione e della comunicazione*, cit.; S. Sica - V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazione,* cit.; L. Aria - C. Contessa - P. Del Vecchio, *Codice delle comunicazioni elettroniche. Annotato e commentato articolo per articolo D. lgs. 8 novembre 2021 n. 207*, Napoli, 2025; E. Albanesi - A. Valastro - R. Zaccaria, *Diritto dell'informazione e della comunicazione*, cit.; P. Caretti - A. Cardone, *Il diritto dell'informazione e della comunicazione nell'era dell'intelligenza artificiale*, cit.

[15] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE.

[16] Sulla direttiva (UE) 2019/790 e sul suo recepimento ad opera del d. lgs. n. 177/2021 cfr., tra gli altri, A. Papa (a cura di), *Il diritto d'autore nell'era digitale*, Torino, 2019; V. Franceschelli, *Gli Ottant'anni della legge sul diritto d'autore (Il nostro diritto d'autore dopo la Direttiva 2019/790/UE)*, in *Rivista di diritto industriale*, 6, 2021, 267 ss.; S. Lavagnini (a cura di), *Il diritto d'autore nel mercato unico digitale. Direttiva (UE) 2019/790 e d.lgs. n. 177/2021 di recepimento*, Torino, 2022; G. Cassano - B. Tassone (a cura di), *Diritto industriale e diritto d'autore nell'era digitale*, Milano, 2022; E. Albanesi - A. Valastro - R. Zaccaria, *Diritto dell'informazione e della comunicazione*, cit.; M. L. Bixio (a cura di), *Crisi e resilienza del diritto d'autore. Il recepimento italiano della direttiva 2019/790*, Torino, 2024.

ro digitale dell'Europa",[17] ha poi formalizzato l'intenzione di ripensare le norme del mercato interno per i servizi digitali, rilevando come tali servizi, in particolare quelli forniti dalle grandi piattaforme online, stiano determinando una profonda trasformazione dei flussi economici, delle relazioni sociali e dell'esercizio di alcuni diritti fondamentali, quali la libertà di espressione e l'accesso a informazioni verificate, offrendo, da un lato, nuove opportunità di crescita per il mercato unico, ma amplificando, dall'altro, i rischi per cittadini e utenti.

In particolare, la Commissione von der Leyen, nel constatare come la pandemia di COVID-19 avesse radicalmente cambiato il ruolo e la percezione della digitalizzazione della società e delle economie, accelerandone il ritmo, e avesse, altresì, messo in luce le vulnerabilità sistemiche dell'ambiente digitale, la dipendenza tecnologica dell'Unione europea e l'incidenza della disinformazione sull'effettivo esercizio dei diritti democratici, ha istituito una bussola per tradurre le ambizioni digitali dell'Unione per il 2030 in obiettivi concreti, inaugurando così "il decennio digitale" dell'Europa.[18]

Da dieci anni a questa parte l'Unione europea è così intervenuta in modo sempre più incisivo nel campo della regolamentazione digitale,[19] riconoscendo il ruolo centrale assunto dalle grandi piattaforme online non solo come attori economici, ma anche come nuovi attori che, attraverso il loro potere, non esclusivamente di carattere economico, ma di natura più pervasiva,[20] sono capaci di incidere in profondità sulla sfera pubblica, sulla circolazione delle informazioni e sull'esercizio dei diritti fondamentali.

Pertanto, in un contesto segnato dall'ascesa di nuovi attori globali, meglio noti come i "giganti digitali", "*Giant-tech*" o "*gatekeeper*"[21] (controllori dell'accesso alla Rete), che operano in condizioni di sostanziale asimme-

---

[17] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Plasmare il futuro digitale dell'Europa", COM (2020) 67 final, Bruxelles, 19 febbraio 2020.

[18] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Bussola per il digitale 2030: il modello europeo per il decennio digitale", COM (2021) 118 final, Bruxelles, 9 marzo 2021.

[19] Sull'intervento regolatorio dell'Unione europea nei confronti dei nuovi poteri privati, ossia le grandi *corporations* del digitale che dominano la Rete, cfr. O. Pollicino, *Costituzionalismo digitale. Pensare la democrazia al tempo dell'IA*, Bologna 2025, 254.

[20] Cfr. O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, cit., 570.

[21] Ai sensi dell'art. 3 del regolamento (UE) 2022/1925 «1. Un'impresa è designata come gatekeeper se:

a) ha un impatto significativo sul mercato interno;
b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e
c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro».

tria normativa e informativa con gli operatori tradizionali del settore delle comunicazioni, le istituzioni europee hanno portato avanti un percorso normativo volto a ripristinare margini di sovranità normativa e tutela democratica.

Con tale obiettivo sono stati adottati due importanti strumenti, promossi con enfasi nel dicembre 2020 sottoforma di proposte legislative dalla Commissione europea, il cd. "*Digital services package*" dell'Unione: il regolamento (UE) 2022/2065 sui servizi digitali, noto anche come "*Digital Services Act*" o "DSA",[22] e il regolamento (UE) 2022/1925 sui mercati digitali, noto anche come "*Digital Markets Act*" o "DMA",[23] volti non solo ad aggiornare la regolazione del mercato digitale europeo, ma anche, e soprattutto, a preservare i valori fondamentali dell'ordinamento unionale, tra cui il pluralismo dell'informazione quale componente essenziale del sistema democratico.

Si tratta di un processo di ridefinizione del quadro giuridico dell'Unione sull'ecosistema digitale tuttora *in fieri*, con l'adozione di misure che si inseriscono all'interno di una strategia volta a riaffermare la centralità del diritto dell'Unione europea nella definizione delle regole dell'ecosistema digitale, nella prospettiva di una "sovranità digitale" fondata sulla protezione dei diritti, sull'autonomia strategica e sulla responsabilità delle piattaforme.

In questa prospettiva, degni di nota sono, pertanto, i recenti interventi del legislatore UE di cui al regolamento (UE) 2024/900 che stabilisce norme per la trasparenza e il targeting della pubblicità politica online, con l'obiettivo di contrastare la manipolazione delle informazioni e le interferenze straniere nelle elezioni[24] e il regolamento (UE) 2024/1083 sulla libertà dei

---

[22] 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). Sull'argomento, cfr., fra gli altri, L. Bolognini - E. Pelino - M. Scialdone (a cura di), *Digital Services Act e Digital Markets Act Definizioni e prime applicazioni dei nuovi regolamenti europei*, Milano, 2023; F. Donà, *Libertà di manifestazione del pensiero online e content moderation dei nuovi poteri privati: rischi ed opportunità alla luce della nuova co-regolazione euro-unitaria*, in questa *Rivista*, 2, 2025, 224 ss.

[23] 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 proposito, cfr., fra gli altri, M. Libertini, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, 1069 ss.; L. Bolognini - E. Pelino - M. Scialdone, *Digital Services Act e Digital Markets Act Definizioni e prime applicazioni dei nuovi regolamenti europei*, cit.

[24] Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio del 13 marzo 2024 relativo alla trasparenza e al targeting della pubblicità politica. Sul tema si v. A. Licastro, *La regolazione dello spazio informativo disintermediato dinanzi alla progressiva avanzata della "synthetic media technology" in tempo di tornate elettorali*, in *Diritto pubblico*, 3, 2024, 577 ss.; C. Lobascio, *Micro-targeting politico e protezione dei dati personali. Il regolamento (UE) 2024/900*,

media (noto anche come "*European Media Freedom Act*" o "EMFA"),[25] che istituisce un quadro normativo per promuovere un sistema mediatico libero e pluralista in tutta l'Unione, con l'obiettivo di tutelare la libertà e il pluralismo dell'informazione con una disciplina che si applica anche ai fornitori di servizi di media digitali e di contenuti online.

A fare da cornice alle citate riforme normative in materia di piattaforme, servizi e mercati digitali è, infine, il regolamento (UE) 2024/1689 sull'intelligenza artificiale (noto come "*AI Act*"),[26] adottato nel quadro del progressivo allineamento della disciplina europea del settore digitale alle istanze provenienti dal contesto globale.

La centralità della regolamentazione dello spazio digitale è stata confermata anche dalla nuova legislatura europea nel programma di lavoro per il mandato 2024-2029 della seconda Commissione von der Leyen,[27] così come centrale è stata considerata l'attuazione del regolamento europeo sull'intelligenza artificiale.

Muovendo da tali premesse poste dal legislatore europeo, il presente saggio si soffermerà sul tentativo da parte della direttiva (UE) 2019/790 di riequilibrare i rapporti di forza tra i giganti del web e altri attori nell'ecosistema digitale (editori) al fine di preservare, attraverso la tutela del diritto

in *Rivista Italiana di Informatica e Diritto*, 1, 2025, 205 ss.

[25] Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media). Per approfondimenti cfr. G. E. Vigevani, *Il Regolamento europeo sulla libertà dei media: un passo verso un servizio pubblico indipendente*, in *Quaderni costituzionali*, 3, 2024, 725 ss.; S. Verza, *What is journalism in the digital age? Key definitions in the European Media Freedom Act*, in *Rivista Italiana di Informatica e Diritto*, 1, 2025, 125 ss.

[26] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Tra i numerosi contributi, si segnala G. Cassano - E. M. Tripodi (a cura di), *Il Regolamento europeo sull'intelligenza artificiale. Commento al Reg. UE n. 1689/2024*, Santarcangelo di Romagna, 2024; G. Taddei Elmi - A. Contaldo, *Intelligenza artificiale. AI Act – Regolamento (UE) 1689/2024. Il nuovo scenario giuridico europeo*, Pisa, 2024; B. Marchetti, *Intelligenza artificiale, poteri pubblici e rule of law*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 1, 2024, 49 ss.; A. Amoroso, *Relazione tra l'Intelligenza Artificiale e i suoi Dati*, in *Diritto dell'Informazione e dell'Informatica*, 3, 2024, 351 ss.; J. P. Solé, *Il regolamento dell'Unione europea sull'intelligenza artificiale, la discrezionalità amministrativa e la riserva di umanità*, in *Rivista Trimestrale di Diritto Pubblico*, 3, 2024, 825 ss.; M. Lembo, *L'intelligenza artificiale, l'identità digitale ed il Digital Services Act: dalla disciplina comunitaria a quella nazionale, in Diritto del Commercio Internazionale,* 4, 2024, 993 ss.; F. Paolucci - O. Pollicino - C. Waldron, *Rule of Law in the Age of AI*, in questa *Rivista*, 3, 2025, 197 ss.

[27] Le priorità della nuova Commissione europea sono pubblicate sul suo sito istituzionale.

d'autore, un'informazione pluralista e sostenibile.
L'analisi prenderà le mosse dalla direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale che, con il suo art. 15 mira a bilanciare gli interessi dei titolari dei diritti d'autore con il diritto all'informazione e alla libera circolazione delle idee, riconoscendo agli editori di pubblicazioni di carattere giornalistico il diritto a un'equa remunerazione per l'utilizzo online dei loro contenuti da parte delle piattaforme del web. Sarà, quindi, esaminata la concreta applicazione di tale disposizione nel nostro ordinamento e il rinvio pregiudiziale disposto dinanzi alla Corte di giustizia dell'Unione europea da parte del giudice amministrativo italiano.
L'attuazione di tale normativa nel nostro ordinamento condurrà ad alcune riflessioni conclusive, alla luce dell'attuale contesto internazionale politico, economico e sociale.
La tutela del pluralismo informativo passa anche dalla tutela del diritto d'autore degli operatori del panorama informativo, richiedendo, in ultima istanza, una maggiore *accountability* dei giganti del web.
Come è stato opportunamente osservato, il processo di privatizzazione della sfera pubblica si è ampliato con l'irrompere del fattore tecnologico e la diffusione del sistema radiotelevisivo dalla seconda metà del secolo scorso,[28] determinando nuove forme di comunicazione collettiva e rinnovati modelli di produzione e circolazione delle informazioni.[29] Affinché il discorso pubblico possa assolvere alle proprie funzioni democratiche, esso non può ridursi a un insieme caotico di impulsi emotivi, ma necessita, invece, di un assetto istituzionale solido che garantisca l'apertura e l'accessibilità degli spazi di formazione dell'opinione pubblica, contrastando i fenomeni di privatizzazione e frammentazione autoreferenziale imposti dalle grandi piattaforme digitali.[30]

2. Tutela del pluralismo informativo ai sensi della Direttiva Copyright: il diritto a un equo compenso degli editori

Dalla metà dell'Ottocento il sistema dell'informazione si è strutturato at-

[28] C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quaderni costituzionali*, 3, 2023, 545. Sull'evoluzione del sistema radiotelevisivo nell'ordinamento italiano cfr. A. Chimenti, *L'ordinamento radiotelevisivo italiano*, Torino, 2007.

[29] G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *medialaws.eu*, 2018, 19 ss.

[30] C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, cit., 544.

torno a tre pilastri: le agenzie di stampa, i giornali e le rassegne stampa. Le agenzie si occupavano della raccolta di informazioni e notizie, i giornali della loro pubblicazione, mentre le rassegne stampa selezionavano e organizzavano gli articoli per offrirli a un pubblico mirato. Sullo sfondo, il diritto d'autore. Al centro di questa filiera si trovano i giornali, che costituiscono l'anello essenziale del processo: senza di essi, né la raccolta delle notizie né la loro selezione e diffusione avrebbero senso. Pertanto, la stampa ha storicamente rappresentato il fulcro del sistema informativo e ha avuto un ruolo fondamentale anche nella conquista della libertà di espressione. Proprio da questa funzione nasce, nel solco della Rivoluzione francese e delle rivoluzioni liberali dell'Ottocento, il diritto costituzionale alla libera manifestazione del pensiero, sancito oggi dall'art. 21 della Costituzione italiana, che tutela la libertà di espressione e garantisce l'indipendenza della stampa da autorizzazioni o censure.[31]

Il principio del pluralismo, nella specifica accezione di pluralismo informativo, rappresenta un valore essenziale dell'ordinamento nel settore delle comunicazioni di massa, e oggi si ritrova inscindibilmente integrato con l'ambito dei servizi digitali offerti tramite Internet. Tale rilevanza si fonda sulla peculiare capacità dei mezzi di comunicazione di veicolare contenuti idonei a influenzare l'opinione pubblica, con il rischio che essi si trasformino in strumenti di parte e compromettano, pertanto, l'equilibrio democratico.

A partire dalla sentenza 10 luglio 1974, n. 226, la Corte costituzionale ha ribadito con continuità che un'eccessiva concentrazione del potere informativo può generare una forza di condizionamento dell'opinione pubblica incompatibile con i principi fondamentali del sistema democratico, come affermato, tra le altre, nelle sentenze 21 luglio 1981, n. 148, 14 luglio 1988, n. 826, e 20 novembre 2002, n. 466.

Muovendo da tali premesse, ai fini del presente contributo, si osserva, in primo luogo, che tra le sfide imposte al legislatore europeo dal rapido sviluppo del settore digitale si può certamente annoverare quella relativa alla modernizzazione del diritto d'autore.

La continua evoluzione delle tecnologie digitali e delle reti di comunicazione ha profondamente modificato – semplificandole e innovandole – le modalità attraverso cui le informazioni vengono reperite, condivise e diffuse. In tale contesto, gli intermediari digitali e i motori di ricerca hanno assunto un ruolo centrale nella vita economica e sociale, offrendo strumenti nuovi per l'accesso e la diffusione dei contenuti informativi.

Parallelamente, le nuove modalità di distribuzione delle informazioni su internet hanno ampliato la platea degli utenti e trasformato la nozione di

[31] V. Franceschelli, *Giornali, agenzie di stampa, rassegne stampa. La filiera dell'informazione e il diritto d'autore*, in *Rivista di Diritto Industriale*, 1, 2021, 48 ss.

"pubblicazione giornalistica", includendovi non solo testi scritti, ma anche contenuti multimediali a essi associati, come immagini e video.
La disponibilità online di una vasta gamma di contenuti giornalistici ha favorito la nascita di nuovi servizi digitali, come gli aggregatori di notizie e i servizi di media monitoring, il cui modello economico si fonda in larga parte sul riutilizzo di tali pubblicazioni, da cui traggono ricavi. Questi servizi vengono generalmente offerti agli utenti in forma gratuita, essendo finanziati prevalentemente con introiti pubblicitari e mediante lo sfruttamento dei dati personali degli utenti attraverso la profilazione algoritmica,[32] pratica che depaupera la riservatezza dell'utente e che, come è stato osservato, costituisce la lesione più significativa del suo rapporto con la piattaforma digitale.[33]
Nel frattempo, i media tradizionali – televisione, radio ed editoria – hanno subìto, nell'ultimo decennio, una contrazione significativa dei ricavi, sia da parte degli utenti sia, soprattutto, sul fronte della pubblicità. Pur essendo cresciuti i ricavi derivanti dalle attività online, essi non sono bastati a colmare le perdite legate al calo delle vendite nei canali tradizionali.
In particolare, il settore della stampa quotidiana, registrando una riduzione complessiva dei ricavi, appare tra i più colpiti, con un continuo declino delle vendite cartacee che non sembra poter essere invertito neanche dall'incremento delle vendite di copie in formato digitale.
In tale contesto si colloca la disciplina europea di cui alla Direttiva Copyright 2019/790 che, *inter alia*, ha inteso proteggere le pubblicazioni di carattere giornalistico in caso di utilizzo online.
Fino all'adozione della direttiva (UE) 2019/790, la tutela del diritto d'autore online è stata affidata nell'Unione alla direttiva 2001/29/CE sul diritto d'autore nella società dell'informazione, cd. "Direttiva *infosoc*",[34] e alla direttiva sul commercio elettronico (2000/31/CE), entrambe aventi lo scopo di creare un quadro giuridico armonizzato, condizione essenziale per l'efficace operatività del mercato unico UE. A questi atti normativi ha fatto poi seguito la direttiva 2004/48/CE, cd. "Direttiva *enforcement*", che ha inteso rafforzare i mezzi a disposizione dei titolari dei diritti.[35]

---

[32] Su come la profilazione algoritmica contribuisca a selezionare contenuti determinanti per la formazione dell'opinione pubblica e per l'*agenda setting* politica cfr. M. Delmastro - A. Nicita, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019, 91.

[33] S. Mannoni - G. Stazi, *Is competition a click away? Sfida al monopolio nell'era digitale*, Napoli, 2018, 34.

[34] Direttiva 2001/29/CE del Parlamento europeo e del Consiglio del 22 maggio 2001 sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.

[35] Direttiva 2004/48/CE del Parlamento europeo e del Consiglio del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale.

Nondimeno, con la "Strategia per il mercato unico digitale in Europa" del 2015 la Commissione europea, rilevando un quadro giuridico UE frammentato in materia, ha evidenziato la necessità di una maggiore certezza giuridica al fine di promuovere un utilizzo più ampio e sicuro delle opere protette, in particolare, assicurando un'equa remunerazione ai titolari dei diritti e precisando le norme sugli intermediari online.[36]

La tutela del diritto d'autore, difatti, riveste un ruolo fondamentale, ancorché spesso poco percepito, nell'industria dell'informazione e nell'assetto dei relativi mercati.[37]

In particolare, con la Direttiva Copyright del 2019 il legislatore UE ha cercato di risolvere il problema del cd. "*value gap*", ossia l'iniqua distribuzione, tra gli autori e i prestatori di servizi che operano in rete, del valore generato dallo sfruttamento in ambito digitale di opere e contenuti protetti da diritto d'autore per la veicolazione dei contenuti generati dai primi. Si tratta di un problema che è stato particolarmente avvertito dagli autori di pubblicazioni di carattere giornalistico.

La direttiva (UE) 2019/790 stabilisce un quadro giuridico che consente di stimolare «l'innovazione, la creatività, gli investimenti e la produzione di contenuti nuovi, anche in ambiente digitale, mirando a evitare la frammentazione del mercato interno» (considerando 2), mediante «norme relative ai diritti sulle pubblicazioni, all'uso di opere o altri materiali da parte dei prestatori di servizi online che memorizzano contenuti caricati dagli utenti e vi danno accesso, alla trasparenza dei contratti per autori e artisti (interpreti o esecutori), alla remunerazione di autori e artisti (interpreti o esecutori), nonché a un meccanismo per la revoca dei diritti che autori e artisti (interpreti o esecutori) hanno trasferito in esclusiva» (considerando 3).

Al riguardo occorre richiamare il considerando 54 della Direttiva Copyright, il quale prevede che: «Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità e l'accesso dei cittadini all'informazione e dà un contributo fondamentale al dibattito pubblico e al corretto funzionamento di una società democratica. […]». Il successivo considerando 55 della direttiva afferma poi che: «Il contributo organizzativo e finanziario degli editori nel produrre pubblicazioni di carattere giornalistico va riconosciuto e ulteriormente incoraggiato per garantire la sostenibilità dell'editoria e favorire in tal modo la disponibilità di informazioni affidabili. […]». La sostenibilità economica rappresenta oggi la principale sfida per il setto-

[36] Per una disamina degli atti programmatici che hanno condotto all'approvazione della direttiva (UE) 2019/790 cfr. S. Lavagnini (a cura di), *Iter della direttiva 2019/790 e sua implementazione in Europa e in Italia*, in *Il diritto d'autore nel mercato unico digitale. Direttiva (UE) 2019/790 e d.lgs. n. 177/2021 di recepimento*, 2022, 2 ss.

[37] G. Priora, *Diritto d'autore e accesso all'informazione giornalistica: accanimento o lungimiranza del legislatore comunitario?*, in *Diritto dell'Informazione e dell'Informatica*, 4, 2020, 836.

re dell'informazione: tanto gli editori tradizionali quanto quelli nativi digitali affrontano serie difficoltà sotto il profilo economico-finanziario, con il concreto rischio di non riuscire più a sostenere un modello di giornalismo fondato sulla qualità.

Tale situazione rischia di impattare il diritto fondamentale alla libertà di espressione e di informazione, tutelato su scala nazionale, europea e internazionale, dal momento che un sistema editoriale sano costituisce una garanzia essenziale per l'effettivo esercizio del diritto dei cittadini a ricevere un'informazione libera, pluralistica e indipendente.

Come riconosciuto dalla stessa giurisprudenza costituzionale italiana, quello fra libertà di informazione e Stato democratico è un legame indissolubile, così come indissolubile è il rapporto tra libertà di informare, libertà di essere informati e pluralismo dei media.[38]

In questa visione il "diritto di informarsi" e di "ricevere informazioni" affermato dalla Corte costituzionale italiana scaturiva come «riflesso indiretto di quella "libertà di informare", che risultava direttamente garantita dall'art. 21, assumendo il suo contenuto in relazione all'obbligo imposto allo Stato ed agli altri soggetti della sfera pubblica di non frapporre ostacoli e di non operare discriminazioni nei confronti dell'accesso dei singoli alle fonti di informazione. […]».[39]

Pertanto, l'intervento del legislatore europeo per garantire un giornalismo di qualità, che trova conferma nei principi della Costituzione italiana, evidentemente non può realizzarsi, in un sistema dell'informazione online, da un lato, non sostenibile economicamente da parte degli editori e, dall'altro, caratterizzato dall'assenza sulle grandi piattaforme digitali di contenuti giornalistici professionali.

In tale prospettiva, l'art. 15 della Direttiva Copyright, intitolato "Protezione delle pubblicazioni di carattere giornalistico in caso di utilizzo online",[40]

---

[38] «[…] negli orientamenti di questa giurisprudenza, il "diritto dell'informazione" si è venuto sempre più a intrecciare con una sorta di "teoria generale della democrazia", che la Corte ha elaborato spinta dall'esigenza di ricercare il fondamento della "libertà di informazione", anche al di là dei contenuti specifici dell'art. 21, nei principi ispiratori della nostra forma di Stato che, in quanto democratica, deve trovare la sua base nell'esistenza di un'opinione pubblica "consapevole", cioè informata. Su questo piano si può, dunque, cogliere il senso di quella "coessenzialità", che la Corte, in numerose pronunce, ha riferito al rapporto tra la libertà di espressione usata a fini informativi e la forma di Stato democratico, la cui essenza implica "pluralità di fonti di informazione, libero accesso alle medesime, assenza di ingiustificati ostacoli legali, anche temporanei, alla circolazione delle notizie e delle idee" (la sent. n. 105/1972, ripresa anche nella sent. n. 94 del 1977)». Così E. Cheli, *Libertà di informazione e pluralismo informativo negli indirizzi della giurisprudenza costituzionale*, in A. Pisaneschi – L. Violini (a cura di), *Poteri, garanzie e diritti a sessanta anni dalla Costituzione. Scritti per Giovanni Grottanelli de' Santi*, I, Milano, 2007, 1405 ss.

[39] *Ibid.*

[40] L'art. 15 della direttiva (UE) 2019/790 recita come segue: «1.Gli Stati membri

prevede il riconoscimento agli editori di giornali di un diritto connesso da parte delle piattaforme per l'utilizzo online delle loro pubblicazioni ed obbliga gli editori medesimi a riconoscere una quota adeguata dei proventi agli autori delle pubblicazioni, contribuendo a correggere il divario di potere contrattuale tra le parti. Si tratta, di un modello che impatta sul ruolo e sulle responsabilità dei prestatori di un servizio della società dell'informazione, inteso come «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi»,[41] e che mira a soddisfare le istanze degli editori rispetto a una iniqua distribuzione del valore generato dallo sfruttamento di opere e contenuti protetti, così da promuovere, per quanto possibile, un *level playing field* nell'ecosistema informativo tra operatori tradizionali e i nuovi attori del web.

riconoscono agli editori di giornali stabilito in uno Stato membro i diritti di cui all'articolo 2 e all'articolo 3, paragrafo 2, della direttiva 2001/29/CE per l'utilizzo online delle loro pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione. I diritti di cui al primo comma non si applicano agli utilizzi privati o non commerciali delle pubblicazioni di carattere giornalistico da parte di singoli utilizzatori. La protezione accordata a norma del primo comma non si applica ai collegamenti ipertestuali. I diritti di cui al primo comma non si applicano all'utilizzo di singole parole o di estratti molto brevi di pubblicazioni di carattere giornalistico.

2.I diritti di cui al paragrafo 1 non modificano e non pregiudicano in alcun modo quelli previsti dal diritto dell'Unione per gli autori e gli altri titolari di diritti relativamente ad opere e altri materiali inclusi in una pubblicazione di carattere giornalistico. I diritti di cui al paragrafo 1 non possono essere invocati contro tali autori e altri titolari di diritti e, in particolare, non possono privarli del diritto di sfruttare le loro opere e altri materiali in modo indipendente dalla pubblicazione di carattere giornalistico in cui sono inclusi. Quando un'opera o altri materiali è inclusa in una pubblicazione di carattere giornalistico sulla base di una licenza non esclusiva, i diritti di cui al paragrafo 1 non possono essere invocati per impedire l'utilizzo da parte di altri utilizzatori autorizzati. I diritti di cui al paragrafo 1 non possono essere invocati per impedire l'utilizzo di opere o altri materiali la cui protezione sia scaduta.

3.Gli articoli da 5 a 8 della direttiva 2001/29/CE, la direttiva 2012/28/UE e la direttiva (UE) 2017/1564 del Parlamento europeo e del Consiglio si applicano, mutatis mutandis, ai diritti di cui al paragrafo 1 del presente articolo.

4.I diritti di cui al paragrafo 1 si estinguono due anni dopo la pubblicazione della pubblicazione di carattere giornalistico. Tale termine è calcolato a decorrere dal 1° gennaio dell'anno successivo alla data di pubblicazione di tale pubblicazione di carattere giornalistico. Il paragrafo 1 non si applica alle pubblicazioni di carattere giornalistico pubblicata per la prima volta prima del 6 giugno 2019.

5.Gli Stati membri provvedono affinché gli autori delle opere incluse in una pubblicazione di carattere giornalistico ricevano una quota adeguata dei proventi percepiti dagli editori per l'utilizzo delle loro pubblicazioni di carattere giornalistico da parte dei prestatori di servizi della società dell'informazione».

[41] Ai sensi dell'art. 1, par. 1, lett. b), della direttiva (UE) 2015/1535 che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione.

L'art. 15 della Direttiva Copyright stabilisce: i) il diritto degli editori di giornali di autorizzare o vietare la riproduzione o la comunicazione al pubblico delle pubblicazioni di carattere giornalistico da parte dei prestatori di servizi della società dell'informazione (in inglese, *Information Society Service Providers* o anche "ISSP"); ii) l'esclusione degli utilizzi privati o non commerciali da parte di singoli utilizzatori; iii) l'esclusione dei collegamenti ipertestuali, delle singole parole, degli estratti molto brevi o delle opere la cui protezione sia scaduta e; iv) il versamento di una quota adeguata dei proventi percepiti dai prestatori di servizi della società dell'informazione agli editori di giornali e, quindi, a giornalisti e agli autori.
Il legislatore dell'Unione europea ha voluto, pertanto, conferire agli editori prerogative che consentono loro di esercitare un controllo concreto ed effettivo sui loro diritti di proprietà intellettuale, potendo questi stabilire se, e a quali condizioni, in particolare economiche, intendano autorizzare i prestatori di servizi della società dell'informazione a riprodurre e a mettere a disposizione del pubblico i loro materiali protetti.
Si tratta di una disposizione la cui adozione è stata accompagnata da dure critiche sia durante l'iter legislativo di approvazione che a seguito dell'entrata in vigore della Direttiva Copyright,[42] sebbene la centralità assunta dalle piattaforme digitali nel veicolare contenuti, opinioni e notizie avesse reso davvero imprescindibile una disciplina giuridica capace di garantire trasparenza, responsabilità e pluralismo.
A tal riguardo basti considerare che la televisione non rappresenta più il principale mezzo di informazione degli italiani, figurando come canale informativo privilegiato solo del 46,5% della popolazione adulta, mentre nel 2019 lo era ancora per il 67,4%. Si tratta di un calo di oltre 20 punti percentuali nell'arco di appena cinque anni che evidenzia con forza la profonda trasformazione in atto nel sistema dell'informazione.[43]
Internet rappresenta, difatti, la principale fonte di accesso all'informazione per la maggior parte degli italiani, dal momento che oltre un italiano su due (52,4%) si informa oggi principalmente attraverso la Rete: motori di

[42] Cfr. *inter alia*, C. Geiger - O. Bulayenko - G.F. Frosio, *The Introduction of a Neighbouring Right for Press Publishers at EU Level: the Unneeded (and Unwanted) Reform*, in *European Intellectual Property Review*, 39(4), 2017, 202; G. Colangelo - V. Torti, *Copyright, Online News Publishing and Aggregators: a Law and Economics Analysis of the EU Reform*, in *International Journal of Law and Information Technology*, 27(1), 2019, 75. E, per ciò che concerne il recepimento della direttiva (UE) 2019/790 nell'ordinamento italiano, come riportato nel successivo § 3, cfr. le critiche riportate in C. Sganga - M. Contardi, *The new Italian press publishers' right: creative, fairness-oriented…and invalid?*, in *Journal of Intellectual Property Law & Practice*, 17, 2022, 421 ss.

[43] In tal senso Autorità per le garanzie nelle comunicazioni, *Osservatorio annuale sul sistema dell'informazione*, 2025. Tuttavia, televisione, radio e carta stampata continuano a essere percepite come fonti più affidabili rispetto ai social network e alle piattaforme digitali.

ricerca, social media, siti web e app di testate giornalistiche sono divenuti le principali porte d'accesso all'informazione.
Si è andata, inoltre, attenuando la convinzione per cui i problemi che la radiotelevisione ha posto in passato, quali la scarsità del mezzo, il costo degli impianti, la natura tendenzialmente oligopolistica del mercato appaiono ormai superati.
Pertanto, stenta ad essere ormai confermata la convinzione che la nuova tecnologia della rete abbia egregiamente superato le lacune informative dei vecchi mass media.[44] Nel contesto attuale convivono, difatti, davanti ai nostri occhi due diversi scenari: «l'utopica generalizzazione della libertà di informazione a favore di tutti; il distopico asservimento di quella libertà alla logica affaristica dei nuovi giganti della rete».[45]

3. La trasposizione dell'art. 15 della Direttiva Copyright nell'ordinamento italiano e la questione di pregiudizialità dinanzi alla Corte di giustizia UE

Il pieno godimento dei diritti da parte degli editori di giornali ai sensi dell'art. 15 della Direttiva Copyright ha richiesto l'adozione, da parte degli Stati membri, di misure attuative capaci di creare un contesto giuridico favorevole al loro esercizio effettivo.
A tal fine, l'art. 15 della Direttiva Copyright è stato trasposto nell'ordinamento italiano ad opera del d.lgs. 177/2021,[46] che ha novellato la legge sul diritto d'autore 22 aprile 1941, n. 633, e ha inserito in quest'ultima l'art. 43-*bis*.[47]

---

[44] M. Manetti, *Internet e i nuovi pericoli per la libertà di informazione*, in *Quaderni costituzionali*, 3, 2023, 524.

[45] *Ibid.*

[46] Recante "Attuazione della direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE".

[47] L'art. 43-*bis* della l. n. 633/1941 prevede che: «1. Agli editori di pubblicazioni di carattere giornalistico, sia in forma singola che associata o consorziata, sono riconosciuti per l'utilizzo online delle loro pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione di cui all'articolo 1, comma 1, lett. b), del decreto legislativo 15 dicembre 2017, n. 223, comprese le imprese di media monitoring e rassegne stampa, i diritti esclusivi di riproduzione e comunicazione di cui agli articoli 13 e 16.
2. Per pubblicazione di carattere giornalistico si intende un insieme composto principalmente da opere letterarie di carattere giornalistico, che può includere altre opere e materiali protetti, come fotografie o videogrammi, e costituisce un singolo elemento all'interno di una pubblicazione periodica o regolarmente aggiornata, recante un titolo unico, quale un quotidiano o una rivista di interesse generale o specifico, con la funzione di informare il pubblico su notizie, o altri argomenti, pubblicata su qualsiasi mezzo di

comunicazione sotto l'iniziativa, la responsabilità editoriale e il controllo di un editore o di un'agenzia di stampa. Ai fini del presente articolo le pubblicazioni periodiche a fini scientifici o accademici non sono considerate quali pubblicazioni di carattere giornalistico.
3. Per editori di pubblicazioni di carattere giornalistico si intendono i soggetti che, sia in forma singola che associata o consorziata, nell'esercizio di un'attività economica, editano le pubblicazioni di cui al comma 2, anche se stabiliti in un altro Stato membro.
4. Sono fatti salvi in ogni caso i diritti riconosciuti dalla presente legge a favore degli autori e degli altri titolari di diritti concernenti opere o altri materiali inclusi in una pubblicazione a carattere giornalistico, compreso il diritto di sfruttarli anche in forme diverse dalla pubblicazione a carattere giornalistico.
5. Quando un'opera o altri materiali protetti sono inclusi in una pubblicazione di carattere giornalistico sulla base di una licenza non esclusiva, i diritti di cui al comma 1 non possono essere invocati per impedire l'utilizzo da parte di altri utilizzatori autorizzati o per impedire l'utilizzo di opere o di altri materiali la cui protezione sia scaduta.
6. I diritti di cui al comma 1 non sono riconosciuti in caso di utilizzi privati o non commerciali delle pubblicazioni di carattere giornalistico da parte di singoli utilizzatori, né in caso di collegamenti ipertestuali o di utilizzo di singole parole o di estratti molto brevi di pubblicazioni di carattere giornalistico.
7. Per estratto molto breve di pubblicazione di carattere giornalistico si intende qualsiasi porzione di tale pubblicazione che non dispensi dalla necessità di consultazione dell'articolo giornalistico nella sua integrità.
8. Per l'utilizzo online delle pubblicazioni di carattere giornalistico i prestatori di servizi della società dell'informazione riconoscono ai soggetti di cui al comma 1 un equo compenso. Entro sessanta giorni dalla data di entrata in vigore della presente disposizione, l'Autorità per le garanzie nelle comunicazioni adotta un regolamento per l'individuazione dei criteri di riferimento per la determinazione dell'equo compenso di cui al primo periodo, tenendo conto, tra l'altro del numero di consultazioni online dell'articolo, degli anni di attività e della rilevanza sul mercato degli editori di cui al comma 3 e del numero di giornalisti impiegati, nonché dei costi sostenuti per investimenti tecnologici e infrastrutturali da entrambe le parti, e dei benefici economici derivanti, ad entrambe le parti, dalla pubblicazione quanto a visibilità e ricavi pubblicitari.
9. La negoziazione, per la stipula del contratto avente ad oggetto l'utilizzo dei diritti di cui al comma 1, tra i prestatori di servizi della società dell'informazione, comprese le imprese di media monitoring e rassegne stampa, e gli editori di cui al comma 3, è condotta tenendo conto anche dei criteri definiti dal regolamento di cui al comma 8. Nel corso della negoziazione i prestatori di servizi delle società dell'informazione non limitano la visibilità dei contenuti degli editori nei risultati di ricerca. L'ingiustificata limitazione di tali contenuti nella fase delle trattative può essere valutata ai fini della verifica del rispetto dell'obbligo di buona fede di cui all'articolo 1337 del codice civile.
10. Fermo restando il diritto di adire l'autorità giudiziaria ordinaria di cui al comma 11, se entro trenta giorni dalla richiesta di avvio del negoziato di una delle parti interessate non è raggiunto un accordo sull'ammontare del compenso, ciascuna delle parti può rivolgersi all'Autorità per le garanzie nelle comunicazioni per la determinazione dell'equo compenso, esplicitando nella richiesta la propria proposta economica. Entro sessanta giorni dalla richiesta della parte interessata, anche quando una parte, pur regolarmente convocata non si è presentata, l'Autorità indica, sulla base dei criteri stabiliti dal regolamento di cui al comma 8, quale delle proposte economiche formulate è conforme ai suddetti criteri oppure, qualora non reputi conforme nessuna delle proposte, indica d'ufficio l'ammontare dell'equo compenso.
11. Quando, a seguito della determinazione dell'equo compenso da parte dell'Autorità

L'art. 43-*bis* l. 633/1941 ha previsto che agli editori siano riconosciuti i diritti esclusivi di riproduzione e comunicazione di cui agli articoli 13 e 16 l. 633/1941 da parte dei prestatori di servizi della società dell'informazione, nel cui alveo vengono anche ricondotte le imprese di media monitoring e rassegne stampa.

In particolare, l'art. 43-*bis* l. 633/1941 rimette in primo luogo alle parti il compito di definire, d'intesa tra loro e sulla base di trattative condotte secondo buona fede, l'ammontare dell'equo compenso, essendo facoltativa ed eventuale la possibilità di adire il giudice ordinario o di richiedere, in alternativa, l'intervento dell'Autorità per le garanzie nelle comunicazioni che si esprime sulla conformità delle rispettive proposte economiche ai criteri individuati nel regolamento da essa adottato ai sensi di legge, formulandone d'ufficio una proposta economica laddove queste siano dall'Autorità

per le garanzie nelle comunicazioni, le parti non addivengono alla stipula del contratto, ciascuna parte può adire la sezione del giudice ordinario specializzata in materia di impresa, competente ai sensi dell'articolo 3, comma 1, lettera b), del decreto legislativo 27 giugno 2003, n. 168, anche al fine di esperire l'azione di cui all'articolo 9 della legge 18 giugno 1998, n. 192.

12. I prestatori di servizi della società dell'informazione, comprese le imprese di media monitoring e rassegne stampa, sono obbligati a mettere a disposizione, su richiesta della parte interessata, anche tramite gli organismi di gestione collettiva o entità di gestione indipendenti di cui al decreto legislativo 15 marzo 2017 n. 35, qualora mandatari, o dell'Autorità per le garanzie nelle comunicazioni, i dati necessari a determinare la misura dell'equo compenso. L'adempimento dell'obbligo di cui al primo periodo non esonera gli editori di cui al comma 3 dal rispetto della riservatezza delle informazioni di carattere commerciale, industriale e finanziario di cui sono venuti a conoscenza. Sull'adempimento dell'obbligo di informazione a carico dei prestatori di servizi vigila l'Autorità per le garanzie nelle comunicazioni. In caso di mancata comunicazione di tali dati entro trenta giorni dalla richiesta ai sensi del primo periodo, l'Autorità applica una sanzione amministrativa pecuniaria a carico del soggetto inadempiente fino all'uno per cento del fatturato realizzato nell'ultimo esercizio chiuso anteriormente alla notifica della contestazione. Per le sanzioni amministrative di cui al quarto periodo è escluso il beneficio del pagamento in misura ridotta previsto dall'articolo 16 della legge 24 novembre 1981, n. 689.

13. Gli editori di cui al comma 3, sia in forma singola che associata o consorziata, riconoscono agli autori degli articoli giornalistici una quota, compresa tra il 2 per cento e il 5 per cento, dell'equo compenso di cui al comma 8, da determinare, per i lavoratori autonomi, su base convenzionale. Per i lavoratori con rapporto di lavoro subordinato tale quota può essere determinata mediante accordi collettivi.

14. I diritti di cui al presente articolo si estinguono due anni dopo la pubblicazione dell'opera di carattere giornalistico. Tale termine è calcolato a decorrere dal 1° gennaio dell'anno successivo alla data di pubblicazione dell'opera di carattere giornalistico.

15. Le disposizioni di cui al presente articolo non si applicano alle pubblicazioni di carattere giornalistico pubblicate per la prima volta anteriormente al 6 giugno 2019.

16. Ai diritti di cui al comma 1 si applicano le disposizioni relative alle eccezioni e alle limitazioni previste dal Capo V del Titolo I, alle misure tecnologiche di protezione previste dal Titolo II-ter, alle difese e sanzioni giudiziarie di cui al Capo III del Titolo III, nonché l'articolo 2 della legge 20 novembre 2017 n. 167».

valutate come non conformi.
Dovendo l'art. 43-*bis* l. 633/1941 essere letto e interpretato alla luce dello spirito del diritto dell'Unione europea e, in particolare, della *ratio* sottesa alla formulazione dell'art. 15 della Direttiva Copyright, l'equo compenso è, preliminarmente, oggetto di una libera negoziazione tra le parti che, nel pieno esercizio della loro autonomia contrattuale, possono addivenire ad un accordo che tenga conto "anche" dei criteri indicati dall'Autorità per le garanzie nelle comunicazioni. L'art. 43-*bis*, nel compiere un necessario bilanciamento tra gli interessi in gioco, tiene conto della libertà di iniziativa economica delle parti, tutelata a livello costituzionale e manifestata nella libertà negoziale.
Cionondimeno, la norma, prevedendo l'intervento dell'Autorità su istanza di parte in caso di mancato accordo, prende in considerazione anche lo squilibrio di forza contrattuale esistente tra le parti coinvolte. Pertanto, il legislatore italiano da un lato ha inteso imporre obblighi di trasparenza ai prestatori di servizi della società dell'informazione, dall'altro ha inteso rafforzare la posizione degli editori di giornali nella negoziazione con i prestatori.[48]
Il nuovo contesto digitale ha battezzato nuovi modelli di business, superando quelli cui si ancorava l'editoria tradizionale e assegnando un ruolo centrale alle piattaforme digitali nella diffusione dei contenuti. In un ambiente aperto e concorrenziale, le fonti di ricavo per gli editori derivano tanto dalla vendita dell'informazione (tramite abbonamenti o accessi a pagamento) quanto dalla pubblicità online.
In tale scenario, i criteri per la definizione dell'equo compenso devono riflettere un equilibrio tra l'esigenza di garantire un'informazione di qualità – assicurando una remunerazione adeguata ai produttori di notizie – e quella di favorire un'evoluzione efficiente e innovativa dell'intero settore, anche sul piano tecnologico. La natura economica dell'informazione, qualificabile come bene esperienza, unita alle trasformazioni strutturali e funzionali del sistema informativo online comporta il rischio di un progressivo deterioramento della qualità dei contenuti circolanti sulla rete, con il conseguente emergere di fenomeni di disinformazione.[49]
In questa prospettiva, i criteri per la determinazione dell'equo compenso dovrebbero incentivare la produzione e la diffusione di contenuti informativi di qualità. Ciò costituisce un valore per tutti gli attori coinvolti: per gli editori, in quanto consente il riconoscimento del valore aggiunto proprio

[48] Così Autorità per le garanzie nelle comunicazioni, delibera n. 3/23/CONS, recante "Regolamento in materia di individuazione dei criteri di riferimento per la determinazione dell'equo compenso per l'utilizzo online di pubblicazioni di carattere giornalistico di cui all'articolo 43-bis della legge 22 aprile 1941, n. 633", 2023, 9.

[49] Ivi, 11.

della pubblicazione giornalistica professionale; per i prestatori di servizi quali le grandi piattaforme online, e incluse le imprese di media monitoring e rassegna stampa, poiché la qualità dell'informazione contribuisce alla loro reputazione e può aumentare l'attrattività dei servizi offerti, anche agli occhi degli inserzionisti pubblicitari, accrescendo così il valore degli spazi da loro gestiti o messi a disposizione dagli editori; per gli utenti finali, poiché le pubblicazioni giornalistiche costituiscono uno strumento essenziale per l'esercizio dei diritti fondamentali e per la formazione di una consapevole percezione dei fenomeni economici, sociali e politici.[50]

In esecuzione di quanto previsto al c. 8 dell'art. 43-*bis* della l. n. 633/1941, che conferisce all'Autorità per le garanzie nelle comunicazioni il potere di adottare un regolamento per definire i criteri e le procedure per la determinazione dell'equo compenso dovuto agli editori di pubblicazioni di carattere giornalistico per l'utilizzo online delle loro opere da parte dei prestatori di servizi della società dell'informazione, il 19 gennaio 2023, AGCom ha adottato la delibera n. 3/23/CONS con cui ha approvato l'allegato "Regolamento in materia di individuazione dei criteri di riferimento per la determinazione dell'equo compenso per l'utilizzo online di pubblicazioni di carattere giornalistico di cui all'art. 43-bis della legge 22 aprile 1941, n. 633".

Il Regolamento dispone che, decorso il termine di trenta giorni dall'avvio del negoziato senza che le parti abbiano raggiunto un accordo sull'ammontare del compenso, ciascuna di esse possa adire l'Autorità per le garanzie nelle comunicazioni per la determinazione dell'equo compenso, restando impregiudicato il diritto di ricorrere all'autorità giudiziaria ordinaria. AGCom, entro sessanta giorni dalla richiesta, individua la proposta economica conforme ai criteri stabiliti dal Regolamento medesimo ovvero, qualora nessuna proposta risulti conforme, determina d'ufficio l'ammontare dell'equo compenso.

In particolare, il Regolamento AGCom: *i)* ha individuato i criteri da utilizzare per determinare l'importo dell'equo compenso (art. 4), che includono la definizione di una base di calcolo che si basa sui ricavi pubblicitari dei prestatori di servizi della società dell'informazione derivanti dall'utilizzo online delle pubblicazioni giornalistiche degli editori, al netto dei ricavi degli editori derivanti dal traffico di reindirizzamento sul loro sito web; *ii)* ha determinato un'aliquota fino al 70% da applicare alla base di calcolo per determinare l'importo dell'equo compenso, sulla base di una serie di ulteriori criteri definiti all'art. 4;[51] *iii)* ha definito i poteri ispettivi di AGCom

[50] *Ibid.*

[51] L'art. 4 del regolamento allegato alla delibera n. 3/23/CONS, rubricato "Criteri per la determinazione dell'equo compenso", prevede che: «1. L'equo compenso dovuto agli editori dai prestatori di servizi della società dell'informazione, diversi dalle imprese di

(art. 5), che può richiedere informazioni ai prestatori di servizi della società dell'informazione, imponendo a questi ultimi un corrispondente obbligo di fornire le informazioni richieste e ha previsto l'applicabilità di una sanzione amministrativa pecuniaria a carico dei soggetti inadempienti fino all'1% del fatturato realizzato sul mercato nazionale nell'ultimo esercizio chiuso anteriormente alla notifica della contestazione; *iv)* ha, infine, disciplinato (artt. 8-12) la procedura per richiedere ad AGCom di determinare l'importo dell'equo compenso e le regole del relativo procedimento, con possibilità per l'Autorità di deliberarne unilateralmente l'ammontare (art. 12).

Tuttavia, il Regolamento dell'Autorità è stato messo in discussione da Meta Platforms Ireland Limited con ricorso proposto dinanzi al TAR del Lazio, sez. IV, per l'annullamento della delibera AGCom n. 3/23/CONS.

---

media monitoring e rassegne stampa, per l'utilizzo online di pubblicazioni di carattere giornalistico è calcolato sulla base dei ricavi pubblicitari del prestatore derivanti dall'utilizzo online delle pubblicazioni di carattere giornalistico dell'editore, al netto dei ricavi dell'editore attribuibili al traffico di reindirizzamento generato sul proprio sito web dalle pubblicazioni di carattere giornalistico utilizzate online dal prestatore.

2. La modalità di determinazione della base di calcolo di cui al comma 1 tiene conto dei meccanismi di funzionamento dei servizi del prestatore e del relativo modello di business.

3. Alla base di calcolo di cui al comma 1 si applica un'aliquota fino al 70% determinata sulla base dei seguenti criteri, considerati cumulativamente e con rilevanza decrescente:

a) numero di consultazioni online delle pubblicazioni di carattere giornalistico dell'editore sui servizi del prestatore, espresse in termini di visualizzazioni e interazioni degli utenti e rilevate in conformità a criteri di correttezza metodologica, trasparenza e verificabilità;

b) rilevanza dell'editore sul mercato, espressa in termini di audience online e rilevata su base periodica da organismi dotati della massima rappresentatività dell'intero settore di riferimento anche alla luce dei processi di convergenza multimediale, ovvero da fonti terze accreditate, le cui metodologie di

rilevazione siano corrette, trasparenti e verificabili e la cui organizzazione risponda altresì a princìpi di terzietà, autonomia e indipendenza;

c) numero di giornalisti, inquadrati ai sensi di contratti collettivi nazionali di categoria, impiegati dall'editore per la realizzazione delle pubblicazioni di carattere giornalistico diffuse online;

d) costi comprovati sostenuti dall'editore per investimenti tecnologici e infrastrutturali destinati alla realizzazione delle pubblicazioni di carattere giornalistico diffuse online;

e) costi comprovati sostenuti dal prestatore per investimenti tecnologici e infrastrutturali dedicati esclusivamente alla riproduzione e comunicazione delle pubblicazioni di carattere giornalistico diffuse online;

f) adesione e conformità, dell'editore e del prestatore, ciascuno per la propria parte, a codici di condotta, ivi inclusi i codici deontologici adottati dal Consiglio nazionale dell'ordine dei giornalisti italiani, codici etici e standard internazionali in materia di qualità dell'informazione e di fact-checking maggiormente riconosciuti;

g) anni di attività dell'editore, anche in relazione alla storicità della testata in ambito nazionale e locale.

4. Fatta salva la libertà negoziale delle parti, la base di calcolo di cui al comma 1, nonché l'aliquota e i criteri di cui al comma 3, concorrono alla determinazione dell'equo compenso da parte dell'Autorità secondo la procedura di cui al Capo IV».

Nell'ambito di tale ricorso, con sentenza del 12 dicembre 2023, n. 18790, il giudice amministrativo, ai sensi dell'art. 267 del Trattato sul funzionamento dell'Unione europea, ha rimesso alla Corte di giustizia dell'Unione europea alcune questioni pregiudiziali[52], relative all'adozione da parte degli Stati membri di obblighi imposti ai prestatori di servizi della società dell'informazione nell'ambito delle loro trattative con gli editori di giornali, interrogando la Corte di Lussemburgo sull'eventuale superamento dei limiti di cui al diritto dell'Unione e all'art. 15 della direttiva (UE) 2019/790 da parte della normativa italiana.

[52] Le questioni pregiudiziali sono indicate al paragrafo 21 della sentenza medesima come di seguito riportate: «1) se l'art. 15 EUCD possa essere interpretato come ostativo all'introduzione di disposizioni nazionali – quali quelle previste dall'art. 43-bis della legge sul diritto di autore e quelle stabilite nella Delibera AGCom 3/23/CONS – nella parte in cui:
1.a) vengono previsti obblighi di remunerazione (equo compenso), in aggiunta ai diritti esclusivi indicati dallo stesso art. 15 EUCD, a carico degli ISSP ed in favore degli editori;
1.b) vengono stabiliti obblighi, a carico dei medesimi ISSP:
- di avviare trattative con gli editori,
- di fornire agli editori stessi ed alla Autorità regolatoria le informazioni necessarie ai fini della determinazione dell'equo compenso,
- nonché di non limitare la visibilità dei contenuti dell'editore nei risultati di ricerca in attesa del perfezionamento della negoziazione;
1.c) viene conferito all'Autorità regolatoria (AGCom):
- un potere di vigilanza e sanzionatorio,
- il potere di individuare i criteri di riferimento per la determinazione dell'equo compenso,
- il potere di determinare, nel caso di mancato accordo fra le parti, l'importo esatto dell'equo compenso;
2) se l'art. 15 EUCD sia ostativo a disposizioni nazionali, quali quelle indicate al precedente punto 1), che impongono ai fornitori di servizi della società dell'informazione (ISSP) un obbligo di divulgazione dei dati, assoggettato a vigilanza da parte della stessa Autorità regolatoria nazionale, la cui inosservanza incontra l'applicabilità di misure sanzionatorie amministrative;
3) se i rammentati principi di libertà di impresa di cui agli articoli 16 e 52della Carta dei diritti fondamentali dell'Unione Europea, di libera concorrenza di cui all'art. 109 T.F.U.E. e di proporzionalità di cui all'art. 52 della Carta dei Diritti Fondamentali dell'Unione Europea, ostino a disposizioni nazionali, quali quelle precedentemente indicate, che:
3.a) introducono diritti di remunerazione in aggiunta ai diritti esclusivi di cui all'art. 15 EUCD, la cui attuazione trova corredo nella già richiamata configurazione, a carico dei fornitori di servizi della società dell'informazione (ISSP), di un obbligo di avviare trattative con gli editori, di un obbligo di fornire agli editori e/o all'Autorità regolatoria nazionale le informazioni necessarie per determinare un equo compenso, nonché un obbligo di non limitare la visibilità dei contenuti dell'editore nei risultati di ricerca in attesa di tali trattative;
3.b) conferiscono a quest'ultima:
- un potere di vigilanza e sanzionatorio,
- il potere di individuare i criteri di riferimento per la determinazione dell'equo compenso,
- il potere di determinare, nel caso di mancato accordo fra le parti, l'importo esatto dell'equo compenso».

La domanda di pronuncia pregiudiziale del giudice del rinvio italiano (causa C-797/23) risulta tuttora pendente dinanzi la Corte di giustizia.
L'Avvocato generale Maciej Szpunar, nel presentare le proprie conclusioni, ha osservato come gli editori si trovino oggi in una «posizione di vulnerabilità» di fronte alle piattaforme online e ha proposto alla Corte di giustizia UE di rispondere alle questioni pregiudiziali sollevate dal TAR del Lazio ritenendo non ostative le disposizioni di cui all'art. 15 della Direttiva Copyright alle disposizioni interne di uno Stato membro che: stabiliscono, per gli editori di giornali, il diritto a un'equa remunerazione come corrispettivo dell'autorizzazione all'utilizzo delle loro pubblicazioni da parte dei prestatori di servizi della società dell'informazione; impongono ai prestatori di servizi della società dell'informazione che intendano utilizzare tali pubblicazioni determinati obblighi in materia di trattative con gli editori, di divulgazione di informazioni e di buona fede nelle trattative; attribuiscono a un ente pubblico il potere di regolamentazione, di vigilanza e sanzionatorio, inclusa la possibilità di proporre criteri per determinare la remunerazione dovuta agli editori o l'importo di tale remunerazione*,* fatta salva la possibilità per gli editori di rifiutarsi di concedere una simile autorizzazione o di concederla a titolo gratuito; non impongano ai prestatori di servizi della società dell'informazione alcun pagamento in assenza di un collegamento con l'utilizzo effettivo di tali pubblicazioni; infine, non limitino in maniera vincolante la libertà contrattuale delle parti.[53]
Nello specifico, l'Avvocato generale ha osservato come il settore dei media, e più in particolare quello della carta stampata, debba confrontarsi con importanti sconvolgimenti dovuti alla rivoluzione digitale che traggono origine: in primo luogo, dall'evoluzione delle abitudini degli utenti, che sostituiscono la carta stampata con un accesso online ai contenuti e, al contempo, diversificano, in ambiente digitale, le fonti di tali contenuti; in secondo luogo, dalla comparsa di servizi di rassegna stampa, spesso proposti dalle grandi piattaforme online, che producono un «effetto di sostituzione», permettendo agli utenti di conoscere, sebbene superficialmente, i contenuti giornalistici senza accedere alle fonti originali, ossia ai siti dei giornali e dei periodici; infine, dalla concorrenza esercitata nei confronti dei media tradizionali da Internet, in particolare dai social media.[54] Si tratta, osserva l'Avvocato generale, di «sconvolgimenti [che] hanno portato a una drastica riduzione delle entrate degli editori di giornali, che non sono più in grado di sostenere i costi associati al loro modello economico tradizionale. Tale riduzione è dovuta sia al crollo delle vendite di copie cartacee dei giornali e dei periodici sia alla perdita di introiti pubblicitari, ormai

[53] Conclusioni dell'Avvocato generale Maciej Szpunar presentate il 10 luglio 2025, causa C-797/23.

[54] *Ibid.*

raccolti, in particolare, dalle grandi piattaforme online».[55]
Tuttavia, le conseguenze della crisi dei media tradizionali non sono solo di ordine economico, ma anche sociale e politico, giacché i media svolgono un ruolo fondamentale nel funzionamento delle società democratiche e costituiscono la principale fonte informativa affidabile per il grande pubblico nonché lo strumento più efficace per garantire il controllo da parte dell'opinione pubblica sull'operato dei protagonisti della vita politica.[56]
Sebbene le conclusioni dell'Avvocato generale non vincolino i giudici della Corte di giustizia, esse rappresentano, nondimeno, un importante tassello nel riconoscere la necessità di riequilibrare l'asimmetria dei rapporti di forza tra piattaforme online e operatori dell'informazione.
Ciò posto, occorre evidenziare che, in attesa della pronuncia della Corte di giustizia UE sul rinvio pregiudiziale disposto dal giudice *a quo* italiano, il Regolamento di cui alla delibera n. 3/23/CONS, conformemente a quanto riconosciuto dalla giustizia amministrativa,[57] ha continuato a trovare applicazione. Ciò ha consentito ad AGCom di adottare la delibera n. 278/24/CONS, ossia il primo provvedimento con cui, per la prima volta, AGCom ha indicato la somma che un gigante del web come Microsoft Ireland Operations Limited deve versare a un editore (GEDI Gruppo Editoriale S.p.A.) per i contenuti giornalistici che il motore di ricerca Bing utilizza.[58]
Come è stato autorevolmente osservato, si tratta di una decisione estremamente importante «perché apre la strada a un riequilibrio dei rapporti di forza nel mercato dell'informazione»,[59] che contribuirà a ristabilire un equilibrio, non solo sul piano economico, ma anche sul terreno culturale, della politica dell'informazione, dei corretti contrappesi democratici. [60]
Merita infine di essere segnalata la delibera n. 180/25/CONS con cui AGCom nella riunione del 10 luglio 2025 ha adottato il provvedimento relativo all'equo compenso dovuto da Meta per l'utilizzo online delle pubblicazioni di carattere giornalistico del Gruppo Editoriale GEDI (tra cui,

[55] *Ibid.*

[56] *Ibid.*

[57] Con ordinanza dell'11 marzo 2024, n. 894, il Consiglio di Stato, ha accolto l'appello proposto da AGCom avverso la decisione cautelare del TAR del Lazio di cui alla sentenza n. 18790/2023 nella parte in cui il TAR sospendeva l'efficacia del regolamento AGCom sulla determinazione dell'equo compenso.

[58] Autorità per le garanzie nelle comunicazioni, delibera n. 278/24/CONS, recante "Determinazione dell'equo compenso ai sensi dell'articolo 12 del regolamento allegato alla delibera n. 3/23/CONS per l'utilizzo delle pubblicazioni di carattere giornalistico delle testate di GEDI Gruppo Editoriale Spa da parte di Microsoft Ireland Operations Limited", 2024.

[59] Così E. Cheli, *I giganti digitali pagino editori e redazioni. Ora regole per gli algoritmi*, cit.

[60] *Ibid.*

Repubblica e La Stampa) su Facebook. Si tratta del primo provvedimento che coinvolge un social network in cui l'Autorità, a seguito del mancato accordo tra le parti, ha esaminato le proposte economiche da esse formulate e, ritenendo che nessuna di queste fosse conforme ai criteri di cui all'art. 4 del Regolamento, ha determinato l'equo compenso spettante all'editore GEDI, in applicazione dei menzionati criteri.[61]

4. Conclusioni

Proprio per il peso delle considerazioni svolte dall'Avvocato generale e in relazione anche al contenuto della delibera AGCom, sarà interessante vedere, in tempi auspicabilmente brevi, le conclusioni a cui giungerà la Corte nella sua prossima sentenza.

Nell'attesa, giova annotare che di recente, il 5 settembre 2025, il Capo dello Stato, all'annuale incontro di Villa d'Este a Cernobbio tra imprenditori, manager e governo, riconoscendo la congruità del problema fin qui analizzato, ha lanciato un atto di accusa sul tema delle *"Giant Tech"*, parlando di «nuovo corporativismo globale» da parte di quelle che ha definito «nuove Compagnie delle Indie» impegnate in un progetto di influenza e sfruttamento coloniale. Il Presidente Mattarella, nel suo videomessaggio, ha esplicitamente parlato di «impulso di dominio di impronta neo-imperialista, letale per il futuro dell'umanità».

Nelle stesse ore Trump incontrava, tra gli altri, Mark Zuckerberg (Ceo di Meta), Sundar Pichai (Ceo di Google), Sergey Brin (co-fondatore di Google), Lisa Su (Ceo di AMD), Satya Nadella (Ceo di Microsoft), Bill Gates (fondatore di Microsoft), Tim Cook (Ceo di Apple), Sam Altman (Ceo di OpenAI) e Safra Catz (Ceo di Oracle), a conferma dei timori sull'eventualità che i titolari delle "*Giant Tech*" volessero rassicurare il presidente americano sull'appoggio che sono impegnate a garantirgli e sulla consapevolezza che hanno del potere della Casa Bianca di influire sui loro destini, sia sul terreno politico che economico.

Impegno che Trump di recente si è assunto e ha mantenuto pubblicamente rispetto a una rilevante decisione della Commissione europea. La quale, per iniziativa della sua vicepresidente Teresa Ribera, aveva comminato una sanzione di quasi tre miliardi di euro a Google perché le forme di "auto-

[61] Autorità per le garanzie nelle comunicazioni, delibera n. 180/25/CONS, recante "Determinazione dell'equo compenso ai sensi dell'articolo 12 del regolamento allegato alla delibera n. 3/23/CONS per l'utilizzo delle pubblicazioni di carattere giornalistico delle testate del Gruppo Editoriale GEDI da parte di Meta Platforms Ireland Limited", 2025.

pubblicità" del colosso violavano le norme concorrenziali dell'Unione.[62] Nelle motivazioni della decisione la Commissione ha spiegato che «Google trae la sua principale fonte di reddito dalla pubblicità. In particolare, vende pubblicità sui propri siti web e applicazioni e funge da intermediario tra gli inserzionisti che desiderano pubblicare i propri annunci on line e gli editori (siti web e app di terze parti) che possono fornire tale spazio».
Seppure siano evidenti le ripercussioni sui bilanci delle aziende editoriali europee di un simile accaparramento del mercato pubblicitario, tuttavia, questa controversia si inserisce nel contesto di una vera e propria guerra commerciale in atto tra l'Unione europea e gli Stati Uniti. E si può, dunque, capire perché la presidente Ursula Von der Leyen e il commissario al commercio Marcos Sefcovic avessero a lungo discusso con Ribera - prima ancora che Google annunciasse ricorso avverso l'ammenda - e insistito per rinviare la decisione fino alla completa attuazione dell'accordo tra UE e USA sui dazi, raggiunto il 28 luglio 2025, dopo una lunga e difficile trattativa tra la stessa Von der Leyen e il presidente degli Stati Uniti Donald Trump.
La preoccupazione, rivelatasi, purtroppo, fondata, era che Trump non avrebbe accolto favorevolmente la pesante ammenda inflitta a una delle *"Giant Tech"* americane, minacciando ritorsioni. E infatti la reazione di Trump è giunta subito dopo la comunicazione della decisione sulla pesante ammenda a Google: «Non possiamo permettere che questo accada alla brillante ingegnosità americana e, se ciò dovesse accadere, sarò costretto ad avviare un procedimento ai sensi della Sezione 301 per annullare le sanzioni ingiuriose imposte a queste aziende americane contribuenti».
Un'aperta contestazione, quella del presidente USA, ai tentativi dell'Unione europea di imporre regole ai giganti del web sul proprio territorio, che lascia temere come, nel caso in cui la sentenza della Corte di giustizia possa - anche in parte - ripercorrere le conclusioni dell'Avvocato generale e quella della Commissione riguardante Google, l'attuazione della stessa possa incontrare serie difficoltà.

[62] Commissione europea, *Case AT.40670-Googlr-Adtech & Data-related practices*, Bruxelles, 2025.

Abstract

Nella odierna "*speed democracy*" i giganti digitali guidano e trasformano sulla Rete la diffusione delle informazioni vere, controllate, false. In tale contesto, il contributo si propone di esaminare le sfide poste dalle "*Giant-tech*" alla tutela del pluralismo informativo e del diritto d'autore attraverso la disamina dell'art. 15 della direttiva (UE) 2019/790, cd. "Direttiva Copyright", e del suo recepimento nell'ordinamento italiano. Il lavoro analizza, pertanto, il ruolo svolto dall'equo compenso nel riequilibrare l'asimmetria normativa e informativa tra piattaforme online e operatori dell'informazione, al fine di garantire, in ultima analisi, un'informazione pluralista e sostenibile.

In today's "speed democracy" digital platforms guide and transform the spread of information - both true and false - on the Internet. This contribution aims to examine the challenges posed by "Giant-tech" to the safeguarding of information pluralism and copyright. It aims to do so through the examination of art. 15 of Directive (EU) 2019/790, so-called "copyright directive", and its transposition into the Italian legal system. The paper examines the role played by fair compensation in rebalancing the regulatory and information asymmetry between online platforms and the media/information professionals, in order to ensure a pluralistic and sustainable information ecosystem.

Keywords

platforms – media pluralism – copyright – Directive (EU) 2019/790 – fair remuneration

La *governance* della cibersicurezza nell'era digitale: una rilettura costituzionale globale*

Omar Caramaschi

Sommario

1. Premessa: la cibersicurezza nello spazio cibernetico – 2. Il ruolo dell'Unione europea nell'ambito della sicurezza digitale – 3. La dimensione internazionale della cibersicurezza – 4. È possibile una *governance* (costituzionale) globale della cibersicurezza?

1. Premessa: la cibersicurezza nello spazio cibernetico

La digitalizzazione globale e la sempre maggiore interconnessione digitale hanno determinato l'avvio di una serie di processi e di cambiamenti riguardanti anche la dimensione costituzionale degli ordinamenti giuridici, non solo interessando le dinamiche organizzative degli apparati statali, ma toccando più nel profondo la tutela e la garanzia dei diritti fondamentali, i quali sempre più spesso si trovano esposti a rischi – come gli attacchi cibernetici – provenienti proprio dal mondo digitale e dal ciberspazio[1].
Viene così in evidenza la sicurezza cibernetica, la quale ha visto una rapida sostituzione semantica di espressioni più tecniche e legate alla natura informatica del tema quali "computer security" o "information security" da parte di quella, oggi sicuramente predominante, di "cybersecurity"[2] (o,

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

Questo lavoro è stato finanziato dal progetto NextGenerationEU "Security and Rights in CyberSpace" (SERICS). L'articolo costituisce una versione ampliata e rivista della relazione presentata alla VI Conferenza italiana di ICON-S (Cagliari 3-4 ottobre 2025).

[1] Cfr. A. Venanzoni, *L'ordine costituzionale della cybersecurity*, in *Forum di Quaderni Costituzionali*, 4, 2024, 34; R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), *La sicurezza nel cyberspazio*, Milano, 2023, 9 ss.

[2] Su tale espansione cfr. R. Brighi - P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 21, 2021, spec. 20, i quali richiamano lo studio di M. Veale - I. Brown, *Cybersecurity*,

come nel prosieguo, cibersicurezza), nella quale il concetto di sicurezza informatica come protezione delle reti e dei sistemi informatici digitali allarga considerevolmente il proprio perimetro di significato. Sicché tale concetto si è evoluto – e continuerà a farlo in ragione della rapida mutabilità del contesto informatico-digitale – pur senza giungere ad una nozione condivisa dalle istituzioni e dalla dottrina giuridica[3].

Un contributo fondamentale è stato quello dell'Unione europea, la quale, in diversi atti che vedremo nel prosieguo, ha fortemente determinato un ampliamento concettuale della definizione di cibersicurezza fino ad arrivare a ricomprendere le «attività necessarie per proteggere i sistemi di rete e di informazione, gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche»[4]. In questa direzione, quindi, parrebbe individuarsi un'evoluzione della stessa cibersicurezza da sicurezza informatica di reti e sistemi digitali a strumento di tutela dell'ordine costituzionale come

in *Internet Policy Review*, 9, 2020, dal quale emerge come "cybersecurity" risulti essere il concetto più diffuso sia nelle pubblicazioni accademiche sia in diversi ambiti come l'ingegneria, le relazioni internazionali e la sicurezza pubblica, in ciò avendo superato termini decisamente più tecnici come "*computer security*", "*system security*" o "*information security*". R. Brighi - P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, cit., spec. 19, osservano inoltre come l'espressione "computer security" faccia riferimento «a una visione originaria di sicurezza informatica intesa come protezione del computer o, più in generale, del sistema informatico, dei suoi apparati, dei programmi informatici, delle infrastrutture e dei dati elaborati e trasmessi. Successivamente, nella "società dei dati", si è approdati a un concetto di sicurezza maggiormente orientato alla protezione delle informazioni, la c.d. information security».

[3] In dottrina v. *ex multis* G. D'Angelo - G. Giacomello, *Cybersicurezza*, Bologna, 2023; G. Ziccardi, *La cybersecurity nel quadro tecnologico (e politico) attuale*, in G. Ziccardi - P. Perri (a cura di), *Tecnologia e diritto*, Milano, 2019, 207 ss.; M.A. Rizzi - F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 2, 2024, 115-136; T. Stevens, *Global Cybersecurity: New Directions in Theory and Methods*, in *Politics and Governance*", 2, 2018; C. Lotta, *Governance della rete, accesso a Internet e cybersicurezza*, Napoli, 2024.

[4] Art. 2, regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»). In maniera analoga il legislatore italiano con il decreto-legge 14 giugno 2021, n. 82 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale), come convertito dalla legge 4 agosto 2021, n. 109, il quale definisce la cibersicurezza come «l'insieme delle attività […] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» (art. 1, c. 1, lett. a).

precondizione essenziale per garantire non solo l'ordinata convivenza, e quindi la sopravvivenza di qualsiasi ordinamento giuridico[5], proprio attraverso «la riaffermazione ordinamentale della sicurezza digitale»[6], ma anche – così come vale in generale per tutto ciò che avviene nel ciberspazio – in qualità di elemento fondamentale per il godimento dei diritti fondamentali dell'uomo[7].

La cibersicurezza non riguarda più soltanto le minacce provenienti dalla dimensione fisica, ma allarga il proprio orizzonte di riferimento includendo quelle del mondo virtuale del ciberspazio[8]; in questo modo, viene meno la distinzione tra sicurezza esterna ed interna[9], in ragione del fatto che le minacce alla cibersicurezza possono provenire da un numero inesauribile di fonti diverse, quindi, per esempio, da attori pubblici come altri Stati ovvero da privati come imprese, società e finanche persone fisiche dotate degli strumenti e delle capacità tecniche adeguate indipendentemente dalla loro residenza fisica e territoriale[10].

Proprio per queste ragioni la cibersicurezza assume una portata trasversale, interessando i singoli individui, le imprese, la società nel suo complesso, ma anche gli Stati e gli organismi sovranazionali e internazionali[11]. Ed è proprio a questi ultimi livelli che la cibersicurezza richiede un'azione istituzionale e regolativa opportunamente in grado di rispondere alle sfide e alle minacce provenienti dallo spazio cibernetico e dal mondo digitale. Sebbene la risposta a tali nuovi elementi problematici dovrebbe partire proprio dagli Stati e dagli strumenti costituzionali a loro disposizione[12],

---

[5] Cfr. M. Matassa, *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, cit., spec. 21.

[6] Cfr. A. Venanzoni, *L'ordine costituzionale della cybersecurity*, cit., 35-36.

[7] Cfr. L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 14, 2024, 179, secondo il quale «tutelare la sicurezza nel cyberspazio è oramai indispensabile per garantire il pieno godimento dei diritti fondamentali nella realtà virtuale», come, ad esempio, la libertà di manifestazione del pensiero, l'identità personale, la libertà del voto ovvero la riservatezza e il diritto all'immagine.

[8] Cfr. S. Savaş - S. Karataş, *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance*, in *International Cybersecurity Law Review*, 3, 2022, 11-12; secondo S.A. Salvaggio - N. Gonzàlez, *The European framework for cybersecurity: strong assets, intricate history*, in *International Cybersecurity Law Review*, 4, 2023, 142, «*[t]he realms of cybersecurity and traditional security have been merged into one*».

[9] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, in *Global Constitutionalism*, 1, 2018, 112 ss., spec. 117.

[10] Cfr. L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, cit., 182-183.

[11] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 117.

[12] Cfr. L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, cit., 185-186.

non può non osservarsi come i singoli Stati siano difficilmente in grado di garantire le condizioni essenziali per la "sicurezza dei diritti"[13] dei cittadini nella dimensione del ciberspazio, essendo invece necessario rispondere alle sfide globali derivanti per la cibersicurezza con forme di cooperazione sovrastatali e altrettanto globali al fine di rendere consistente la sicurezza nello spazio cibernetico ed effettiva la tutela dei diritti fondamentali anche nel nuovo mondo digitale[14]. Sicché viene così in evidenza l'obiettivo che si intende perseguire in questa sede, vale a dire quello di fornire un contributo che indaghi la portata globale della cibersicurezza, partendo dal livello eurounitario per muovere verso quello internazionale e globale, con particolare riguardo alle relative forme di regolazione e specialmente alla possibilità di sviluppare modelli di *governance* costituzionale della cibersicurezza di portata globale, mantenendo tuttavia una prospettiva di analisi e un metodo di ricerca propri del diritto costituzionale e del costituzionalismo, in una sorta di rilettura della cibersicurezza attraverso le lenti del costituzionalismo globale.

2. Il ruolo dell'Unione europea nell'ambito della sicurezza digitale

Come si diceva poc'anzi, le sfide multidimensionali poste dalla cibersicurezza non possono essere affrontate dai singoli Stati, proprio per la natura globale e reticolare della sicurezza digitale e informatica (nonché delle minacce per la stessa), ma richiedono necessariamente il protagonismo degli organismi sovranazionali e, come vedremo, internazionali e globali.
Se vogliamo procedere in via incrementale, e anche secondo una modalità di analisi cronologicamente coerente, occorre muovere dalla posizione dell'Unione europea, che negli ultimi anni ha ricoperto un ruolo determinante nel panorama normativo[15], di fatto occupandosi della sicurezza digi-

[13] Su questa particolare e condivisibile concezione v. per tutti M. Rutolo, *Sicurezza, dignità e lotta alla povertà. Dal "diritto alla sicurezza" alla "sicurezza dei diritti"*, Napoli, 2012.

[14] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 117; L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, cit., 186.

[15] Secondo F. Pizzetti, *Introduzione alla regolazione europea della società digitale*, in Aa. Vv., *La regolazione europea della società digitale*, Torino, 2024, 4, ciò avrebbe determinato un'espansione globale dell'azione dell'Unione europea, in maniera analoga a quanto avvenuto in materia di dati personale con il GDPR o potrebbe avvenire, secondo alcuni, con l'AI Act, nella logica del cd. effetto Bruxelles (sul punto v. A. Bradford, *The Brussel Effect. How the European Union Rules the World*, Oxford, 2020). Sul punto v. anche Z. Bederna - Z. Rajnai, *Analysis of the cybersecurity ecosystem in the European Union*, in *International Cybersecurity Law Review*, 2, 2022, 35 ss.; G. Cassano - M. Iaselli - G. Spangher, *Cybersecurity: contesto normativo di riferimento a livello nazionale ed europeo*, in *Diritto di internet*, 4, 2022, 637 ss.

tale nel suo essere «ambito trasversale»[16] e coordinando la disciplina della cibersicurezza con la regolazione di altri ambiti che, in particolare, avendo come strumento comune quello della Rete, si collegano più o meno direttamente ad essa come la protezione dei dati personali, il mercato digitale o l'intelligenza artificiale[17].

Proprio al fine di rendere effettiva la tutela dei diritti fondamentali anche nello spazio cibernetico attraverso forme adeguate di cibersicurezza, pare necessario indagare quali strumenti siano stati approntati dall'Unione europea e dagli Stati membri al fine di disegnare una *governance* della cibersicurezza in grado di assolvere a tali compiti; in questa direzione troviamo numerosi atti europei che verranno ora passati in rassegna con l'intento di meglio ricostruire l'architettura istituzionale europea della sicurezza informatica e digitale.

I primi atti europei strategici e di indirizzo, sostanzialmente di *soft law* e in qualche modo collegati con la cibersicurezza, fanno la loro comparsa all'inizio degli anni 2000[18], laddove viene offerta una panoramica generale delle principali minacce provenienti dallo spazio cibernetico, tuttavia il termine cibersicurezza – o meglio "cybersecurity" – verrà impiegato ufficialmente solo qualche anno più tardi nella relazione pubblicata nel 2008 sull'implementazione della "Strategia europea in materia di sicurezza" del 2003[19].

In questa prima fase la legislazione europea si segnala per la creazione da

[16] D. Marrani, *Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia*, in *Freedom, Security & Justice: European Legal Studies*, 1, 2021, spec. 80.

[17] Cfr. G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, in *Rivista italiana di informatica e diritto*, 2, 2025, spec. 12. Si pensi quindi al GDPR, al Digital Markets Act, al Digital Services Act ovvero all'Ai Act, collegati anche da un comune approccio di natura costituzionale come osservato da O. Caramaschi, *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?*, in *Rivista italiana di informatica e diritto*, 1, 2025, 29-51.

[18] Si pensi alla Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni - Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica del 26 gennaio 2001, COM(2000) 890 def., nonché alla Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo del 6 giugno 2001, COM (2001) 298 def., laddove la sicurezza delle reti e dell'informazione viene identificata «come la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema» (par. III).

[19] Consiglio dell'Unione europea, Relazione sull'attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione (S407/08), 11 dicembre 2008.

parte del regolamento (CE) 2004/460 dell'Agenzia europea per la sicurezza delle reti e dell'informazione (meglio nota con l'acronimo "ENISA" da European Network and Information Security Agency)[20], con lo scopo di garantire un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità europea[21]. Questa struttura – oggi ridenominata Agenzia dell'Unione europea per la cibersicurezza – ha ricoperto un ruolo più formale che sostanziale, fino all'approvazione della Strategia europea per la cibersicurezza del 7 febbraio 2013[22], che ha dato nuovo impulso all'approccio europeo alla sicurezza digitale[23], delineando una visione europea in materia di cibersicurezza sempre più articolata, con una particolare e mirata attenzione alla tutela dei diritti fondamentali e della privacy da perseguirsi attraverso una nuova *governance* multilivello e *multistakeholder* in grado di coniugare democraticità, efficienza e responsabilità condivisa dei vari attori coinvolti, altresì proponendo alcuni strumenti pratici per poter raggiungere gli obiettivi posti in tema di sicurezza cibernetica[24].

---

[20] Su questa prima fase anteriore al 2013 v. in particolare in dottrina B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *Federalismi.it*, 14, 2020, 11-45; E. Longo, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in Aa. Vv., *La regolazione europea della società digitale*, cit., 209 ss.

[21] Regolamento (CE) 2004/460 del Parlamento europeo e del Consiglio del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione; art. 1.1.

[22] Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, JOIN/2013/01 final. Sulla Strategia il Parlamento europeo ha adottato la Risoluzione del 12 settembre 2013 sulla strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro (2013/2606(RSP)), nella quale il Parlamento europeo, condividendo il contenuto della Strategia, formula alcune indicazioni; in particolare «sottolinea la necessità di sviluppare una politica di comunicazione strategica in materia di cibersicurezza nell'UE, situazioni di crisi cibernetica, revisioni strategiche, collaborazione pubblico-privato e segnalazioni, nonché raccomandazioni destinate al pubblico» (punto 3) e «invita nuovamente gli Stati membri ad adottare, senza indebito ritardo, strategie nazionali per la cibersicurezza che coprano gli aspetti tecnici e quelli relativi al coordinamento, alle risorse umane e alla dotazione finanziaria e comprendano regole specifiche sui benefici e le responsabilità del settore privato, al fine di garantire la partecipazione di quest'ultimo, nonché a prevedere procedure complete per la gestione del rischio e a salvaguardare il quadro normativo» (punto 5).
In particolare, a seguito della Strategia per la cibersicurezza, è stato approvato il regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio del 21 maggio 2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004.

[23] Secondo G. Borriello - G. Fristachi, *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in *Rivista di Digital Politics*, 1-2, 2022, 162, il 2013 rappresenta «l'anno spartiacque in termini di avanzamento cibernetico a livello comunitario».

[24] Cfr. C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, in *Quaderni*

Inizia così a prospettarsi l'impegno delle istituzioni europee quanto alla necessità di regolazione del ciberspazio al fine di tutelare i diritti fondamentali e i valori basilari per l'ordinamento giuridico europeo, non solo mostrandosi in ciò già ben consapevoli della pluralità di soggetti, pubblici e (sempre più) privati, coinvolti nel funzionamento dello spazio cibernetico, ma anche nell'evidenziare l'importanza della dimensione internazionale della cibersicurezza attraverso un nuovo ruolo per la diplomazia internazionale[25], la quale a sua volta contribuirebbe a formare una politica estera dell'Unione europea più coesa in materia di ciberspazio, volta a promuovere i valori europei fondamentali[26].

Sulla base di questa prima strategia europea sulla cibersicurezza viene approvata nel 2016 la Direttiva (UE) 2016/1148, cd. Direttiva NIS (Network and Information Security)[27] con la finalità di raggiungere un elevato livello comune di sicurezza delle reti e dei sistemi informativi, in particolare attraverso il conseguimento di un livello minimo di cibersicurezza in ciascuno Stato membro. Come esplicitato anche dal successivo regolamento di esecuzione (UE) 2018/151[28], lo scopo era il coinvolgimento di tutti gli attori

IAI, 2014, 35 ss.

[25] Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, in *Rivista AIC*, 4, 2022, 7.

[26] La Strategia prevede, a tal proposito, che l'Alto rappresentante si occupi, insieme agli Stati membri e all'Agenzia europea per la difesa, di «curare il dialogo con i partner internazionali, in particolare la NATO, con altre organizzazioni internazionali e centri di eccellenza multinazionali, per garantire capacità efficaci di difesa, individuare settori di cooperazione ed evitare duplicazioni degli sforzi» (punto 2.3); inoltre l'Unione europea è chiamata «ad elaborare una politica internazionale dell'UE in materia di ciberspazio coerente e mirante ad aumentare l'impegno e a intensificare le relazioni con i principali partner e le principali organizzazioni internazionali […] come il Consiglio d'Europa, l'OCSE, le Nazioni Unite, l'OSCE, la NATO, l'UA, l'ASEAN e l'OSA» (punto 2.5).
Inoltre, come ricorda E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, cit., 7, lo studio della Commissione europea *International Cyber Capacity Building: Global Trends and Scenarios*, pubblicato il 23 settembre 2021 dallo EU Institute for Security Studies, avrebbe evidenziato come tra le capacità fondamentali di cui uno Stato necessita per godere di una discreta sicurezza cibernetica ci sia una tendenza favorevole verso quelle legate alle relazioni internazionali nel ciberspazio, inclusa «*the capacity to develop and act upon an understanding of how international law applies in cyberspace, norms of responsible state behaviour and confidence building measures*», nonché quella «*to engage in the international cyber diplomacy around these issues, for example in the UN Open-Ended Working Group and UN Group of Government Experts*» (sul punto v. *infra*).

[27] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[28] Regolamento di esecuzione (UE) 2018/151 della Commissione del 30 gennaio 2018 recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori

(sia pubblici sia privati) interessati all'elaborazione delle strategie europea e nazionali per la cibersicurezza, nonché, specialmente attraverso la cooperazione a livello nazionale, al conseguimento della "resilienza cibernetica" nell'intero territorio europeo, in modo da tutelare tanto il mercato unico europeo quanto i diritti fondamentali dei cittadini[29].

Tale prospettiva di risultato richiedeva il coinvolgimento dei principali soggetti destinatari della normativa europea, in particolar modo degli Stati ai quali venivano affidati diversi obblighi tra i quali quello di elaborare strategie nazionali in materia di cibersicurezza – sulla base di contenuti minimi indicati dalla Direttiva NIS, in una precisa logica di armonizzazione a livello europeo – le quali dovevano non solo determinare obiettivi e priorità della strategia nazionali, ma anche definire «un quadro di *governance* per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti»[30]; quello di designare una o più autorità nazionali responsabili della sicurezza delle reti e dei sistemi informativi (cd. Autorità NIS) al fine di controllare l'applicazione della Direttiva a livello nazionale[31]; nonché, infine, l'istituzione di gruppi di intervento per la sicurezza informatica in caso di incidenti informatici (cd. CSIRT, ossia *Computer Security Incident Response Team*)[32].

Anche sulla base di questi sviluppi normativi si è giunti all'adozione della seconda Strategia in materia di cibersicurezza[33], nella quale si anticipava la necessità di riformare l'ENISA – che fino a quel momento aveva rappresentato uno dei principali sforzi dell'Unione europea per istituzionalizzare

di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.

[29] Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, cit., 7-8.

[30] Direttiva (UE) 2016/1148, art. 7; si prevede inoltre che le strategie nazionali debbano individuare «misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato»; indicare «programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi», «un piano di valutazione dei rischi per individuare i rischi», nonché «un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi».

[31] Direttiva (UE) 2016/1148, art. 8; nonché la designazione di «un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi» (coincidente con l'Autorità nel caso in cui questa fosse unica), entrambi da dotare «di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva».

[32] Direttiva (UE) 2016/1148, art. 9.

[33] Comunicazione congiunta al Parlamento europeo e al Consiglio - Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, JOIN(2017) 450 final.

il processo legislativo in materia di cibersicurezza[34] – come poi effettivamente avvenuto con il regolamento (UE) 2019/881[35] (cd. Cybersecurity Act o Regolamento sulla cibersicurezza), il quale ha, di fatto, rideterminato obiettivi, funzioni, poteri e aspetti organizzativi della ridenominata Agenzia dell'Unione europea per la cibersicurezza[36], nonché individuato un quadro comune europeo per l'introduzione di sistemi di certificazione non soltanto per garantire un livello adeguato della cibersicurezza di prodotti, servizi e processi legati alle tecnologie dell'informazione e della comunicazione, ma anche con la finalità dichiarata di evitare la frammentazione del mercato interno[37] con riguardo ai sistemi europei di certificazione della cibersicurezza[38]. In particolare, quindi, l'Agenzia per la cibersicurezza viene resa permanente e ne vengono aumentate le funzioni, di natura tipicamente consultiva[39], specialmente in supporto agli Stati membri e alle istituzioni,

[34] Sull'evoluzione della normativa europea sulla cibersicurezza e, contestualmente, del ruolo svolto dell'Unione europea sul tema v. in dottrina E. Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, 2022; A. Contaldo - L. Salandri, *La disciplina della cybersecurity nell'Unione europea*, in A. Contaldo - D. Mula (a cura di), *Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020, 1 ss.

[35] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[36] Regolamento (UE) 2019/881, artt. 3 ss.

[37] Cfr. E. Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, cit., 95, la quale osserva come la politica europea in materia di cibersicurezza si collochi storicamente in una logica legata al mercato interno, più da un punto di vista teorico che pratico. In questo senso è stato principalmente il Cybersecurity Act del 2019 ad orientare la sicurezza cibernetica europea verso il mercato interno, non solo dal momento che le politiche europee in tema di cibersicurezza sono rilevanti per il funzionamento del mercato interno, per la sicurezza dei consumatori e per il funzionamento delle imprese, ma anche, in particolare, perché tale regolamento è stato adottato in virtù dell'art. 114 TFUE che costituisce la base giuridica fondamentale per il ravvicinamento e l'armonizzazione delle legislazioni nazionali a tutela del mercato interno.

[38] Cfr. art. 1 del regolamento (UE) 2019/881. In questa direzione lo stesso regolamento prevede l'istituzione di un Quadro europeo di certificazione della cibersicurezza istituito proprio «al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC» (art. 46, par. 1).

[39] Alcuni in dottrina si sono mostrati critici rispetto alla natura meramente consultiva di tali attribuzioni, sostenendo che invece «sarebbe stato preferibile attribuire all'Agenzia funzioni maggiormente incisive, in considerazione della rilevanza del bene giuridico

agli organi e agli organismi dell'Unione europea, su tutti la Commissione europea, anche in funzione di coordinamento[40], principalmente nella definizione e nell'attuazione delle politiche europee in materia di cibersicurezza, nonché del coordinamento delle stesse[41], sebbene questo incremento delle funzioni attribuite all'ENISA non sia stato accompagnato da un (necessario) incremento dei poteri, i quali, invece, si limitano ad essere consultivi e di supporto, ciò rappresentando un elemento di forte restrizione dell'effettiva efficacia dell'attività dell'agenzia stessa[42].
Tuttavia, l'impianto normativo europeo, specialmente con riguardo alla Direttiva NIS, ha mostrato alcune lacune e punti di debolezza, emersi particolarmente durante un periodo piuttosto intenso di attacchi informatici in concomitanza della pandemia e del conflitto russo-ucraino[43]. Pertanto, per incrementare il livello di coordinamento delle politiche di cibersicurezza in grado di fornire agli Stati membri ulteriori strumenti di contrasto e tutela al fine di accrescere il livello generale della cibersicurezza europea si è giunti alla riforma della Direttiva NIS con la Direttiva (UE) 2022/2555 (meglio nota come Direttiva NIS 2[44]).

---

tutelato e della crescente esigenza di sicurezza informatica all'interno del mercato unico digitale» (L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi.it*, 25, 2022, 74).

[40] Sul punto in particolare v. la successiva Cybersecurity Strategy for the Digital Decade del dicembre 2020, nella Comunicazione congiunta al Parlamento europeo e al Consiglio - La strategia dell'UE in materia di cibersicurezza per il decennio digitale, JOIN(2020) 18 final, la quale si segnala in questa sede per aver istituito la Joint Cyber Unit (o JCU) la quale costituisce una «piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cibersicurezza all'interno dell'Ue, ciò con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera» (G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, cit., 15).

[41] Art. 4 del regolamento (UE) 2019/881, laddove si asserisce, inoltre, che l'Agenzia «promuove la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato su questioni relative alla cibersicurezza», nonché, tra le altre, «contribuisce a rafforzare le capacità di cibersicurezza a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri».

[42] Cfr. F. Sanchini, *Sicurezza cibernetica e architettura istituzionale: verso una* governance *costituzionalmente orientata?*, in *Federalismi.it*, 26, 2025, 170-191, spec. 177-178.

[43] Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, cit., 8-9.

[44] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

Quest'ultima si segnala per il fatto di essere intervenuta sulle criticità relative al recepimento da parte degli Stati della precedente normativa, in particolare introducendo e rafforzando gli strumenti di cooperazione tra le autorità nazionali in una logica di armonizzazione europea[45], nonché rivedendo i settori e ampliando il novero degli operatori di servizi pubblici e privati sottoposti agli obblighi in tema di cibersicurezza[46]. Per quanto più rileva in questa sede, la Direttiva NIS 2, al fine di accrescere la cibersicurezza dell'Unione europea e ridurre le minacce ai sistemi di rete e informatici qualificati come essenziali e importanti dalla normativa stessa, si preoccupa di rafforzare notevolmente il sistema di *governance* della cibersicurezza delineato con la Direttiva NIS. In particolare, troviamo al vertice del sistema l'autorità europea rappresentata dall'ENISA, mentre al livello inferiore vi sono le autorità e gli organismi degli Stati membri; in particolare la Direttiva NIS 2 ha previsto l'istituzione di alcuni organi quali le autorità nazionali competenti NIS, le autorità di gestione delle crisi informatiche e i team di risposta agli incidenti di sicurezza informatica (CSIRT)[47]; inoltre, al fine di svolgere le funzioni di attuazione della Direttiva NIS 2 e della vigilanza quanto alla corretta applicazione delle disposizioni in essa contenute[48], alle autorità nazionali sono attribuiti importanti poteri

[45] Direttiva (UE) 2022/2555, artt. 7-13.

[46] Direttiva (UE) 2022/2555, artt. 2-3 e allegati I e II. La direttiva, in particolare, superando la distinzione precedente tra operatori di servizi essenziali e fornitori di servizi digitali, individua criteri più precisi e definiti proprio al fine di individuare tali soggetti e contestualmente ridurre la discrezionalità statale nello svolgimento di questa rilevante operazione; inoltre, viene attivata una policy di "divulgazione coordinata delle vulnerabilità" (o "*coordinated vulnerability disclosure*") affiancata dalla creazione di una banca dati europea delle vulnerabilità, prescrivendo altresì che in sede di attuazione ciascuno Stato adotti una propria regolazione interna relativa alle forme di rilevamento delle vulnerabilità dei sistemi informatici. Sul punto in dottrina v. almeno F.N. Ricotta, *Vulnerability disclosure e penetration testing: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2*, in *Rivista italiana di informatica e diritto*, 2, 2024, 82 ss.; F. Casarosa - G. Comandé, *Aspettando la NIS2: ovvero il diritto privato della cybersecurity*, in *Il Diritto dell'informazione e dell'informatica*, 1, 2024, 29 ss.; da ultimo G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, cit.

[47] Direttiva (UE) 2022/2555, art. 1, par. 2, lett. a).

[48] In questo senso v. direttiva (UE) 2022/2555, art. 1, laddove si prevede che «1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno. 2. A tal fine, la presente direttiva stabilisce: a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT); b) misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557; c) d) norme e

di controllo[49]. L'architettura istituzionale europea così delineata e il ruolo delle autorità nazionali competenti NIS con riguardo alla loro rilevanza quanto alle strategie europee in tema di cibersicurezza dovrebbero richiedere un'attuazione uniforme a livello nazionale; tuttavia, già a seguito della Direttiva NIS, la quale all'art. 8 aveva previsto per prima l'istituzione delle autorità nazionali competenti, vi è stata un'applicazione delle disposizioni piuttosto eterogenea tra gli Stati membri[50].

Senza entrare nel merito di tale questione, si ritiene utile focalizzare soltanto brevemente l'attenzione quantomeno sull'architettura istituzionale derivata da tale normativa europea nell'ordinamento italiano, il quale rientra nel gruppo di Stati che hanno attribuito il ruolo di autorità nazionale competente NIS ai vertici dell'esecutivo ovvero a un'agenzia ad esso in qualche misura riconducibile. Inizialmente sono state attribuite al Presidente del Consiglio dei ministri importanti prerogative in tema di sicurezza cibernetica, in particolare quanto alla predisposizione della strategia nazionale in materia di cibersicurezza, ricoprendo un ruolo apicale anche in veste, almeno in un primo periodo, di autorità nazionale competente NIS[51]. Un

obblighi in materia di condivisione delle informazioni sulla cibersicurezza; obblighi in materia di vigilanza ed esecuzione per gli Stati membri». Inoltre, l'art. 8, par. 2, della stessa direttiva stabilisce che le autorità nazionali competenti «controllano l'attuazione della presente direttiva a livello nazionale».

[49] Direttiva (UE) 2022/2555, art. 32, par. 2.

[50] In dottrina v. A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Rivista del Gruppo di Pisa*, 3, 2021, 532 ss.; L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, cit., 186 ss. Si possono individuare tre gruppi di Stati: un primo gruppo ha affidato il ruolo di autorità nazionale competente NIS a organici tecnici di regolazione ovvero a svariate autorità amministrative indipendenti (ad es. Lussemburgo, Cipro); un secondo gruppo ha invece assegnato tale ruolo a Ministeri ovvero ad organismi collegati direttamente ad essi (ad es. Irlanda, Germania); un terzo gruppo, infine, ha conferito il ruolo di autorità nazionale competente direttamente al vertice del Governo ovvero a un'agenzia governativa dipendente da esso (ad es. Francia, Italia).

[51] Così è stato con l'approvazione della legge 7 agosto 2012, n. 133 "Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto" e con il d. lgs. 18 maggio 2018, n. 65 di recepimento della Direttiva NIS, rubricato "Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione", il quale agli artt. 6 e 7 affidava al Presidente del Consiglio dei ministri l'adozione della strategia nazionale di cibersicurezza mentre ad alcuni Ministeri il ruolo di autorità competente NIS in base al settore di riferimento (così al Ministero dello sviluppo economico per il settore energia; al Ministero delle infrastrutture e dei trasporti per il settore trasporti; al Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari; al Ministero della salute per l'attività di assistenza sanitaria; al Ministero dell'ambiente e della tutela del territorio e del mare e alle Regioni e alle Province autonome di Trento e di Bolzano in merito al settore fornitura e distribuzione di acqua potabile).

tale impianto istituzionale è stato modificato con l'istituzione dell'Agenzia per la cybersicurezza nazionale (o cd. ACN)[52] indicata come autorità nazionale competente NIS, la quale rappresenta uno degli elementi fondamentali della *governance* italiana della cibersicurezza proprio laddove è chiamata a dare attuazione alla strategia nazionale di sicurezza cibernetica adottata dal Presidente del Consiglio dei ministri[53], il quale esercita la propria influenza sull'Agenzia[54] già a partire dalla nomina – ed eventualmente revoca – dei vertici della stessa[55].

In sostanza, ciò che emerge dalla normativa interna e dall'architettura istituzionale che ne è derivata, anche a seguito delle più recenti modifiche normative intervenute con la legge 28 giugno 2024, n. 90 in materia di rafforzamento della cibersicurezza nazionale[56] e con il d. lgs. 4 settembre 2024, n. 128 di recepimento della Direttiva NIS 2[57], è un significativo ac-

[52] Questo cambiamento è avvenuto con il d.l. 14 giugno 2021, n. 82, convertito con modificazioni dalla l. 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale". Sul punto in dottrina v. almeno F. Serini, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 12, 2022, 241 ss.; per quanto riguarda l'Agenzia v. per tutti I. Forgione, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, cit., 106 ss.

[53] Cfr. art. 2, c. 1, lett. b) del d.l. 14 giugno 2021, n. 82, laddove inoltre si prevede il parere del Comitato interministeriale per la cybersicurezza (v. art. 4, c. 2).

[54] Secondo T.F. Giupponi, *Il governo nazionale della cybersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277-304, spec. 297, il ruolo dell'Agenzia per la cybersicurezza nazionale risulta «sostanzialmente strumentale» con riguardo «alle competenze della Presidenza del Consiglio in materia di cybersicurezza».

[55] Cfr. art. 2, c. 1, lett. c), del d.l. 14 giugno 2021, n. 82.

[56] In dottrina v. almeno A. Iannuzzi, *Considerazioni sul disegno di legge "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717)*, in *Rivista italiana di informatica e diritto*, 1, 2024, 59-63; E. Longo, *Audizione informale per il disegno di legge in materia di "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" (AC 1717)*, ivi, 66-70.

[57] D. lgs. 4 settembre 2024, n. 138 "Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148". Inoltre, tra la principale normativa di attuazione si segnalano: DPCM 9 dicembre 2024, n. 221 "Regolamento per la definizione dei criteri per l'applicazione della clausola di salvaguardia di cui all'articolo 3, commi 4 e 12, del decreto legislativo del 4 settembre 2024, n. 138, di recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148"; DPCM 30 aprile 2025 "Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale"; DPCM 2 ottobre 2025 "Modifica del decreto del

centramento di poteri e attribuzioni attorno all'esecutivo e particolarmente al Presidente del Consiglio dei ministri, con ciò determinandosi una rilevante questione circa la portata del controllo parlamentare che viene esercitato in questo specifico ambito[58]. La funzione parlamentare di controllo nei confronti del potere esecutivo è stata rafforzata – rispetto ai classici strumenti previsti in via ordinaria come interrogazioni, interpellanze, mozioni, inchieste, indagini conoscitive ovvero audizioni in sede di commissioni – dallo stesso legislatore italiano, il quale ha individuato nel Comitato parlamentare per la sicurezza della Repubblica (cd. COPASIR[59]) l'organo di derivazione parlamentare in grado di svolgere la funzione di controllo sul Governo nell'esercizio dell'attività di indirizzo politico in tema di cibersicurezza, in modo particolare attraverso diverse attribuzioni ad esso appositamente assegnate[60]. Tuttavia, un tale impianto presenta alcune criticità quanto all'effettiva capacità di questo organo di controbilanciare adeguatamente l'accentramento di poteri in capo all'esecutivo attraverso un'opportuna ed efficace azione di controllo in tema di sicurezza digitale in grado di offrire maggiore trasparenza e democraticità alla complessiva *governance* della cibersicurezza[61].

Presidente del Consiglio dei ministri 30 aprile 2025, concernente la disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale".

[58] Cfr. F. Sanchini, *Sicurezza cibernetica e architettura istituzionale: verso una* governance *costituzionalmente orientata?*, cit., 179-180; T.F. Giupponi, *Il governo nazionale della cybersicurezza*, cit., 287 ss. e 295 ss.; L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, cit., 191 ss.

[59] Su questi aspetti v. A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., 541 ss.; O. Caramaschi, *La cybersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in *Osservatorio costituzionale*, 4, 2022, 77 ss.

[60] Cfr. d.l. 14 giugno 2021, n. 82; tra queste troviamo il potere di chiedere l'audizione del Presidente dell'ACN (art. 5, c. 6) e di esprimere pareri sull'adozione di alcuni atti, quali i regolamenti che riguardano l'organizzazione dell'ACN (art. 6, c. 3); il regolamento di contabilità dell'ACN (art. 11, c. 3); le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'ACN (art. 11, c. 4); disciplina del contingente di personale addetto all'ACN (art. 12, c. 8). Inoltre, viene previsto che ogni anno entro il 30 giugno il Presidente del Consiglio dei ministri trasmetta al COPASIR una relazione annuale sulle attività svolta dall'ACN negli ambiti relativi alla tutela della sicurezza nazionale nello spazio cibernetico con riguardo ai profili di competenza del Comitato (art. 14, c. 2); contestualmente occorre notare, per completezza, che si prevede altresì che entro il 30 aprile di ogni anno il Presidente del Consiglio dei ministri debba trasmettere una analoga relazione in materia di cibersicurezza nazionale al Parlamento (art. 14, c. 1).

[61] Le principali criticità riguardano la composizione ristretta del COPASIR e la segretezza che ne contraddistinguono i lavori, nonché il fatto di operare secondo il principio di riservatezza, subendo in questo senso il ruolo del Presidente del Consiglio dei ministri che può rappresentare un limite all'azione dell'organo quanto ad efficacia e trasparenza, per

Tornando brevemente e conclusivamente al quadro giuridico e istituzionale europeo in tema di cibersicurezza – negli ultimi anni arricchito da ulteriori atti di rilievo[62] – tra i vari elementi di interesse che emergono (come, ad esempio, la protezione dei diritti fondamentali ovvero il coinvolgimento degli attori fondamentali del settore sia pubblici sia privati[63]),

esempio nell'accesso a documenti riservati per ragioni di sicurezza ovvero nell'esercizio di talune attività ispettive.

In dottrina cfr. E. Longo, *Il diritto costituzionale e la cybersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, 2, 2024, 340 ss., il quale osserva come a fronte di un aumento dei poteri del Presidente del Consiglio dei ministri il controllo svolto dal COPASIR non risulti «adeguato a garantire un sufficiente livello di trasparenza necessario in questi ambiti»; F. Sanchini, *Sicurezza cibernetica e architettura istituzionale: verso una* governance *costituzionalmente orientata?*, cit., 181-183; A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., spec. 542, il quale ritiene che il ruolo del COPASIR sia «limitante rispetto alla vastità di ambiti cui ormai presiede e limitato tanto nella composizione che nelle forme di pubblicità»; L. Moroni, *La governance della cybersicurezza a livello interno ed europeo: un quadro intricato*, cit., 186 ss., 192-193, il quale individua alcuni interventi del legislatore che potrebbero ovviare alle criticità emerse, in particolare la «previsione di audizioni parlamentari pubbliche semestrali o quadrimestrali dell'ACN» ovvero «l'istituzione di nuova commissione parlamentare bicamerale ad hoc di controllo sull'attività del Governo, la cui maggiore rappresentatività della composizione e pubblicità dei lavori garantiscano una adeguata conoscenza delle decisioni assunte in materia di cybersicurezza».

[62] Si pensi alla direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio del 14 dicembre 2022 che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario (sul punto v. anche il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011) ovvero alla direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, nonché al regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i Regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) e al regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio del 19 dicembre 2024 che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà).

Quanto al rapporto tra Cyber Resilience Act e Artificial Intelligence Act v. F. Bagni, *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, in *Rivista italiana di informatica e diritto*, 2, 2023, 201-217, mentre con riguardo agli altri atti europei in tema di cibersicurezza v. P.G. Chiara, *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali*, in *Rivista italiana di informatica e diritto*, 1, 2023, 143 ss.

[63] Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional*

quello che qui più rileva è il rapporto tra *governance-government* nella relazione tra Unione europea e Stati membri[64]. Gli atti europei sulla cibersicurezza riaffermano più volte che, in molti ambiti e con riferimento a diversi profili, l'ordinamento dell'Unione europea rispetta la sovranità e la discrezionalità politica degli Stati membri[65], in maniera conforme ai Trattati, i quali stabiliscono, come è noto, che l'Unione europea rispetta le funzioni essenziali dello Stato, con particolare riguardo alle «funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro»[66]. Si tratta quindi di un ambito competenziale nel quale gli Stati godono di una discreta autonomia nell'adottare le misure ritenute idonee per proteggere beni e valori essenziali dei propri ordinamenti giuridici e, contestualmente, nel definire le Strategie di sicurezza nazionali e le rispettive strutture amministrative dedicate. Di converso si determina come il ruolo dell'architettura istituzionale europea – su tutti si pensi all'Agenzia dell'Unione europea per la cibersicurezza (ENISA)[67] – sia quello di supporto e cooperazione con

law, cit., 9.

[64] Sul punto v. ampiamente G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cybersicurezza: tra sovranità e modelli di governance*, cit., 16-17.

[65] In questo senso vanno si vedano, ad esempio, l'art. 1, par. 6, della Direttiva NIS, laddove si prevede che la «direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati», oppure l'art. 1, par. 6, della Direttiva NIS 2, dove si stabilisce che la «direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico», o, ancora, l'art. 1, parr. 4 e 5, del regolamento (UE) 2025/38 i quali prevedono, rispettivamente, che «[l]e azioni intraprese a norma del presente regolamento sono realizzate nel debito rispetto delle competenze degli Stati membri e integrano le attività svolte dalla rete di CSIRT, da EU-CyCLONe e dal gruppo di cooperazione NIS» e che «[i]l presente regolamento lascia impregiudicate le funzioni statali essenziali degli Stati membri, tra cui la garanzia dell'integrità territoriale dello Stato, il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza nazionale. In particolare, la sicurezza nazionale resta una competenza esclusiva di ciascuno Stato membro».

[66] Art. 4, par. 2, Trattato sull'Unione europea (TUE).

[67] In questo senso sottolinea C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, cit., 26, che «l'attività principale dell'ENISA è quella di coordinare l'operato degli stati membri e favorire il dialogo intra-europeo, attraverso l'elaborazione di linee guida e l'individuazione di best practices. A questo scopo, l'agenzia pubblica molti documenti, disponibili online e liberamente consultabili, per cercare di tenere aggiornato lo stato dell'arte della cybersecurity in Europa e stimolare il confronto tra i vari stati, nell'intento

gli Stati membri e le autorità statali preposte al fine di un maggiore coordinamento e dell'attuazione della normativa europea. Sicché, più che di verticalizzazione dell'impianto normativo europeo, potrebbe parlarsi, più opportunamente, di orizzontalizzazione dovuta al processo di armonizzazione delle legislazioni nazionali, in una logica di *governance* europea[68] della cibersicurezza analogamente a quanto può (o potrebbe) realizzarsi anche a livello globale (v. *infra*).

3. La dimensione internazionale della cibersicurezza

Nel corso degli anni l'approccio europeo si è sempre più evoluto in quello che è stato definito "*geopolitical turn*" verso uno sviluppo estensivo internazionale e globale della cibersicurezza[69]. Emblematica in questo senso è la Strategia in materia di cibersicurezza del 2020[70] nella quale si afferma esplicitamente che, per promuovere e difendere la propria visione del ciberspazio e della cibersicurezza, l'Unione europea «deve intensificare il suo impegno e la sua leadership nei processi di normazione internazionale, nonché rafforzare la sua rappresentanza negli organismi di normazione internazionali ed europei e in altre organizzazioni per lo sviluppo di norme», nonché continuare «a collaborare con i partner internazionali per far progredire e promuovere un ciberspazio globale, aperto, stabile e sicuro in cui il diritto internazionale, in particolare la Carta delle Nazioni Unite (ONU), sia rispettato» con la necessità che l'Unione europea e gli Stati membri «assumano una posizione maggiormente proattiva nelle discussioni in seno all'ONU e in altre sedi internazionali pertinenti»[71].
Questa "propensione" internazionale e globale dell'Unione europea ci consente di allargare l'analisi anche (e soprattutto per quanto riguarda l'obiettivo di questo scritto) a tali dimensioni. L'Unione europea è ben rappresentata negli organismi internazionali[72], svolgendo un ruolo signifi-

che si affermino le pratiche più avanzate».

[68] Sul punto v. A. Kasper, *EU Cybersecurity Governance – Stakeholders and Normative Intentions Towards Integration*, in M. Harwood - S. Moncada - R. Pace (eds.), *The future of the European Union: Demisting the Debate*, Institute for European Studies, 2020.

[69] Cfr. F. Delerue - A. Géry, *International Law and Cybersecurity Governance: The Way Forward*, in Iid. (eds.), *International Law and Cybersecurity Governance*, Leiden, 2022, 10.

[70] Comunicazione congiunta al Parlamento europeo e al Consiglio - La strategia dell'UE in materia di cibersicurezza per il decennio digitale, JOIN(2020) 18 final.

[71] Cfr. par. 3 "Promuovere un ciberspazio globale e aperto" della Strategia in materia di cibersicurezza 2020.

[72] Si pensi al Consiglio d'Europa, all'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), all'Organizzazione per la cooperazione e lo sviluppo economico

cativo nella promozione del diritto internazionale e degli sviluppi in tema di cibersicurezza a livello globale[73].

Seguendo pertanto questa tendenza europea e spostandoci su un piano pienamente internazionale, vengono in rilievo due principali "arene" dove in tema di cibersicurezza si è giunti alla previsione di convenzioni internazionali e forme di *governance* di portata assai rilevante: il Consiglio d'Europa e le Nazioni Unite.

Quanto al primo pare necessario annoverare fin da subito la Convenzione sulla criminalità informatica del Consiglio d'Europa, meglio nota come Convenzione di Budapest[74], la quale rappresenta (perlomeno finora) l'accordo internazionale più rilevante che affronta specificamente il tema della sicurezza informatica essendo un trattato di cd. *law enforcement* che si concentra su diversi tipi di azione e intervento – tra cui l'adozione di legislazioni appropriate e la promozione della cooperazione internazionale – per l'integrità dei sistemi informatici da crimini commessi attraverso la Rete, con particolare riguardo alla violazione del diritto d'autore, alla pornografia minorile, alle frodi informatiche e all'integrità stessa dei sistemi informatici[75].

Sebbene non manchino certamente altri strumenti a carattere pattizio sul tema della cibersicurezza e con una portata "regionale"[76], il caso della

(OCSE) e alle Nazioni Unite, nonché ad alcuni organismi a quest'ultima riferibili come l'Unione internazionale delle telecomunicazioni (ITU), il World Summit on the Information Society (WSIS) e l'Internet Governance Forum (IGF).

[73] Cfr. E. Fahey, *Developing EU Cybercrime and Cybersecurity: On Legal Challenges of EU Institutionalisation of Cyber Law-Making*, in T. Hoerber - G. Weber - I. Cabras (eds.), *The Routledge Handbook of European Integrations*, London, 2022, 82-84. Sul ruolo dell'Unione europea come attore internazionale di cibersicurezza v. anche J. Odermatt, *The European Union as a Cybersecurity Actor*, in S. Blockmans - P. Koutrakos (eds.), *Research Handbook on the EU's Common Foreign and Security Policy*, Cheltenham, 2018, 354-373; A. Verhelst - J. Wouters, *Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives*, in *International Organization*, 2, 2020.

[74] Convention on Cybercrime (ETS No. 185) del 23 novembre 2001, entrata in vigore il 1 luglio 2004. La Convenzione è stata successivamente integrata dai due protocolli addizionali: troviamo così il *First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)* del 28 gennaio 2003, entrato in vigore il 1 marzo 2006 (firmato da 47 Stati e ratificato da 38), seguito dal *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)* del 12 maggio 2022 (firmato da 51 Stati, ma ratificato soltanto da 2 quindi non ancora entrato in vigore).

[75] Cfr. E. Fahey, *Developing EU Cybercrime and Cybersecurity: On Legal Challenges of EU Institutionalisation of Cyber Law-Making*, cit., 99-100; A. Gascón Marcén, *The Budapest Convention and the UN Cybercrime Convention negotiations*, in A. Segura Serrano (ed.), *Global Cybersecurity and International Law*, London, 2024, 175-176.

[76] Tra questi si vedano la cd. Convenzione di Minsk del 2001 della Comunità degli Stati Indipendenti (*Agreement on cooperation among the States members of the Commonwealth of*

Convenzione di Budapest si segnala come particolarmente interessante in ragione della sua ratifica da parte di 81 Stati, quindi ben oltre il numero degli Stati membri del Consiglio d'Europa e pertanto con una presenza di Stati non solo europei, ma anche africani, americani e pacifico-asiatici[77], in quello che potremmo definire "effetto Strasburgo", sul modello del cd. effetto Bruxelles, dal momento che questa Convenzione ha continuato ad espandere la propria portata (anche indirettamente[78]) nel corso degli anni, con un evidente influsso positivo per quanto riguarda l'azione globale in materia di cibersicurezza anche, e soprattutto, in seno alle Nazioni Unite, costituendo in tal senso una sorta di *transnational gold standard* per la regolazione nazionale della cibersicurezza a livello globale[79], altresì in ragione del fatto che contiene alcune importanti disposizioni a tutela dei diritti

Independent States in combating offences relating to computer information); la cd. Convenzione di Ekaterinburg del 2009 (*Agreement on Cooperation in Ensuring International Information Security*) tra gli Stati membri dell'Organizzazione per la Cooperazione di Shanghai (tra cui Cina, Federazione russa e alcuni Stati dell'Asia centrale); la cd. Convenzione del Cairo nel 2010 della Lega degli Stati arabi (A*rab Convention on Combating Information Technology Offences*) sottoscritta da 18 Stati arabi; la cd. Convenzione di Malabo nel 2014 dell'Unione degli Stati africani (*African Union Convention on Cyber Security and Personal Data Protection*) ratificata al momento da 16 Stati su 55. Per un'analisi di dottrina sul punto v. M. Fidler, *Fragmentation of International Cybercrime Law*, in *Utah Law Review*, 3, 2025, 737 ss.; E. Tikk - M. Kerttunen (eds.), *Routledge Handbook of International Cybersecurity*, London, 2020.
Secondo I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 131-132, emerge così, almeno per il momento, un quadro complesso e di profonda frammentazione, tanto che secondo K. Bannelier - T. Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, in *Les Cahiers de la Revue Défense Nationale*, 2017, 82, il problema sarebbe che «*the proliferation of these initiatives in very diverse fora does not necessarily reflect good governance of cybersecurity*».

[77] Si tratta di 45 Stati membri del Consiglio d'Europa su 46 (l'Irlanda ha firmato la Convenzione, tuttavia senza ancora averla ratificata), oltre a Stati quali, tra gli altri, Argentina, Australia, Brasile, Canada, Cile, Colombia, Ghana, Giappone, Marocco, Nigeria, Paraguay, Perù, Senegal e Stati Uniti. Oltre a questi altri 16 Stati al momento risultano essere firmatari della Convenzione o essere stati invitati ad aderirvi. Cfr. Council of Europe, *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, consultato il 16 ottobre 2025.

[78] Alcuni studiosi sostengono che diversi Stati dell'Oceano pacifico e del nordest asiatico abbiano allineato le proprie legislazioni nazionali alle disposizioni contenute nella Convenzione di Budapest pur non essendone parti; cfr. C. Le Nguyen - W. Golman, *Diffusion of the Budapest Convention on cyber-crime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action*, in *Computer Law & Security Review*, 2021; L. Chang, *Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia*, in T.J. Holt - A.M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, London, 2020, 327 ss.

[79] Cfr. E. Fahey, *Developing EU Cybercrime and Cybersecurity: On Legal Challenges of EU Institutionalisation of Cyber Law-Making*, cit., 99-100.

fondamentali[80].
Similmente interessanti risultano essere i recenti sviluppi nell'ambito delle Nazioni Unite che sembrano trovarsi ad un punto di svolta apprezzabile con specifico riferimento alla dimensione "globale" della cibersicurezza[81]. Sebbene l'impegno sul tema da parte delle Nazioni Unite sia ormai storicamente piuttosto risalente[82], deve osservarsi come vi siano stati alcuni tentativi recenti di affrontare il tema della sicurezza informatica nella forma più compiuta e articolata di un trattato internazionale, specialmente nella direzione più ambiziosa di individuare una cornice regolatoria di portata globale[83]. Ciò è avvenuto segnatamente con riguardo al contrasto della criminalità digitale con la Risoluzione 74/247 del 27 dicembre 2019 dell'Assemblea generale delle Nazioni Unite, laddove è stato istituito un Comitato intergovernativo speciale di esperti (noto come "open-ended ad hoc intergovernmental committee of experts" o AHC), a composizione non limitata e volutamente rappresentativa di tutte le regioni, con il preciso compito di elaborare una convenzione internazionale concernente il con-

[80] Si pensi all'art. 15 della Convenzione di Budapest: «*1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure […]*».

[81] Sebbene le Nazioni Unite siano centrali in questo contributo, non mancano altre importanti organizzazioni internazionali che si occupano della cibersicurezza a livello internazionale. Ad esempio, I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130, evidenzia il ruolo dell'International Telecommunications Union (ITU) e di alcune rilevanti iniziative, tra le quali si segnalano la Global Cybersecurity Agenda (GCA) lanciata nel 2007 al fine di stabilire un «*framework for international cooperation aimed at enhancing confidence and security in the information society*» e il Global Cybersecurity Index (GCI) il quale rappresenta una rilevante iniziative volta al monitoraggio dell'impegno sulla cibersicurezza da parte dei diversi Stati e che è giunto alla sua quinta pubblicazione (2014, 2017, 2018, 2020 e 2024).

[82] In dottrina v. almeno A. Stiano, *Il cyberspazio nel diritto internazionale contemporaneo: tra frammentazione e patrimonio comune dell'umanità*, in *La Comunità Internazionale*, 4, 2018; A. Henriksen, *The end of the road for the UN GGE process: The future regulation of cyberspace*, in *Journal of Cybersecurity*, 1, 2019, 1 ss.; G.M. Farnelli, *Il contributo delle Nazioni Unite allo sviluppo dell'International Cybersecurity Law*, in *Osorin Working Paper*, 1, 2020; C. Henderson, *The United Nations and the Regulation of Cyber-Security*, in N. Tsagourias - R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2021, 582 ss.

[83] In dottrina A. Segura Serrano, *Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 3, 2021, 718 ss., ha definito la Convenzione sul cybercrime come «*test case of norm-development*».

trasto all'uso delle tecnologie dell'informazione e della comunicazione per finalità criminali, capace di tenere debitamente conto sia degli strumenti internazionali esistenti sia degli sforzi a livello nazionale, regionale-sovranazionale e internazionale[84]. Muovendo rapidamente verso l'epilogo e tralasciando per motivi di opportunità le fasi intermedie, il 24 dicembre 2024 l'Assemblea generale delle Nazioni Unite, con la Risoluzione 79/243, ha ufficialmente adottato la nuova Convenzione contro il cybercrime[85], la quale è stata sottoscritta da settantadue Stati nel corso di una cerimonia formale ad Hanoi, in Vietnam, il 25-26 ottobre 2025 – restando aperta alla firma fino al 31 dicembre 2026 presso la sede delle Nazioni Unite a New York – ed entrerà in vigore novanta giorni dopo la ratifica da parte del quarantesimo firmatario[86]. L'obiettivo primario di questa Convenzione è quello di rafforzare la cooperazione internazionale per accrescere la cibersicurezza e proteggere le società dai pericoli provenienti dal ciberspazio, in particolare aggiornando il quadro normativo globale previsto in larga parte dalla Convenzione di Budapest rispetto al nuovo contesto tecnologico-digitale e geopolitico[87]. In questo senso vengono introdotti nuovi obblighi di incriminazione[88] e relative misure procedurali-applicative, sebbene, per

---

[84] Assemblea generale delle Nazioni Unite, Risoluzione 74/247 del 27 dicembre 2019, *Countering the use of information and communications technologies for criminal purposes* (UN Doc A/RES/74/247). Si veda anche la Risoluzione 75/282 del 26 maggio 2021 per alcune questioni pratico-organizzative relative al Comitato intergovernativo speciale di esperti (UN Doc A/RES/75/282).

[85] Assemblea generale delle Nazioni Unite, Risoluzione 79/243 del 24 dicembre 2024, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes* (UN Doc A/RES/79/243).

[86] La Convenzione è stata firmata da 72 Stati durante la cerimonia dell'ottobre 2025, tra cui si segnalano Cina, Federazione russa, Unione europea (e 12 Stati membri europei, tra cui Francia, Spagna e Polonia), Regno Unito e Australia. Al momento risultano 74 Stati firmatari; il dato è aggiornato al 18 febbraio 2026.

[87] Come si legge nel Preambolo, tra gli obiettivi principali della Convenzione vi è «*to pursue, as a matter of priority, a global criminal justice policy aimed at the protection of society against cybercrime by, inter alia, adopting appropriate legislation, establishing common offences and procedural powers and fostering international cooperation to prevent and combat such activities more effectively at the national, regional and international levels*». *Si insiste inoltre sulla necessità «to enhance coordination and cooperation among States by, inter alia, providing technical assistance and capacity-building, including the transfer of technology on mutually agreed terms, to countries, in particular developing countries, upon their request, to improve national legislation and frameworks and enhance the capacity of national authorities to deal with cybercrime in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations plays*».

[88] Come osserva M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, in *Freedom, Security & Justice: European Legal Studies*, 2, 2025, 109 ss., spec. 112-113, quanto agli obblighi di incriminazione, il testo finale della Convenzione prevede una serie limitata di crimini informatici tipici (cd. crimini

quanto riguarda il contributo della Convenzione alla determinazione della legalità dello spazio cibernetico, questa non si occupi in alcun modo dei cd. attacchi cibernetici, vale a dire di quei tentativi intenzionali di ledere le infrastrutture, i sistemi informatici o le reti statali ovvero di rilevanza considerevole per i servizi strategici di portata nazionale che sono promossi direttamente da altri Stati o da gruppi che agiscono per conto di questi[89]. Tale Convenzione rappresenta – o meglio, potrebbe rappresentare – un primo passo di regolazione della criminalità informatica nello spazio cibernetico, nella direzione di poter giungere a un quadro normativo globale soddisfacente in tema di regolazione del ciberspazio, specialmente per quanto riguarda i profili della cibersicurezza. Sarà fondamentale seguire il processo di applicazione della Convenzione a livello statale, in quanto essa coinvolge Stati che possono essere alquanto disomogenei tra di loro con riferimento alle strutture e ai principi costituzionali dei corrispondenti ordinamenti giuridici, con la conseguenza che le medesime disposizioni potrebbero trovare applicazione in maniera anche estremamente differenziata nei vari ordinamenti[90]; sotto questo profilo, risultano sostanziali e

"*cyber-dependent*", vale a dire quelli che possono essere commessi soltanto attraverso sistemi informatici) e soltanto alcuni specifici reati che possono essere commessi "offline", ma che le tecnologie digitali possono rendere più agevoli o efficaci (cd. crimini "*cyber-enabled*"); fra questi troviamo sia crimini che tutelano l'integrità dei sistemi tecnologici di informazione e comunicazione, come l'accesso illegale (art. 7), l'intercettazione illegale (art. 8), l'interferenza con dati elettronici attraverso il danneggiamento, l'alterazione o l'eliminazione degli stessi (art. 9), la creazione di interferenze al funzionamento dei sistemi di tecnologie della comunicazione e dell'informazione (art. 10), sia altri crimini i quali, diversamente, offrono tutela a beni diversi, come quelli relativi alla diffusione online di materiale attinente ad abusi o sfruttamento sessuale di minori (art. 16) o alla divulgazione non autorizzata di immagini intime (art. 17).

[89] Cfr. M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, cit., 127-129. Se per alcuni autori questa scelta rappresenta la volontà degli Stati di ritenere non necessaria una regolazione internazionale pattizia sul punto, potendo essere invece sufficiente il diritto internazionale generale, in particolare per quanto riguarda la responsabilità internazionale degli Stati (cfr. per tutti A. Stiano, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, 260-261; in maniera più critica F. Delerue, *Cyber Operations and International Law*, Cambridge, 2020, 184 ss.), trattandosi quindi di una scelta di natura "politica", per altri autori, invece, il diritto internazionale, specialmente nella sua configurazione di *jus ad bellum*, non sarebbe affatto idoneo a disciplinare gli attacchi informatici condotti dagli Stati in ragione delle caratteristiche tecniche di siffatti attacchi cibernetici (cfr. L. Baudin, *Cyberattaques et droit international public: de la négociation entre États à l'intégration des acteurs privés pour parvenir à la cyberpaix?*, Paris, 2023, 140: «*[d]e nos observations sur le jus ad bellum, nous parvenons à la conclusion que celui-ci est, en l'état actuel, inadapté dans les cas d'attaques informatiques. […] Déjà parce que les différentes notions liées à l'emploi du cyberespace n'ont pas été définies, ensuite parce que les particularités techniques des attaques informatiques n'ont pas été prises en considération*»).

[90] Cfr. A. Balsamo, *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime*, in *Diritto penale e processo*, 2, 2025, 246-247.

decisivi il ruolo svolto dai giudici nazionali – i quali potrebbero sviluppare un approccio comune in grado di tutelare i diritti fondamentali – e gli strumenti di cooperazione previsti dalla Convenzione per lo sviluppo delle capacità tecnico-organizzative anche degli Stati tecnologicamente meno avanzati[91], con l'obiettivo un'armonizzazione di natura tecnica, ma soprattutto di applicazione uniforme della normativa a livello globale.

Parallelamente occorre soffermarsi anche sugli sviluppi per quanto concerne la *governance* internazionale della cibersicurezza. Senza volersi addentrare nelle complicate e tortuose vicende che hanno caratterizzato gli ultimi trent'anni, basti qui ricordare che il tema della cibersicurezza, in quel momento intesa come il rapporto tra le nuove tecnologie digitali e il contesto della sicurezza internazionale, viene affrontato per la prima volta dall'Assemblea generale delle Nazioni Unite verso la fine degli anni '90 tramite una proposta di risoluzione presentata dalla Federazione russa, poi approvata per *consensus* il 4 dicembre 1998 come Risoluzione 53/70[92]. L'effetto più significativo di tale risoluzione fu l'istituzione del Gruppo di esperti governativi, meglio noto semplicemente come *Group of Governmental Experts* (GGE)[93], creato attraverso la Risoluzione 58/32 del 18 dicembre 2003 dall'Assemblea generale quale gruppo di lavoro di esperti governativi in tema di cibersicurezza, nominati dal Segretario generale sulla base di una distribuzione geografica equa e ponderata, con il compito specifico di valutare le questioni prioritarie e le strategie nazionali per la cibersicurezza, nonché identificare le misure più adatte da adottare per rafforzare la sicurezza internazionale dei sistemi digitali globali di informazione e comunicazione. In questa direzione, l'Assemblea generale ha istituito dal 2004 in poi diversi GGE, con mandati biennali e una composizione variabile (oscillante tra 15 e 25 membri), i quali si sono focalizzati sull'esame delle principali minacce (anche potenziali) alla sicurezza provenienti dallo spazio cibernetico nel tentativo di individuare, nei report finali, strumenti

[91] Cfr. M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, cit., 112-113. La Convenzione dedica al tema il Capitolo VII (Technical assistance and information exchange); in particolare v. gli artt. 54-56.

[92] Assemblea generale delle Nazioni Unite, Risoluzione 53/70 del 4 dicembre 1998, Developments in the field of information and telecommunications in the context of international security (UN Doc A/RES/53/70). In dottrina v. P. Gargiulo, *The United Nations and Cybersecurity*, in *La Comunità internazionale*, Quaderno n. 29, P. Gargiulo - D. Giovannelli - A.L. Sciacovelli (eds.), *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, Napoli, 2024, 205 ss.; I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130.

[93] Nella denominazione ufficiale *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGGE).

e forme di cooperazione internazionali adeguati ad affrontarle[94]. Sebbene queste relazioni contenessero importanti elementi sugli sviluppi della sicurezza digitale nel ciberspazio che confermavano le necessità di applicare pienamente il diritto internazionale allo spazio cibernetico – rappresentando, di fatto, un importante sforzo di implementare quanto previsto dall'Assemblea generale in alcune risoluzioni circa la necessità che una solida cultura globale della cibersicurezza debba essere incoraggiata, promossa, sviluppata e attuata con vigore[95] – il lavoro dei GGE è contestabile non solo per uno scarsissimo impatto concreto, ma anche in ragione del fatto che forse il compito di raggiungere un accordo di rilevanza globale in relazione all'applicazione uniforme del diritto internazionale alla sicurezza informatica e ai mezzi di informazione e comunicazione nel ciberspazio era troppo ambizioso, specialmente per un organismo – è bene ribadirlo, formato da esperti dei governi statali – non in grado di produrre impegni politici o giuridici di vasta portata da parte della comunità internazionale come sarebbe invece necessario se si vuole giungere ad una protezione efficace della cibersicurezza[96].

Nondimeno, l'emersione di profonde divergenze tra gli Stati membri delle Nazioni Unite portò nel 2018 ad una sorta di "opposizione istituzionale", dal momento che furono istituiti due diversi "gruppi" di lavoro. Da un lato, il GGE per il periodo 2019-2021 composto da 25 esperti nazionali nominati sulla base di una distribuzione geografica equa, ma pur sempre

[94] L'Assemblea generale delle Nazioni Unite ha istituito sei GGE nel 2004, 2009, 2012, 2014, 2016 e 2019 attraverso sei Risoluzioni analoghe, le prime cinque aventi il medesimo oggetto, vale a dire "Developments in the field of information and telecommunications in the context of international security" (Risoluzione 58/32 dell'8 dicembre 2003 UN Doc A/RES/58/32; Risoluzione 60/45 dell'8 dicembre 2005 UN Doc A/RES/60/45; Risoluzione 66/24 del 2 dicembre 2011 UN Doc A/RES/66/24; Risoluzione 68/243 del 27 dicembre 2013 UN Doc A/RES/68/243; Risoluzione 70/237 del 23 dicembre 2015 UN Doc A/RES/70/237), e l'ultima avente come oggetto *Advancing responsible State behaviour in cyberspace in the context of international security* (Risoluzione 73/266 del 22 dicembre 2018 UN Doc A/RES/73/266). Quanto ai risultati di questi gruppi di esperti v. da ultimo il *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* del 14 luglio 2021 (UN Doc A/76/135). In dottrina v. F. Delerue - A. Géry, *International Law and Cybersecurity Governance: The Way Forward*, cit., 9-10; P. Gargiulo, *The United Nations and Cybersecurity*, cit., 205 ss.; I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130.

[95] Risoluzione 64/211 del 21 dicembre 2009, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures* (UN Doc A/RES/64/211); analogamente v. anche la Risoluzione 58/199 del 23 dicembre 2003, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* (UN Doc A/RES/58/199).

[96] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130.

un gruppo ristretto come previsto dalla Risoluzione 73/266[97]. Dall'altro lato, invece, un nuovo gruppo denominato "*Open-Ended Working Group*" (OEWG)[98], individuato dalla Risoluzione 73/27[99] con il medesimo scopo di studiare l'applicazione del diritto internazionale al ciberspazio, anche con riguardo alla sicurezza, ma contraddistinto da una diversa composizione capace di rappresentare tutti gli Stati delle Nazioni Unite al fine di ricercare un processo negoziale più democratico e inclusivo. Sono stati istituiti due OEWG (2018 per il 2019-2020 e 2020 per il 2021-2025)[100], i quali hanno determinato, il secondo in modo particolare, rilevanti esiti per quanto concerne un possibile sviluppo in termini globali della *governance* della cibersicurezza (v. *infra*).

4. È possibile una *governance* (costituzionale) globale della cibersicurezza?

La rivoluzione digitale ha portato con sé numerosi benefici, ma anche diversi aspetti problematici, tra i quali sono stati evidenziati, anche in questa sede, quelli legati alla cibersicurezza quanto ai pericoli per sistemi informatici, reti e dispositivi digitali, nonché, in maniera conseguente, per i diritti fondamentali. La risposta a tale "lato oscuro" della digitalizzazione segue itinerari diversi, come la diffusione del concetto di "sovranità digitale", spesso intesa come aspetto della più generale sovranità nazionale e quindi

[97] Risoluzione 73/266 del 22 dicembre 2018, *Advancing responsible State behaviour in cyberspace in the context of international security* (UN Doc A/RES/73/266); si tratta di una risoluzione proposta degli Stati Uniti e approvata con 138 voti favorevoli, 12 contrari (tra cui Cina e Russia) e 16 astensioni.

[98] V. in dottrina almeno P. Gargiulo, *The United Nations and Cybersecurity*, cit., 211; F. Delerue - A. Géry, *International Law and Cybersecurity Governance: The Way Forward*, cit., 9-10.

[99] Risoluzione 73/27 del 5 dicembre 2018, *Developments in the field of information and telecommunications in the context of international security* (UN Doc A/RES/73/27); si tratta di una risoluzione proposta dalla Federazione russa e approvata con 119 voti favorevoli, 46 contrari (tra cui Stati Uniti e i Paesi membri dell'Unione europea) e 14 astensioni.

[100] L'Assemblea generale delle Nazioni Unite ha creato due OEWG successivi con un'agenda analoga, nel 2018 (2019-2020) e nel 2020 (2021-2025); Risoluzione 73/27, *Developments in the field of information and telecommunications in the context of international security* del 5 dicembre 2018 (UN Doc A/RES/73/27); Risoluzione 75/240, *Developments in the field of information and telecommunications in the context of international security* del 31 dicembre 2020 (UN Doc A/RES/75/240). Quanto agli esiti di questi due OEWG si vedano: United Nations General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* del 18 marzo 2021 (UN Doc A/75/816); United Nations General Assembly, *Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025* del 24 luglio 2025 (UN Doc A/80/257).

come forma di autonomia tecnologica nel mondo digitale e di controllo, specialmente da parte di uno Stato, su dati, tecnologie e infrastrutture digitali al fine di proteggerli da interferenze esterne[101], ovvero, come è emerso nelle pagine precedenti, forme di cooperazione internazionale le quali procedono – lentamente, con numerose difficoltà e (al momento) parzialmente – nella direzione di un integrale quadro normativo del ciberspazio[102].
In un siffatto contesto sembra possibile immaginare un nuovo approccio globale, di natura anche costituzionale, alla *governance* e alla regolazione della cibersicurezza[103], in quella che è stata definita come "*digital constellation*", vale a dire un modello in grado sia di ricomprendere un panorama complesso e interconnesso di attori (Stati, organismi internazionali, aziende digitali e società civile), sia di coinvolgere i vari livelli di governo interessati dall'evoluzione tecnologica (locale, statale, sovranazionale, internazionale e globale)[104]. Sicché l'approccio teorico che meglio potrebbe informare tale formula globale di *governance* e di sviluppo di una cornice costituzionale (anche regolatoria) globale potrebbe essere quello del costituzionalismo globale, nella sua dimensione "verticale" di costituzionalizzazione del diritto internazionale[105]; infatti, pur in assenza di un governo mondiale e di un potere costituente tradizionalmente inteso, si tratta di affrontare il tema della legittimazione democratica di decisioni che travalicano i confini delle politiche e della sovranità nazionali e, di conseguenza, costituzionalizzare in una logica democratica il frammentato sistema del diritto internazionale e della *governance* globale (v. *infra*)[106].

---

[101] In dottrina v. almeno V. Bertola, *La sovranità digitale e il futuro di Internet*, in *Rivista italiana di informatica e diritto*, 1, 2022, 39-46; G. Finocchiaro, *La sovranità digitale*, in *Diritto pubblico*, 3, 2022, 809 ss.

[102] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 113-114, 116.

[103] Quanto al contesto generale della governance globale della cibersicurezza v. in dottrina, tra gli altri, V. Greiman, *Cybersecurity and Global Governance*, in *Journal of Information Warfare*, 4, 2015; P. Rosenzweig, *The International Governance Framework for Cybersecurity*, in *Canada-United States Law Journal*, 2, 2012, 405 ss.; S. Jayawardane - J.E. Larik - E. Jackson, *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*, The Hague Institute for Global Justice Policy Brief, 2015; S. Savaş - S. Karataş, *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance*, cit.

[104] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 116; I. Pernice, *Risk Management in the Digital Constellation – A Constitutional Perspective*, HIIG Discussion Paper Series, 7, 2017; e il chiaro rimando, quanto alla "*postnational constellation*", a J. Habermas, *The Postnational Constellation: Political Essays*, Cambridge, 2001.

[105] V. sul punto O. Caramaschi, *Il costituzionalismo globale: teorie e prospettive*, Torino, 2022, 119 ss.

[106] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 113. L'A. inoltre, 118, insiste sul ruolo di Internet a tal proposito, in quanto «*multilevel and, as an element of it, global constitutionalism is taken as a normative theory that informs and allows to frame a model of governance that includes legitimate rule-making at the global level as it would not be possible*

Restringendo il campo d'osservazione, almeno per il momento, alla *governance* (globale) della cibersicurezza, questa può essere delineata come un ambito specifico della più generale *governance* di Internet laddove diversi organismi internazionali si trovano coinvolti nel processo di normazione del settore, in una forte interconnessione tra soggetti pubblici e privati[107]; alcuni sono specificamente interessati dalla *governance* della cibersicurezza da un punto di vista normativo di diritto internazionale pubblico come il Consiglio d'Europa o le Nazioni Unite, come in parte già osservato, altri svolgono, nell'ambito della *governance* della Rete, un ruolo più tecnico-normativo – come la Internet Engineering Task Force (IETF) o la International Organization for Standardization (ISO) – ovvero consultivo e di promozione del dialogo come l'Internet Governance Forum (IGF) vale a dire la piattaforma globale *multistakeholder* creata dalle Nazioni Unite nel 2006, come parte del World Summit on the Information Society (WSIS), al fine di promuovere la collaborazione tra governi, organizzazioni internazionali, aziende, società civile e accademia per discutere e affrontare le sfide derivanti dal ciberspazio nonché, sempre più, i temi legati alla sicurezza cibernetica, nell'intento di favorire la definizione di taluni requisiti minimi come prima fase di un processo normativo orientato all'identificazione di norme applicabili a livello globale[108].

Eppure, di recente vi è stato un evento di portata significativa e, potenzialmente, rivoluzionaria per quanto riguarda il futuro della *governance* globale della cibersicurezza. Infatti, a luglio 2025 si sono conclusi i lavori dell'*Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs) 2021-2025* e nel report finale è stata prevista l'istituzione del *Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs*[109].

---

without the internet and, simultaneously, ensures that the internet itself is regulated and can be trusted as an communication infrastructure for not only economic but also democratic processes at all levels».

[107] Cfr. T. Nascimento Heim, *Global governance and regulation of cybersecurity: Towards coherence or fragmentation?*, Twente, 2023, 19-22, secondo la quale, inoltre, il ruolo degli attori privati «*is related to the proper functioning of the system (confidentiality, integrity and availability), which aims to prevent/combat cyber threats [or] to promote alternative norms processes opposing state cyber operations. The civil society groups, in turn, became interested in promoting privacy, human rights law and regulating the behaviour of the States and non-state actors in cyberspace*».

[108] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 133-134.

[109] United Nations General Assembly, *Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025* del 24 luglio 2025 (UN Doc A/80/257). La creazione del meccanismo globale si basa sulla proposta dell'OEWG contenuta nell'Allegato C del *Third Annual Report* del luglio 2024 (UN Doc A/79/214), a sua volta sostenuta dall'Assemblea generale nella Risoluzione 79/237 *Open-ended working group on security of and in the use of information and communications technologies*

Questo "meccanismo globale" avrà carattere permanente, diversamente dai precedenti gruppi di lavoro, e rimarrà a guida statale, nel senso che i negoziati sulla sicurezza delle tecnologie della comunicazione e dell'informazione resteranno prerogativa esclusiva degli Stati, sebbene esso sarà aperto a tutti i membri delle Nazioni Unite con la possibilità di coinvolgere attori e *stakeholders* esterni interessati, quali, ad esempio, le imprese private, le organizzazioni non governative e il mondo accademico[110]. I lavori del meccanismo globale si svolgeranno con cicli quinquennali attraverso sessioni plenarie, gruppi tematici, riunioni intermedie appositamente dedicate, conferenze di revisione o qualsiasi altra riunione convocata in diversi formati, purché tali differenti modalità si rafforzino reciprocamente ed evitino discussioni duplicate[111]. In particolare, il meccanismo globale si riunirà due volte all'anno, con una settimana di riunioni dei gruppi tematici e una settimana di riunioni in sessione plenaria[112], per svolgere alcune delle rilevanti funzioni che gli sono attribuite, come, ad esempio, l'esame delle ciberminacce esistenti e potenziali, il rafforzamento della sicurezza delle tecnologie della comunicazione e dell'informazione degli Stati, la predisposizione e l'attuazione di strumenti di soft law volontari e non vincolanti quanto al comportamento responsabile degli Stati nell'ecosistema cibernetico, ovvero l'applicazione del diritto internazionale al mondo

2021-2025 established pursuant to General Assembly resolution 75/240 del 24 dicembre 2024 (UN Doc A/RES/79/237). Come si legge nell'Allegato C, un meccanismo globale permanente e orientato all'azione che si baserà su «*the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports with the aim of continuing to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment»* (par. 1) e su un *«open, inclusive transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and as well as in accordance with developments in the ICT environment*» (par. 4 b-c).

110 Cfr. l'apposita sezione *Additional Elements on Modalities on the Participation of Other Interested Parties and Stakeholders, including Businesses, Non-Governmental Organizations and Academia* prevista nell'*Annex I: Additional Elements for the Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs* (UN Doc A/80/257).

111 Cfr. *Annex I*, cit., par. 4.

112 Cfr. *Annex I*, cit., par. 14. Al par. 7 vengono delineati i *Dedicated Thematic Groups*, i quali «*will aim to build on and complement the discussions in the substantive plenary sessions», in particolare offrendo «the opportunity for more detailed and action-oriented discussions, allowing in particular the participation of experts*». Si tratta, nel dettaglio, dei seguenti gruppi tematici: «*An integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to address specific challenges in the sphere of ICT security in the context of international security in order to promote an open, secure, stable, accessible, peaceful, and interoperable ICT environment, with the participation of, inter alia, technical experts and other stakeholders. (DTG 1)*»; «*An integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to accelerate ICT security capacity-building, with the participation of, inter alia, capacity-building experts, practitioners, and other stakeholders. (DTG 2)*».

digitale e della cibersicurezza anche con particolare riguardo alla possibilità di elaborare ulteriori norme vincolanti[113].

Ora questo nuovo meccanismo globale, al momento delineatosi soltanto in maniera parziale e pertanto ancora da valutare nel suo concreto funzionamento, ben potrebbe rappresentare il punto di partenza di uno sforzo di individuazione (almeno teorico) di un nuovo modello – basato su organismi, strutture e politiche già presenti (o da sviluppare) – di «complementary normative process» per la governance della cibersicurezza a livello globale[114]. Questo si dovrebbe fondare su organismi globali *multistakeholder*, come l'IGF e l'appena menzionato meccanismo globale, deputati all'elaborazione di principi e norme in materia di cibersicurezza da trasporre in una fase successiva in normative applicabili a livello globale, rese giuridicamente vincolanti attraverso la combinazione di normazione e standardizzazione da parte di organismi tecnici – come i richiamati IETF o ISO – da un lato, e i processi legislativi nazionali e sovranazionali sul modello europeo dall'altro[115]. Contestualmente si renderà necessario procedere anche in maniera più generale e globale per il tramite di convenzioni internazionali elaborate, come nel recente caso della Convenzione sul cybercrime, dalle Nazioni Unite, le quali si troveranno impegnate in una doppia veste attraverso i propri organi appositamente dedicati, da un lato incaricandosi di coordinare e supervisionare l'adozione di tali norme vincolanti e applicabili globalmente nonché l'approvazione – sul modello della Convenzione di Budapest – delle strategie e delle legislazioni nazionali in tema di cibersicurezza, dall'altro assumendosi la responsabilità di supervisionare tali processi, ad esempio affidandola al Consiglio di sicurezza o, forse preferibilmente, al Segretario generale, ovvero di monitorare sull'applicazione di queste stesse norme, anche (e forse soprattutto) attraverso il contributo determinante di corti e tribunali di tutti i livelli nel vigilare sull'applicazione concreta e possibilmente uniforme di tali disposizioni[116]. Inoltre, se l'attuazione di tali norme sulla cibersicurezza negli ordinamenti giuridici resterà compito delle autorità nazionali, magari sotto la supervisione di or-

[113] Cfr. A. Insolia, *The impact of the practice of international organizations on the United Nations recent works on cybersecurity*, in *DPCE online*, 2, 2025, 966-967.

[114] I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 136.

[115] Ivi, 136-138. Secondo l'A. IETF e ISO «*have proved to be an excellent framework for setting technical standards as a basis for interoperability, and they should focus on privacy and cybersecurity engineering even more*». *Inoltre, con riguardo alla cibersicurezza, una stretta interazione tra questi soggetti e i processi legislativi «could lead to a burden-sharing between legislators on the one hand, who would be responsible for setting up, on the basis of the principles adopted by the bodies described, minimum security requirements for products and services, and standardisation bodies like IETF or ISO on the other, which would turn these requirements into technical norms to be met by products or terms of services before they are put on the markets*».

[116] Ivi, 137-138.

ganismi delle Nazioni Unite, come appunto il nuovo meccanismo globale, quest'ultimo potrebbe, infine, ricoprire un fondamentale compito di vigilanza sull'implementazione delle norme, nonché, contestualmente, quello di elaborazione di proposte di revisione delle stesse[117].

Un così delineato modello di *governance* della cibersicurezza necessiterebbe, a questo punto, di una dimensione "costituzionale" di legittimazione democratica, nella misura in cui tali organismi, istituzioni e processi dovrebbero trovare una qualche forma di legame, più o meno diretto, con la volontà dei cittadini nella loro veste di "cittadini globali". L'elemento politico-democratico potrebbe essere contestualizzato nella cornice teorica del costituzionalismo globale, recuperando e declinando anche a livello globale l'approccio e gli strumenti propri del costituzionalismo multilivello, il quale consentirebbe di concettualizzare tale quadro "costituzionale" non tanto come un sistema centralizzato di potere a livello globale, ma piuttosto in quanto parte di un sistema costituzionale composito nel quale trovano collocazione elementi nazionali, sovranazionali e globali, in modo tale da collegare tra loro i cittadini e gli attori dei vari livelli[118].

La produzione di normativa globale nel contesto della *governance* globale della cibersicurezza, necessiterebbe, a tal proposito, di essere accettata e legittimata democraticamente dai "cittadini globali", in particolare attraverso processi decisionali e di formazione della volontà che dovranno essere costruiti in maniera inclusiva e non sostitutiva dei processi politico-democratici e legislativi nazionali, ma che anzi saranno necessariamente basati proprio su questi nella dimensione costituzionale multilivello, pur nella consapevolezza che sarebbe opportuno integrarli con nuove e complementari forme globali di «action, control and judicial review»[119]. Proprio in questa direzione gli strumenti della democrazia digitale (o *e-democracy*[120]) costituiscono una delle possibili strade per sviluppare questa declinazione del costituzionalismo globale, peculiarmente perché potrebbero integrare le forme di democrazia tradizionale attualmente esistenti per quanto

---

[117] Per un primissimo commento al nuovo meccanismo e alle sue prospettive future v. R. Payne, *The OEWG ends and a new UN cybersecurity permanent mechanism is born*, in *Global Partners Digital*, 24 luglio 2025; P. Pavlova - C. Painter, *The UN's Permanent Process on Cybersecurity Faces an Uphill Battle*, in *Lawfare*, 13 agosto 2025.

[118] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 139-140. Sul punto in particolare v. Id., *The Global Dimension of Multilevel Constitutionalism: A Legal Response to the Challenges of Globalisation*, in P.-M. Dupuy - C. Tomuschat (eds.), *Völkerrecht als Wertordnung: Festschrift für Christian Tomuschat. Common values in international law: essays in honour of Christian Tomuschat*, Kehl am Rhein, 2006, 973 ss.

[119] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 139-140.

[120] Per un inquadramento generale dell'*e-democracy* nel contesto dello spazio cibernetico v. almeno, da ultimo, O. Caramaschi, *La democrazia digitale (o e-democracy) nello spazio cibernetico: inquadramento teorico e profili applicativi*, in *Federalismi.it*, 33, 2025, 14 ss.

riguarda la legittimazione democratica della *governance* globale della cibersicurezza[121]; ciò dovrebbe avere luogo secondo una logica bidirezionale, perché se è vero che la democrazia digitale può svolgere un ruolo importante di partecipazione e legittimazione democratica nel ciberspazio anche con riguardo alla cibersicurezza, è altrettanto certo che lo sviluppo stesso dell'*e-democracy* richieda strumenti adeguati di tutela della sicurezza informatica dalle sempre più crescenti minacce provenienti dallo spazio cibernetico[122].

Proprio quelle stesse minacce, come sfida posta dall'avvento della rivoluzione digitale, che richiedono di essere affrontate non tanto dagli Stati individualmente, ma a tutti i livelli da quello locale fino a quello globale, in una cornice costituzionale di *governance* della cibersicurezza che, nella logica del costituzionalismo globale, sia in grado di tutelare i diritti fondamentali e offrire adeguate forme di regolazione e controllo del potere digitale anche con specifico riguardo alla sicurezza cibernetica.

---

[121] Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 140-141, nonché Id., *E-Democracy, the Global Citizen, and Multilevel Constitutionalism*, in C. Prins - C. Cuijpers - P.L. Lindseth - M. Rosina (eds.), *Digital Democracy in a Globalised World*, Cheltenham, 2017, 27 ss.

[122] Cfr. C.M. Codreanu, *Digital democracy in peril. Safeguarding e-democracy by boosting cybersecurity*, in *Proceedings of the Smart Cities International Conference*, 9, 2021, 471-472. Secondo l'A., infatti, «*liberal democracies should develop policies regarding cybersecurity, as cybersecurity should not be enhanced whilst democracy, individual freedoms and human rights deteriorated, but on the contrary cybersecurity should be strengthened alongside the promotion and consolidation of democratic processes, and this policy should also be promoted internationally. […] Nevertheless, in order to develop e-democracy, governments should also take into consideration and seriously address cyber threats. The more democratic processes move (even partially) in cyberspace, the more vulnerabilities are created, which also means there will be more opportunities for malicious cyber operations, and hence cybersecurity should be a core element of every policy, programme, initiative or activity of anything digital done by governments, whether it is about e-democracy, e-government platforms or political parties campaigning on social media during elections*».

Omar Caramaschi

Abstract

Nel contesto della digitalizzazione globale e della sempre maggiore interconnessione digitale viene in evidenza il tema della sicurezza cibernetica o cibersicurezza, la quale non riguarda soltanto le minacce provenienti dalla dimensione fisica, ma allarga il proprio orizzonte di riferimento includendo quelle del mondo virtuale del ciberspazio, assumendo una dimensione trasversale che interessa i singoli individui, le imprese, la società nel suo complesso, ma anche gli Stati e gli organismi sovranazionali e internazionali. Ed è proprio a questi ultimi livelli che la cibersicurezza richiede un'azione istituzionale e regolativa opportunamente in grado di rispondere alle sfide e alle minacce provenienti dallo spazio cibernetico e dal mondo digitale. Sebbene la risposta a tali nuovi elementi problematici dovrebbe partire proprio dagli Stati e dagli strumenti costituzionali a loro disposizione, non può non osservarsi come i singoli Stati siano difficilmente in grado di garantire le condizioni essenziali per la sicurezza dei diritti dei cittadini nel ciberspazio, essendo invece necessario rispondere alle sfide globali derivanti per la cibersicurezza con forme di cooperazione sovrastatali e altrettanto globali al fine di rendere consistente la sicurezza nello spazio cibernetico ed effettiva la tutela dei diritti fondamentali anche nel nuovo mondo digitale.

In the context of global digitalization and ever-increasing digital interconnection, the issue of cybersecurity comes to the fore. This concerns not only threats from the physical realm but also expands its scope to include those from the virtual world of cyberspace. This encompasses a transversal dimension that affects individuals, businesses, society as a whole, but also States and supranational and international organizations. It is precisely at these latter levels that cybersecurity requires appropriate institutional and regulatory action capable of responding to the challenges and threats posed by cyberspace and the digital world. While the response to these new challenges should begin with States and the constitutional instruments at their disposal, it is clear that individual States are unlikely to be able to guarantee the essential conditions for the security of citizens' rights in cyberspace. Instead, it is necessary to respond to the global challenges posed by cybersecurity with supranational and equally global forms of cooperation in order to ensure consistent cybersecurity and effective protection of fundamental rights in the new digital world.

Keywords

cybersecurity – cyberspace – global constitutional governance – digitalisation – digital security

La governance della cybersecurity nell'era dell'intelligenza artificiale tra quadro normativo europeo e nazionale*

Stefania Ardito

Sommario

1. L'evoluzione normativa in materia di *cybersecurity* – 2. L'approccio *risk-based* della normativa in materia di *cybersecurity* e di intelligenza artificiale – 2.1 Modalità di valutazione del rischio della normativa *cyber* e di intelligenza artificiale – 3. Le intersezioni dell'intelligenza artificiale con la *cybersecurity* – 3.1 L'intelligenza artificiale per la *cybersecurity* – 3.2 La *cybersecurity* per l'intelligenza artificiale – 4. Conclusioni.

1. L'evoluzione normativa in materia di *cybersecurity*

La progressiva interconnessione di reti[1] e sistemi informativi[2] ha condotto alla formazione di un tessuto infrastrutturale unitario, la cui funzionalità costituisce il presupposto imprescindibile per l'esercizio di funzioni pubbliche e per la continuità dei processi produttivi. La disponibilità e l'inte-

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

Il presente articolo riprende, integra e approfondisce il contributo dell'*Autrice* intitolato "*Tutela della cybersecurity e dell'intelligenza artificiale*" e destinato al volume "*Le regole dei dati e dell'intelligenza artificiale. Dal GDPR alla Legge 132/2025*" a cura di G. Cassano ed E. Prosperetti.

[1] In termini tecnici, per reti (*network*) si intendono le reti di comunicazione elettronica, cioè collegamenti fisici e logici che permettono la trasmissione di dati, incluse le infrastrutture fisiche (mezzi di comunicazione, nodi e dispositivi di rete) e i protocolli che supportano le connessioni. Sono le reti a permettere la trasmissione dei dati fra dispositivi o sistemi e sono componenti essenziali delle infrastrutture digitali.

[2] In termini tecnici, i *sistemi informativi* sono dispositivi, *software*, processi e dati che, connettendosi alle reti, consentono di trattare, memorizzare, elaborare, recuperare, utilizzare e trasmettere le informazioni digitali, supportando servizi e applicazioni.

grità delle infrastrutture digitali[3] sono condizioni strutturali del funzionamento dei settori vitali per l'economia e la società,[4] al punto da configurare una dipendenza di questi ultimi, che, da una prospettiva regolatoria, impone un ripensamento delle categorie tradizionali della sicurezza, integrità, affidabilità e resilienza.

Gli utenti (cittadini, pubbliche amministrazioni e organizzazioni private), generano, raccolgono, elaborano e conservano quantità crescenti di informazioni, inclusi dati personali, attraverso un insieme eterogeneo di dispositivi interconnessi, che spaziano dai *computer* agli *smartphone*, fino ai sistemi IoT.[5] [6] La loro capillare diffusione ha moltiplicato la superficie di esposizione ai rischi informatici. Tale situazione è stata aggravata dall'integrazione di sistemi, modelli e strumenti basati sull'AI generativa nelle tecnologie di uso quotidiano, e, dunque, ha aumentato la probabilità che si verifichino incidenti alle reti e ai sistemi; siano questi dovuti ad attacchi o a guasti, malfunzionamenti tecnici o a un errore umano.[7] L'impiego dell'AI generativa - ancorché amplifichi i benefici in termini di efficienza, produttività e capacità predittiva - introduce inevitabilmente nuove vulnerabilità connesse alla produzione di informazioni *unsafe*. L'informazione sicura diventa, pertanto, un obiettivo primario delle normative che regolamen-

[3] In termini tecnici, le infrastrutture digitali costituiscono l'insieme integrato di reti, sistemi informativi, ovvero di componenti *hardware* e *software*, servizi *cloud*, sistemi di supporto (come la sicurezza, l'alimentazione, la gestione operativa) necessari per garantire il funzionamento sicuro, continuo e affidabile dell'ecosistema digitale, in particolare per le attività critiche delle organizzazioni pubbliche e private e la fornitura dei servizi. Questo insieme di componenti fisiche, logiche e di servizio permette l'erogazione dei servizi digitali.

[4] Considerando 97 NIS2.

[5] Considerando 96 NIS2.

[6] Inclusi i prodotti con elementi digitali, ovvero «qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware immesso sul mercato separatamente» (art. 3, punto 1, CRA).

[7] Considerando 96 NIS2.

tano il digitale[8] e delle *policy* di *data governance*[9], le quali integrano studi[10] e strategie di *risk management*[11] facendo propria la regola «*the higher the risk, the stricter the rules*».[12] La stessa disponibilità di dati e contenuti digitali, infatti, se non governata, può trasformarsi in un vettore di rischi sistemici per l'economia, i diritti fondamentali e la sicurezza collettiva. L'interruzione o la compromissione delle reti e dei sistemi informativi sui quali si fondano queste attività produrrebbe conseguenze negative non solo per gli utilizzatori diretti, ma anche per soggetti terzi (*non-users*) a causa della natura sistemica e interconnessa del rischio informatico.[13]

---

[8] Tra le principali fonti che a livello unionale disciplinano l'informazione in ambito digitale, secondo prospettive differenti, si annoverano, *inter alia*, il Regolamento (UE) 2016/679 (GDPR), la Direttiva (UE) 2022/2555 (NIS2), il Regolamento (UE) 2022/2554 (DORA), il Regolamento (UE) 2022/2065 (Digital Services Act – DSA), il Regolamento (UE) 2024/1689 (AI Act), il Regolamento (UE) 2024/2847 (Cyber Resilience Act – CRA), nonché il Regolamento (UE) n. 910/2014 (eIDAS), come modificato dal Regolamento (UE) 2024/1183 (eIDAS2) in materia di identificazione elettronica e servizi fiduciari. A livello nazionale, si richiamano, non esaustivamente, il Perimetro di Sicurezza Nazionale Cibernetica, il Codice dell'Amministrazione Digitale (CAD), introdotto con d.lgs. 82/2005 e successivamente oggetto di interventi integrativi e di modifica, nonché la recente l. 132/2025 in materia di intelligenza artificiale, entrata in vigore il 10 ottobre 2025.

[9] J.M. Balkin, *Free speech in the algorithmic society: Big data, private governance, and new school speech regulation*, in *UC Davis Law Review*, 51, 2018, 1149 ss.

[10] La letteratura di *management* parla di informazioni "*unsafe*" in quanto «errate, opache o potenzialmente dannose», dunque irrispettose dei principi fondanti della sicurezza delle informazioni (c.d. *CIA triad*), mentre sarebbero da considerarsi *cybersafe* quelle informazioni «*correct, open, benignant*». Per maggiori chiarimenti si veda lo studio P. Spagnoletti-R. Baskerville*, Safe and Unsafe Information: Managing Risks in the Era of Generative Artificial Intelligence,* in *Proceedings of the 35th European Safety and Reliability Conference (ESREL2025) and the 33rd Society for Risk Analysis Europe Conference*, 2025, 1934 ss.

[11] A. Burgess-A. Alemanno-J. Zinn (a cura di), *Routledge handbook of risk studies*, London, 2016; B.T. Sørensen, *Digitalisation: an Opportunity or a Risk?*, in *Journal of European Competition Law & Practice*, 6, 2018, 349 ss.

[12] Si veda European Council, *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*, in *consilium.europa.eu*, 2 febbraio 2024.

[13] Si pensi, a titolo esemplificativo, agli attacchi di disinformazione *online* attuati mediante tecniche coordinate di manipolazione informativa veicolate dalle piattaforme digitali, con ricadute concrete sulla libertà di espressione e di informazione. In tale contesto, reti di propagazione strategiche - *bot*, account falsi, *cluster* tematizzati, reti di amplificazione automatica - operano come moltiplicatori e veicolano contenuti *unsafe*, nella misura in cui frammentano il discorso pubblico, polarizzano opinioni e generano asimmetrie informative. Si veda A. Gullo-I. Pasquetto-G. Riotta-N. Apolito, *Come individuare e contrastare operazioni coordinate di disinformazione in Italia*, in *esteri.it*, 2023; J.L. Vargas Valdez, *Study on the role of social media and the internet in democratic development*, Council of Europe (Venice Commission), in *venice.coe.int*, 2018; ENISA, *Foreign Information Manipulation and Interference (FIMI) and cybersecurity - Threat Landscape*, in *enisa.europa.eu*, dicembre 2022.

L'espansione esponenziale delle attività svolte *online* non solo ha moltiplicato la quantità dei dati generati e scambiati, ma ha altresì innalzato il livello qualitativo e la granularità dell'informazione, consentendo di ricostruire profili progressivamente più dettagliati e potenzialmente invasivi della sfera privata e professionale delle persone.[14] Negli ultimi anni, la *cyber awareness*, istituzionale[15]e normativa, ha conosciuto un'accelerazione senza precedenti traducendosi in un progressivo rafforzamento dei quadri regolatori[16] e della cooperazione pubblico-privata.[17] L'incremento di eventi *cyber*[18] che si registrano ogni anno è riconducibile, *prima facie*, a una crescita quantitativa delle minacce,[19] ma riflette anche l'evoluzione degli strumenti tecnici, normativi e di cooperazione che consentono ai CSIRT (*Computer Security Incident Response Team*) europei[20], incluso quello italiano[21], un monitoraggio continuo, processi di *information sharing*[22] e, pertanto, una rileva-

[14] ENISA, *Threat Landscape*, in *enisa.europa.eu*, settembre 2024.

[15] D. Eckert, *40 Years of European Digital Policies. Forgotten Lessons*, Cham, 2024.

[16] L. A. Bygrave, *The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes*, in *Computer Law & Security Review*, 56, 2024, 106071 s.

[17] A. Gullo, *Compliance*, in *Archivio Penale*, 1, 2023, 1 ss.

[18] Per evento *cyber* si intende «Qualsiasi evento osservabile in una rete o in un sistema informativo». Si veda ACN, *Domini della cybersicurezza - Event, Threat and Incident Management*, su *acn.gov.it*.

[19] Nel solo primo semestre 2025, l'Italia ha registrato 1.549 eventi *cyber* (+53% rispetto al primo semestre 2024), che hanno colpito 2.367 soggetti (in diversi casi più volte), di cui 346 con un impatto confermato (+98% rispetto allo stesso periodo del 2024) e dunque con conseguenze tangibili "nel mondo reale". Si veda ACN, *Operational Summary del 1° semestre 2025*, in *acn.gov.it*.

[20] Ai sensi dell'art. 15.1, lett. a), Decreto NIS2 «è l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i settori, i sottosettori e le tipologie di soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso».

[21] I dati vengono raccolti dal CSIRT Italia. Il CSIRT Italia è stato istituito con il d.lgs. 65/2018 che ha recepito la Direttiva NIS1 e definito compiti e funzioni. Successivamente, il D.P.C.M. 8 agosto 2019 ne ha disciplinato organizzazione e funzionamento presso il Dipartimento delle informazioni per la sicurezza (DIS). Con il d.l. 14 giugno 2021, n. 82, il CSIRT è stato trasferito presso l'ACN, assumendo la denominazione di CSIRT Italia e configurandosi come punto di contatto nazionale unico per la gestione e la notifica degli incidenti *cyber*. Nel quadro attuale, ulteriormente rafforzato dalla normativa NIS2, il CSIRT Italia è l'articolazione tecnico-operativa di ACN, destinatario delle notifiche di tutti gli incidenti *cyber* che si verificano sul territorio nazionale e che coinvolgono i soggetti individuati e disciplinati dalla normativa, tra cui il Perimetro di Sicurezza Nazionale Cibernetica, l. 90/2024, e d.lgs 138/2024, che recepisce la Direttiva NIS2. Inoltre, svolge un ruolo centrale nella prevenzione, nel monitoraggio e nella risposta agli incidenti, operando quale nodo fondamentale del sistema nazionale ed europeo di gestione del rischio *cyber*.

[22] F. Serini, *Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche.*

zione più capillare e proattiva di vulnerabilità, minacce e attacchi *cyber*. [23]

Verso una definizione di cybersicurezza integrata?, in questa *Rivista*, 3, 2023, 1 ss.

[23] L'art. 23 Direttiva NIS2 afferma che «*Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority … of any incident that has a significant impact on the provision of their services*». L'*Operational Summary* di ACN, relativo al mese di gennaio 2026, registra un aumento del numero di incidenti *cyber* segnalati dalle organizzazioni nei diversi settori disciplinati. Questo riflette, da un lato, una maggiore consapevolezza del rischio da parte delle organizzazioni e, dall'altro, la progressiva adozione di corrette procedure di notifica. Nel contesto italiano i risultati in termini di *compliance* appaiono particolarmente significativi se si considera che le organizzazioni rientranti nel perimetro normativo - sia unionale sia nazionale - sono di dimensione e tipologia variegata. Inoltre, come noto, esse non partivano da livelli omogenei di conoscenza e maturità tecnologica (cfr., ad esempio, i Report Eurostat o ISTAT annuali in ambito Imprese e ICT antecedenti e successivi al periodo Covid-19). In questo processo evolutivo, un ruolo rilevante è svolto dall'emersione di obblighi di *compliance* sempre più strutturati contenuti nelle normative ma anche dalle iniziative di indirizzo e supporto di natura non cogente, ma funzionalmente connesse all'attuazione degli obblighi previsti per gli Stati membri quali, ad esempio, quelli della Direttiva NIS2 che richiede, *inter alia*, di: (*i*) adottare una strategia nazionale in materia di *cybersecurity*, che comprenda politiche per la sicurezza della catena di approvvigionamento; (*ii*) la gestione delle vulnerabilità; (*iii*) l'educazione e la sensibilizzazione in materia, applicate in combinato con le necessità derivanti dalla normativa domestica.
Tra le iniziative non cogenti portate avanti da ACN si annoverano strumenti operativi, anche con funzione di coordinamento tra normativa unionale e nazionale, quali la "tassonomia *cyber*": linee guida finalizzate all'adozione di un lessico comune a livello nazionale, esigenza particolarmente rilevante alla luce della derivazione unionale e della prevalente lingua inglese della materia.
Le linee guida sulla *constituency* del CSIRT Italia che individuano l'insieme dei soggetti nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta, al fine di prevenire e gestire eventi e incidenti di sicurezza informatica. In tale documento, la principale distinzione tra i soggetti - obbligati, non obbligati e "ulteriori" - si fonda sulla sussistenza o meno di obblighi di notifica degli incidenti rilevanti per la sicurezza nazionale, nonché sul diverso grado di responsabilità strategica attribuito loro da leggi specifiche. In particolare, rientrano tra i soggetti obbligati quelli a cui sono conferiti specifici obblighi di sicurezza e notifica da fonti normative settoriali, quali: il d.l. 105/2019 (soggetti PSNC), il Codice delle Comunicazioni Elettroniche (CCE) - d.lgs. 259/2003 (Operatori TELCO) e della l. 90/2024 (soggetti individuati dall'articolo 1, co. 1). Si veda ACN, *La constituency del CSIRT Italia Definizione dei soggetti parte della constituency*, in acn.gov.it, 31 luglio 2024. Si noti che il documento si rivolge inoltre ai soggetti individuati ai sensi del d.lgs. n. 65/2018 (operatori di servizi essenziali e fornitori di servizi digitali), che ha recepito la direttiva NIS1, oggi superata e ampliata dalla Direttiva NIS2, la quale estende significativamente il perimetro soggettivo ai 18 settori individuati a livello europeo. Accanto ai soggetti obbligati, le linee guida includono anche i «soggetti operanti nei settori critici senza obbligo di notifica», che, pur non essendo formalmente individuati dal legislatore, sono considerati parte della *constituency* in ragione della loro operatività in ambiti strategici. Infine, vi rientrano gli "ulteriori soggetti", ossia quelli non sottoposti ad obblighi di notifica e operanti in settori diversi da quelli per i quali tali obblighi sono previsti, ai quali il CSIRT Italia continua a fornire servizi di base. Nel complesso, il documento evidenzia come l'operatività integrata e continuativa dell'insieme dei soggetti coinvolti sia considerata essenziale a livello

Tuttavia, gli sviluppi tecnologici, geopolitici e sociali, al pari, contribuiscono a ridefinire costantemente il panorama *cyber* ampliando la superficie di attacco, introducendo nuove sfide alla sicurezza informatica[24] e dinamiche di rischio più sofisticate, che incidono sui dati raccolti dalle autorità nazionali, tra cui, in Italia, l'Agenzia per la Cybersicurezza Nazionale (ACN). In tale contesto, la *cybersecurity*[25] dimostra una peculiare capacità di adattamento, derivante dalla sua natura intrinsecamente multidisciplinare, che le consente di rispondere alla complessità strutturale dei fenomeni digitali. Ne consegue che istituzioni e organizzazioni sono chiamate a esercitare una responsabilità condivisa nella prevenzione e gestione degli incidenti *cyber*, assumendo obblighi di protezione[26] che si estendono oltre la dimensione meramente tecnica[27] e incidono direttamente sulla tutela degli interessi giuridici[28], inclusi quelli delle persone[29], che vivono nella cosiddetta «società del rischio».[30]

A partire dalla Direttiva NIS1 del 2016[31] - primo atto normativo europeo

nazionale per il mantenimento di funzioni rilevanti «per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese, nonché per evitare pregiudizi alla sicurezza nazionale» necessitando forme di partnership pubblico-private. Pur richiedendo un aggiornamento alla luce delle più recenti evoluzioni normative, il documento costituisce ancora uno strumento utile per comprendere la logica sistemica e inclusiva della gestione degli incidenti *cyber* a livello nazionale, anche oltre il perimetro dei soggetti formalmente obbligati.

Come ultimo documento, si richiama, infine, ACN, *Guida alla notifica degli incidenti*, in acn.gov.it, 26 luglio 2024 dove viene definito un "testo unico" delle istruzioni per i diversi soggetti, pubblici e privati, tenuti per legge alla notifica degli incidenti, che, benché antecedente alla NIS2 e privo di efficacia vincolante, ha contribuito a rendere effettivi gli obblighi strategici, di gestione del rischio e di notifica degli incidenti favorendo il coordinamento e la standardizzazione delle pratiche di gestione e segnalazione per rafforzare la consapevolezza e la capacità operativa delle organizzazioni nazionali.

[24] "L'insieme delle attività volte a proteggere reti e sistemi informativi, gli utenti e tutte le persone coinvolte, contro le minacce informatiche». Così art. 2, lett. r), d.lgs 138/2024 e art. 2, punto 1, Regolamento (UE) 2019/881.

[25] In alcuni atti dell'UE, nelle traduzioni ufficiali in lingua italiana è possibile trovare anche il termine "cibersicurezza" o "cybersicurezza", come nel caso dell'AI Act, delle Direttive NIS1 e NIS2, del Cybersecurity Act e del CRA.

[26] M. Pietrangelo, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista italiana di informatica e diritto*, 6(2), 2024, 13 ss.

[27] R. Brighi-P. G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto UE*, in *Federalismi.it*, 8 settembre 2021.

[28] L. Picotti, *Cybersecurity: quid novi?*, in *Diritto di Internet*, 1, 2020, 11 ss.

[29] P.G. Chiara, *Towards a right to cybersecurity in EU law? The challenges ahead*, in *Computer Law & Security Review*, 53, 2024, 105961 ss.

[30] U. Beck, *Risk society. Towards a new modernity*, Londra, 1992.

[31] Direttiva (UE) 2016/1148 del Parlamento europeo e del consiglio del 6 luglio 2016

di carattere generale in materia di sicurezza delle reti e dei sistemi informativi – la produzione normativa europea si è progressivamente intensificata[32] andando a delineare due macro-filoni normativi complementari,[33]che impongono, ai soggetti interessati, obblighi di *cybersecurity*.[34] Il primo filone, definibile normativo-strategico, è volto alla protezione e alla resilienza[35] delle reti e dei sistemi informativi[36]. Esso includeva la Direttiva NIS1, successivamente sostituita dalla Direttiva NIS2[37] (di seguito NIS2), recepita in Italia mediante il d.lgs. 138/2024 (Decreto NIS2)[38], che attualmente ne fa parte, imponendo obblighi armonizzati di gestione del rischio *cyber* e doveri di notifica ai soggetti essenziali e importanti individuati a livello nazionale. Si affianca, a quanto precede, la Direttiva (UE) 2022/2557 sulla

recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[32] Con un'accelerazione notevole dopo il periodo della pandemia da Covid-19.

[33] La normativa *cyber* è estremamente trasversale e multidisciplinare e in questo contesto si richiameranno solo le normative ad applicazione più generalizzata ma per una rapida consultazione del quadro normativo europeo si consideri l'*overview of EU legislative landscape* offerta da ENISA, *Report on the State of the Cybersecurity in the Union*, in *enisa.europa.eu*, 2024.

[34] F. Teichmann-B.S. Sergi, *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in *Computer Law & Security Review*, 59, 2025, 106209 ss.

[35] Per "sicurezza dei sistemi informatici e di rete" si intende «la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi» (art. 6, punto 2, Direttiva NIS2).

[36] Per "sistema informativo e di rete" si intende: (*i*) una rete di comunicazione elettronica ai sensi dell'art. 2, c. 1, lettera vv), del d.l. 259/2003; (*ii*) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; (*iii*) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri (*i*) e (*ii*), per il loro funzionamento, uso, protezione e manutenzione. Si veda l'art. 2, c.1, lett. p), Decreto NIS2, in allineamento con l'art. 6, punto 1, Direttiva NIS2 ed all'art. 1 D.P.C.M. 81/2021 Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informatici e servizi informatici (c.d. DPCM 2) – si noti che quest'ultimo è stato aggiornato dal DPCM 111/2025, ma le modifiche principali riguardano l'aggiornamento dell'Allegato A, con la definizione di nuove macrocategorie di incidenti da segnalare.

[37] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[38] Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

resilienza dei soggetti critici (CER) recepita mediante il d.lgs. 134/2024, che arricchisce l'architettura regolatoria estendendo la logica della resilienza alla dimensione fisica delle infrastrutture, per fronteggiare minacce fisiche e antropiche, oltre a quelle digitali. Completa il quadro il Regolamento (UE) 2022/2554 (DORA), che si configura come *lex specialis* rispetto alla Direttiva NIS2, ma con una verticalizzazione ancora più stringente applicabile al settore finanziario.[39]

Il secondo macro-filone riguarda le normative che si occupano di certificazione e standardizzazione della *cybersecurity* di determinati prodotti ICT, che mirano a stabilire un livello uniforme di fiducia, sicurezza e interoperabilità nel mercato digitale europeo, attraverso la creazione di schemi armonizzati di valutazione. Dette normative richiedono processi di *compliance* finalizzati a verificare che i prodotti rispettino i requisiti minimi fissati dagli *standard* di settore, così da attestare il livello di sicurezza e l'affidabilità informatica del prodotto, garantendone al contempo «autenticità, idoneità e integrità[40] sotto il profilo della sicurezza informatica»[41]. Tra la normativa attualmente applicabile assume particolare rilievo il Cybersecurity Act[42] (successivamente emendato)[43], che impone l'adozione di schemi di certificazione europei per prodotti, servizi e processi ICT, inclusi i "*managed security services*"[44], introducendo altresì *l'European common criteria-based cybersecuri-*

[39] Commissione europea, *Comunicazione C (2023) 6068, Orientamenti sull'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva (UE) 2022/2555 (direttiva NIS2)*, in *eur-lex.europa.eu*, 18 settembre 2023.

[40] Si ritiene importante chiarire che Autenticità e Integrità sono due concetti interconnessi fondamentali in materia. Rispettivamente sono la capacità di garantire che le informazioni e i sistemi informativi siano non alterati, e dunque che i dati e le fonti informative siano ciò che affermano di essere (verificate e affidabili), mentre, l'integrità garantisce l'assenza di modifiche non autorizzate nel tempo.

[41] L'affermazione è ormai condivisa in materia, ma per una panoramica si veda S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, in questa *Rivista*, 2, 2023, 398 ss.

[42] Regolamento (UE) 2019/881 del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

[43] European Council, *Cybersecurity package: Council adopts new laws to strengthen cybersecurity capacities in the EU*, in *consilium.europa.eu*, 2 dicembre 2024.

[44] "Servizi prestati a un terzo consistenti nello svolgimento di attività, o nella fornitura di assistenza per tali attività, legate alla gestione dei rischi in materia di cybersecurity, ad esempio servizi di gestione degli incidenti, test di penetrazione, audit di sicurezza e consulenza, tra cui consulenza specialistica, relativa all'assistenza tecnica». Così l'art. 1, punto 2, lett. b), Regolamento (UE) 2025/37 del Parlamento e del Consiglio del 19 dicembre 2024 che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti.

ty certification scheme (EUCC).[45] Il più recente Regolamento (UE) 2024/2847 Cyber Resilience Act (CRA), entrato in vigore nel dicembre 2024, altrettanto rilevante, diversamente, troverà piena applicazione a partire dall'11 dicembre 2027. Il CRA stabilisce requisiti obbligatori di *cybersecurity* per i prodotti con componenti digitali, sia *hardware* che *software*, prevedendo che i medesimi debbano essere *secure by design* e *by default* da vulnerabilità e minacce informatiche per il loro intero ciclo di vita.

A queste due macro aree di derivazione unionale si aggiunge un terzo livello di intervento, di carattere nazionale, istituito con il d.l. 105/2019 e suoi decreti attuativi[46] (Decreto Perimetro), convertito con modificazioni dalla l. 133/2019, che ha comportato la creazione di un Perimetro di Sicurezza Nazionale Cibernetica (PSNC) finalizzato a garantire un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici da cui dipendono l'esercizio di funzioni essenziali dello Stato e la prestazione di servizi essenziali per attività civili, sociali o economiche fondamentali.

La matrice esclusivamente domestica della normativa è dovuta alla competenza esclusiva degli Stati membri in materia di sicurezza nazionale, come previsto dall'art. 4, par. 2, Trattato sull'Unione Europea (TUE).

Il PSNC è composto da un insieme di organizzazioni, pubbliche e private, che esercitano una funzione o assicurano un servizio essenziale dello Stato (c.d. soggetti perimetro o soggetti PSNC).[47] Esse sono individuate da decreti attuativi, a seconda del settore strategico, sulla base dei criteri di gradualità[48] e dell'analisi del rischio.[49] Le reti, i sistemi informativi, i servizi e i prodotti ICT identificati e comunicati da tali entità sono critici in quanto «dal malfunzionamento, interruzione, anche parziali, ovvero utilizzo

---

[45] Regolamento di esecuzione (UE) 2024/482 della Commissione del 31 gennaio 2024 recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC).

[46] D.l. 105/2019 recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica (c.d. Decreto Perimetro).

[47] Soggetti «da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero assicura la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche» e che «l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici» (art.1, c. 1, Decreto Perimetro).

[48] L'identificazione dei soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (PSNC) è disciplinata dal D.P.C.M. 131/2020, in attuazione dell'articolo 1, comma 2, del d.l. 105/2019. Tale processo si fonda su criteri procedurali e su un principio di gradualità, che tiene conto del potenziale pregiudizio (entità) per la sicurezza nazionale derivante dal malfunzionamento, dall'interruzione o dall'uso improprio di reti, sistemi informativi e servizi ICT.

[49] Art.1. c. 2, Decreto Perimetro.

improprio, potrebbe derivare un pregiudizio per la sicurezza nazionale»[50]. Per questo motivo il PSNC prevede il potere del Presidente del Consiglio dei ministri di disporre la loro disattivazione, parziale o totale, in caso di rischio grave e imminente per la sicurezza nazionale.
I soggetti perimetro hanno obblighi di sicurezza quali l'analisi dei rischi relativi a beni, servizi e funzioni essenziali e l'applicazione di misure di sicurezza elevate,[51] nonché la notifica degli incidenti,[52] al fine di proteggere le infrastrutture vitali da attacchi *cyber* che potrebbero comprometterle. Tali doveri, se disattesi, comportano il rischio dell'irrogazione delle sanzioni previste dell'art. 9 Decreto Perimetro.
Al PSNC è seguita la creazione dell'architettura istituzionale nazionale, definita innanzitutto dal d.l. 82/2021 che ha, *inter alia*, istituito l'ACN quale autorità centrale di coordinamento.[53] Si inserisce, successivamente, la l. 90/2024, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di contrasto ai reati informatici,[54] che amplia il perimetro soggettivo degli obblighi di notifica rispetto al PSNC, introducendo altresì misure di coordinamento tra le amministrazioni pubbliche e nuove funzioni. In particolare, l'articolo 1, c. 1, l. 90/2024 estende gli obbliga di notifica degli incidenti *cyber* un ampio insieme di amministrazioni pubbliche e operatori di servizi essenziali a livello territoriale e locale, tra cui le amministrazioni centrali dello Stato,[55] le regioni, le province autonome,

[50] Art.1, c.1, Decreto Perimetro.

[51] Si tratta di obblighi che discendono da un combinato disposto di norme. Si veda S. Mele, *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano–S. Previti (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, 186; S. Poletti, *La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica*, cit.

[52] La lista deli incidenti da notificare è stata recentemente aggiornata dal DPCM 4 giugno 2025, n. 111 Regolamento recante modificazioni all'allegato A al decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81.

[53] Si veda l'art. 1, c. 1, punto 1, d.l. 82/2021 recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'ACN definisce la cybersicurezza come «l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza».

[54] Per una visione di insieme sulla l. 90/2024 recante Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, si veda S. Mele, *La L. 90/2024 sulla Cybersicurezza in G.U.: tutti gli adempimenti per P.A. e società private,* in *altalex.com*, 3 luglio 2024; G. Fiorinelli, *I "perimetri penali" di cybersicurezza dopo la legge n. 90/2024: dissimmetrie intra-sistematiche ed extra-sistematiche nella tutela penale dei sistemi informatici e telematici di rilevanza pubblica*, in *Cybersicurezza*, 1, 2025, 71 ss.

[55] Individuate ai sensi dell'articolo 1, c. 3, l. 196/2009

le città metropolitane, i comuni di maggiori dimensioni[56] o capoluogo, nonché specifici operatori nei settori del trasporto pubblico e della sanità. La disciplina si estende altresì alle società *in house* dei suddetti enti, qualora operino in ambiti rilevanti, quali i servizi informatici, il trasporto pubblico, la gestione delle acque reflue e dei rifiuti, evidenziando un approccio funzionale basato sulla rilevanza dei servizi erogati.
Sotto il profilo degli obblighi ai sensi dell'art. 1, c. 2, la normativa prevede un meccanismo di notifica che si articola in una segnalazione iniziale (*early warning*), da effettuarsi senza ritardo e comunque entro 24 ore dalla conoscenza dell'incidente, seguita da una notifica completa entro 72 ore contenente tutti gli elementi informativi disponibili, seguendo le fasi previste dal Decreto Perimetro ed in linea anche con la logica europea.
La legge introduce, inoltre, obblighi organizzativi rilevanti, imponendo ai soggetti interessati di dotarsi di una struttura dedicata alla cybersicurezza, se non già presente, e di individuare un referente quale punto di contatto unico con l'ACN, con funzioni di coordinamento e gestione del rischio *cyber* all'interno dell'amministrazione.[57]
La legge 90/2024 ha anticipato alcuni profili poi sistematizzati nel decreto di recepimento della Direttiva NIS2.

2. L'approccio *risk-based* della normativa in materia di *cybersecurity* e di intelligenza artificiale

Le fonti di derivazione unionale che disciplinano le materie connesse alla digitalizzazione articolano, nelle rispettive previsioni normative, approcci differenziati fondati sul modello c.d. *risk-based*. Questo emerge chiaramente dalla lettura delle disposizioni in materia di *cybersecurity*, di intelligenza artificiale (AI Act), di protezione dei dati personali (General Data Protection Regulation - GDPR) e di servizi digitali (Digital Services Act – DSA). Tali normative impongono ai loro destinatari specifici obblighi di *governance* del rischio. Si tratta di una valutazione che viene realizzata attraverso sistemi di gestione del rischio, ovvero mediante un insieme di metodologie, modelli e processi finalizzati a prendere decisioni razionali basate su potenziali opportunità o minacce future.[58] Studi evidenziano come tale approccio

[56] Con popolazione superiore a 100.000 abitanti.

[57] Per ulteriori chiarimenti sulla *ratio* e sulle altre modifiche apportate dalla legge si veda il *Dossier* del Centro Studi della Camera dei Deputati e del Senato della Repubblica, *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici,* 22 maggio 2024.

[58] G. De Gregorio-P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, 59(2), 2022.

consente di prioritizzare ed indirizzare la *compliance* in modo proporzionato al rischio effettivo.[59]

Nella normativa *cyber* rivolta alla protezione delle infrastrutture critiche, l'adozione di programmi di gestione del rischio si configura quale obbligo prodromico imprescindibile. La *ratio* sottesa è quella di mitigare la probabilità che un evento *cyber*[60] possa determinare effetti pregiudizievoli sull'operatività dell'organizzazione, sugli *asset* critici[61] e sui servizi essenziali, con conseguenze che si ripercuotono sulle persone e sulla sicurezza pubblica. A tal fine, le organizzazioni pubbliche e private, individuate dalla normativa, sono tenute a sviluppare una mappatura completa delle attività e dei servizi suscettibili di incidere negativamente sulle reti e sui sistemi informativi connessi, traducendo tale analisi in *policy* di *risk assessment*[62]. Tali obblighi di *governance* si estendono, conseguentemente, alla predisposizione di misure di sicurezza,[63] proporzionate alla gravità del rischio rilevato, e all'osservanza degli obblighi di notifica degli incidenti all'autorità competente (in Italia, ACN).[64] La gestione del rischio implica controlli continui, processi di *audit* e obblighi di adeguamento;[65] in caso di violazioni, è prevista l'irrogazione di sanzioni pecuniarie.

In modo analogo, ma non identico, la normativa che regolamenta la *cyber* resilienza[66] dei prodotti con elementi digitali[67] - questi ultimi qualificati

---

[59] *Ibid.*

[60] "Qualsiasi evento osservabile in una rete o in un sistema informativo»; così ACN, *Domini della cybersicurezza - Event, Threat and Incident Management*, cit.

[61] I soggetti «predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica» trasmettendo tali elenchi all'ACN ai sensi dell'art.1, c. 2, lett. b), Decreto Perimetro.

[62] Art. 21, par. 2, lett. a), Direttiva NIS2; art.1, c. 3, lett. b), Decreto Perimetro.

[63] In particolare, per gli obblighi di adozione delle misure di sicurezza in capo ai soggetti Perimetro il riferimento è il Capo III -Misure di sicurezza del D.P.C.M. 14 aprile 2021, n. 81.

[64] Considerando 97, NIS2; art.1, c. 3, lett. a), Decreto Perimetro.

[65] R. Baskerville-P. Spagnoletti-J. Kim, *Incident-centered information security: Managing a strategic balance between prevention and response*, in *Information & Management*, 51(1), 2014, 138 ss.

[66] Nella traduzione ufficiale dell'UE in lingua italiana viene usato il termine "ciberresilienza", infatti il CRA è anche denominato "legge sulla ciberresilienza".

[67] Ai fini dell'individuazione dell'ambito di applicazione del Cyber Resilience Act (CRA), un prodotto con elementi digitali (c.d. prodotto digitale) rientra nella disciplina del Regolamento qualora siano soddisfatte tre condizioni cumulative. In primo luogo, il prodotto deve integrare la definizione di *product with digital elements*, ossia includere *software* o *hardware* in grado di elaborare dati e di connettersi, direttamente o indirettamente, a reti o dispositivi. Tali prodotti comprendono sia i prodotti finali che i componenti immessi separatamente sul mercato. In secondo luogo, esso deve essere messo a disposizione del

come importanti o critici ai sensi del CRA - introduce un modello di gestione del rischio fondato su requisiti orizzontali di sicurezza, parametrati al grado di rischio associato alla funzione del prodotto e al potenziale impatto sistemico derivante da una sua compromissione. La disciplina relativa all'immissione nel mercato dei prodotti con elementi digitali si fonda su un insieme articolato di obblighi in capo agli operatori economici e, soprattutto, ai fabbricanti, riguardanti le fasi di progettazione, sviluppo e produzione, nonché di adozione di processi strutturati di gestione delle vulnerabilità per l'intero periodo di utilizzo previsto del prodotto (art. 1). Nel contesto del CRA, l'attenzione del legislatore europeo si sposta dalla sicurezza delle reti e dei sistemi, alla sicurezza del prodotto in quanto tale, imponendo che questo sia immesso sul mercato, *inter alia*: (*i*) privo di vulnerabilità sfruttabili[68] note, (*ii*) con una superficie di attacco limitata[69] e (*iii*) in modo tale da non costituire una fonte di rischio per utenti e dati personali, né per altri prodotti, reti e servizi, inclusi i soggetti disciplinati dalla normativa NIS2 e le relative *supply chain*.[70]

mercato UE, secondo la nozione propria del diritto dell'Unione. In terzo luogo, la sua finalità d'uso prevista o ragionevolmente prevedibile deve comportare una connessione, logica o fisica, a un dispositivo o a una rete, rilevante ai fini della valutazione del rischio di *cybersecurity*. Tali elementi, espressamente previsti dall'art. 2, par. 1, CRA, operano congiuntamente e delimitano il perimetro oggettivo di applicazione del Regolamento, fermo restando il sistema di esclusioni stabilito dai paragrafi 2, 3 e 4 del medesimo articolo, che sottrae specifiche categorie di prodotti alla disciplina. Tra le altre cose si consideri che, per applicare la procedura della conformità corretta, bisogna verificare se il prodotto sia classificato come sistema di IA ad alto rischio ai sensi dell'art. 6 AI Act e se esso appartenga alle categorie dei prodotti importanti o critici del CRA.

[68] Dal punto di vista tecnico, la vulnerabilità è intesa come una condizione di fragilità o una debolezza intrinseca di un sistema informativo, suscettibile di essere sfruttata da soggetti malevoli per comprometterne il funzionamento e, quindi, realizzare un attacco, generalmente al fine di trarne un indebito vantaggio. In termini non troppo dissimili l'art. 2, co. 1, lett. ii), d.lgs. 138/2024 (recepimento della NIS2), così come l'art. 2, n. 40), definisce la vulnerabilità descrivendola come «una debolezza, suscettibilità o difetto di prodotti, servizi o processi TIC che può essere sfruttato da una minaccia informatica». Per completezza, si riporta anche la definizione riportata all'art. 3, n. 16, DORA, che guarda la vulnerabilità rispetto all'ambito finanziario specificando che si tratta di «*a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited*».

[69] L'intelligenza artificiale, prodotti con elementi digitali e l'Internet of Things (IoT) emergono come tecnologie capaci di amplificare le vulnerabilità dell'ecosistema *cyber*, estendendo la superficie di attacco e aumentando la complessità dei sistemi esposti: ogni dispositivo connesso funge da potenziale punto di ingresso per cyberattacchi spesso a causa di vulnerabilità tecniche, mancanza degli aggiornamenti o misure di sicurezza deboli.

[70] Artt. 6 e 7 CRA: rispettivamente rubricati "Requisiti per i prodotti con elementi digitali" e "Prodotti con elementi digitali critici". Cfr. Allegato I, parte I relativo ai Requisiti di cibersicurezza relativi alle proprietà dei prodotti con elementi digitali.

Pur configurando il rischio come una caratteristica intrinseca[71] del prodotto digitale, il CRA impone ai fabbricanti di governarlo sin dalla fase di progettazione e lungo l'intero ciclo di vita, mediante un approccio *risk-based*. Esso si traduce, in particolare, in obblighi di valutazione del rischio[72] fondati su parametri giuridicamente rilevanti quali la finalità prevista, l'uso ragionevolmente prevedibile[73] (incluso l'uso improprio ipotizzabile)[74] e la durata attesa del prodotto. Si tratta di elementi espressamente richiamati dall'interpretazione fornita dalla Commissione.[75] Specularmente, il regolamento mira a garantire che utenti e consumatori siano adeguatamente informati sugli *standard* di sicurezza del prodotto sin dal momento dell'acquisto, consentendo loro di poter fare affidamento su prodotti digitali conformi, certificati[76], aggiornati,[77] e, pertanto, in questo senso, *cybersafe*.
L'obbligo generale principale per i fabbricanti è quello di conformarsi ai

[71] R. Leszczyna, *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*, Cham, 2019, 149 ss.

[72] Ai sensi dell'art. 13 CRA, rubricato "Obblighi dei fabbricanti", il fabbricante è tenuto a effettuare una valutazione dei rischi *cyber* che deve essere presa in considerazione durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto. Se il fabbricante integra componenti di terze parti, deve esercitare la dovuta diligenza in modo che tali componenti non compromettano la *cybersecurity* del suo prodotto con elementi digitali. La valutazione del rischio, nonché i mezzi che il fabbricante sceglie per attuare i requisiti essenziali (ad esempio, norme o altre misure tecniche), devono essere inclusi nella documentazione tecnica. Il fabbricante è tenuto a tenere la documentazione a disposizione delle autorità di vigilanza del mercato, in quanto possono richiederla nell'ambito delle loro attività di applicazione.

[73] Ovvero un uso che è probabile possa derivare da un comportamento umano o da operazioni o interazioni tecniche ragionevolmente prevedibili, come previsto dall'art. 2, n. 24), CRA.

[74] L'art. 2, n. 25), CRA lo definisce come «l'uso di un prodotto con elementi digitali in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi ragionevolmente prevedibili».

[75] Commissione Europea, *FAQs on the Cyber Resilience Act*, in *digital-strategy.ec.europa.eu*, 3 dicembre 2025.

[76] Prima dell'immissione sul mercato di un prodotto con elementi digitali, il fabbricante è tenuto a svolgere la procedura di valutazione della conformità prescelta (*conformity assessment*), secondo quanto previsto dal capo III del regolamento. Qualora tale procedura abbia esito positivo, il fabbricante redige la dichiarazione UE di conformità, attestando così il rispetto dei requisiti essenziali di *cybersecurity* applicabili, come definiti nell'allegato I e richiamati, in particolare, dagli artt. 27 e 28 del regolamento, e appone la marcatura CE sul prodotto (artt. 29 e 30).

[77] Il fabbricante deve stabilire un periodo di supporto per il suo prodotto con elementi digitali, durante il quale garantirà che le vulnerabilità di tale prodotto siano gestite in modo efficace, in linea con i requisiti di gestione delle vulnerabilità (cfr. allegato I). La data di fine del periodo di supporto (compresi mese e anno) deve essere chiaramente e comprensibilmente specificata al momento dell'acquisto.

requisiti essenziali di *cybersecurity* di cui all'Allegato I, parte I (cfr. art. 13, par. 1),[78] nonché di implementare processi strutturati di *vulnerability assestment*,[79] divulgazione coordinata delle vulnerabilità e rilascio di aggiornamenti di sicurezza lungo l'intero ciclo di vita del prodotto (Requisiti di processo allegato I, parte II),[80] ai quali si aggiungono obblighi specifici di segnalazione (delle vulnerabilità, degli incidenti e dei quasi-incidenti) al CSIRT competente.[81] Nella prospettiva del CRA, la vulnerabilità non si

[78] L'art. 13 CRA stabilisce che i fabbricanti, al momento dell'immissione sul mercato, devono garantire che i prodotti con elementi digitali siano progettati, sviluppati e realizzati in conformità ai requisiti essenziali di *cybersecurity* di cui all'allegato I. A tal fine, essi sono tenuti a svolgere una valutazione dei rischi *cyber*, i cui risultati devono essere integrati lungo l'intero ciclo di vita del prodotto - dalla pianificazione alla manutenzione - al fine di ridurre i rischi, prevenire gli incidenti e limitarne l'impatto, anche in relazione alla salute e alla sicurezza degli utilizzatori.

[79] Il sistema di valutazione si articola secondo un approccio graduato, proporzionato al livello di rischio associato al prodotto. In linea generale, il fabbricante può ricorrere a procedure di autocertificazione o valutazione da parte di terzi; tuttavia, per determinate categorie di prodotti (prodotti importanti e critici elencati rispettivamente nell'allegato III e nell'allegato IV) considerati rilevanti sotto il profilo della *cybersecurity* quali, ad esempio, *software* di sicurezza, sistemi di gestione delle reti o componenti critici del sistema, è richiesto il rispetto di norme armonizzate oppure l'intervento di un organismo notificato, ossia un soggetto terzo incaricato della valutazione indipendente della conformità. Inoltre, per specifiche categorie di prodotti ritenuti particolarmente critici, tra cui taluni componenti destinati a garantire funzioni di sicurezza avanzate (quali *firewall*, elementi di sicurezza o *hypervisor*), il ricorso alla valutazione da parte di terzi assume carattere obbligatorio (art. 32 e allegato VIII). Tale articolazione riflette la logica del CRA, che combina un approccio *risk-based* con meccanismi differenziati di verifica della conformità, al fine di garantire un elevato livello di sicurezza dei prodotti digitali immessi nel mercato.

[80] Inoltre, assieme al prodotto con elementi digitali, deve fornire anche specifiche informazioni. L'art. 13 e l'Allegato II CRA definiscono un set minimo di informazioni e istruzioni rivolte all'utilizzatore che il fabbricante accompagna ai prodotti con elementi digitali, tra cui: dati identificativi e contatti del fabbricante, punto di contatto per la segnalazione delle vulnerabilità e politica di *disclosure*, caratteristiche e finalità del prodotto, proprietà di sicurezza e rischi prevedibili, durata del supporto e aggiornamenti di sicurezza, nonché istruzioni per l'uso sicuro, l'installazione degli aggiornamenti, la gestione del fine vita e, ove applicabile, l'integrazione in altri sistemi.

[81] Gli obblighi di segnalazione sono obbligatori ai sensi dell'art. 14 CRA. L'articolo in parola prevede che, una volta immesso il prodotto sul mercato, il fabbricante è tenuto a notificare le vulnerabilità sfruttate attivamente e gli incidenti gravi che hanno un impatto sulla sicurezza del prodotto di cui esso viene a conoscenza. In caso di incidente, il fabbricante deve notificare al CSIRT dello Stato membro in cui ha lo stabilimento principale e all'ENISA (entro 24 ore con una rapida segnalazione ed entro 72 ore con una notifica, oltre a successive relazioni da effettuarsi anche a seconda della gravità), mediante una piattaforma unica di comunicazione istituita e gestita dall'ENISA che sarà pienamente operativa da settembre 2026. Il CSIRT ricevente diffonderà la notifica ai CSIRT di altri Stati membri sul cui territorio è presente il prodotto in questione. Gli obblighi di comunicazione si applicano già a tutti i prodotti digitali che sono stati immessi sul mercato UE, dunque anche prima dell'11 dicembre 2027. Inoltre, il successivo art. 15 CRA prevede

configura come un mero fattore eventuale di rischio: la sua gestione non è completamente rimessa alla valutazione del soggetto obbligato, come piuttosto avviene nel sistema di gestione delle vulnerabilità previsto dalla NIS2.[82] La vulnerabilità è un elemento strutturale e intrinseco del prodotto digitale, che deve essere identificato, monitorato e gestito in modo continuo e autonomo rispetto ad altri fattori di rischio, secondo la logica proattiva[83] e proceduralizzata del CRA. Questa impostazione riflette una più ampia evoluzione della *governance* europea della *cybersecurity*, che si sposta da un paradigma centrato sulla resilienza tecnico-organizzativa - tipico delle infrastrutture e dei servizi essenziali - a un modello orientato alla security by design, nel quale la *compliance* è incorporata nella stessa architettura tecnica dei prodotti.[84]

Sebbene, in linea teorica, ogni processo di gestione del rischio dovrebbe muovere dall'identificazione delle vulnerabilità, nel CRA emerge un approccio che può definirsi "atomistico", in quanto incentrato sul singolo prodotto con elementi digitali, in contrapposizione alla logica sistemica propria della normativa NIS2 e, come si dirà, del PSNC.

Il CRA, infatti, disciplina la sicurezza a livello di prodotto, imponendo che ciascun elemento *hardware* o *software* sia progettato, sviluppato e mantenuto aggiornato in modo tale da gestire le proprie vulnerabilità lungo l'intero ciclo di vita, conformemente ai requisiti essenziali di *cybersecurity* e ai processi di *vulnerability handling* previsti dal regolamento.[85] Tuttavia, tale impostazione presuppone un'interazione con la dimensione sistemica: qualora il prodotto digitale o le sue componenti siano utilizzati all'interno di un soggetto rientrante nell'ambito della NIS2 o in contesti critici, anche nazionali - come i soggetti PSNC - essi divengono parte integrante del sistema organizzativo e, come tale, possono rilevare ai fini della gestione del rischio complessivo. Le vulnerabilità del singolo prodotto, pertanto, vengono riportate al contesto in cui esso è inserito.

In questa prospettiva, vulnerabilità e minacce informatiche non restano confinate alla dimensione tecnica, ma si proiettano nel sistema-organiz-

anche le segnalazioni volontarie che possono essere fatte da qualsiasi persona fisica o giuridica notificando le vulnerabilità, le minacce informatiche, gli incidenti e i quasi incidenti attraverso la suddetta piattaforma unica di comunicazione. Si veda Commissione Europea, *Legge sulla ciberresilienza - Sintesi del testo legislativo*, in *digital-strategy.ec.europa.eu*, 3 dicembre 2025.

[82] Art. 21 NIS2 trasposto nell'art. 24, c. 2, lett. e), Decreto NIS2.

[83] J. Ruohonen-P. Timmers, *Vulnerability coordination under the Cyber Resilience Act*, in *Applied Cybersecurity & Internet Governance*, 2025.

[84] ENISA, *Coordinated Vulnerability Disclosure Policies in the EU*, in *enisa.europa.eu*, aprile 2022.

[85] J. Ruohonen-P. Timmers, *Vulnerability coordination under the cyber resilience act*, in Applied Cybersecurity & Internet Governance, 4(1), 2025.

zazione, contribuendo a determinarne il livello di esposizione al rischio e attivando, conseguentemente, i relativi obblighi di gestione previsti dalle normative di riferimento. Il CRA è destinato a configurarsi come un punto di riferimento per i prodotti digitali "a marchio CE"[86] - analogamente al ruolo svolto dal GDPR nell'ambito della protezione dei dati personali contribuendo alla progressiva standardizzazione europea dei requisiti di sicurezza digitale[87] e minimizzazione di rischi nel mercato interno.[88] La mancata conformità ai requisiti essenziali di *cybersecurity* e agli ulteriori obblighi previsti dal CRA può comportare, infatti, sanzioni pecuniarie significative, limitazioni o divieti di commercializzazione del prodotto, nonché potenziali forme di responsabilità, rafforzando la natura cogente della disciplina.[89]

Nel contesto nazionale, il quadro della gestione del rischio *cyber* è ulteriormente rafforzato dal Perimetro di Sicurezza Nazionale Cibernetica (PSNC), istituito dal d.l. 105/2019 (Decreto Perimetro), convertito con modificazioni dalla l. 133/2019 (Legge Perimetro), con l'obiettivo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi ICT[90] delle amministrazioni pubbliche e degli operatori pubblici e privati che svolgono funzioni essenziali o erogano servizi essenziali per lo Stato. In particolare, il Perimetro si applica ai soggetti da cui dipende l'esercizio di funzioni fondamentali dello Stato o la prestazione di servizi essenziali per il mantenimento di attività civili, sociali ed economiche di rilevanza strategica, il cui malfunzionamento, interruzione o uso im-

[86] La Commissione Europea ha specificato che i prodotti interessati recheranno la marcatura CE per indicare la conformità *cyber* ai requisiti del CRA, mentre le autorità nazionali di vigilanza del mercato garantiranno l'applicazione delle relative disposizioni. In generale, il "marchio CE" compare già su molti prodotti commercializzati nel mercato unico esteso dello Spazio Economico Europeo ed indica che sono stati valutati come conformi a elevati requisiti di sicurezza, salute e tutela dell'ambiente. Si veda Commissione Europea, *Cyber Resilience Act,* in *digital-strategy.ec.europa.eu*, 3 dicembre 2025.

[87] I. Kamara, *Standardizing personal data protection*, Oxford, 2025; I. Kamara, *European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience*, in *Innovation: The European Journal of Social Science Research*, 37(5), 2024, 1441 ss.

[88] P. Car-S. De Luca, *EU Cyber resilience act*, European Parliament Research Service, in *europarl.europa.eu*, dicembre 2024.

[89] Per una panoramica più approfondita della disciplina del CRA, anche in merito ai requisiti orizzontali di *cybersecurity*, si rimanda a F. Teichmann-B.S. Sergi, *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in *Computer Law & Security Review*, 59, 2025; P.G. Chiara, *Understanding the regulatory approach of the Cyber Resilience Act: protection of fundamental rights in disguise?*, in *European Journal of Risk Regulation*, 16(2), 2025, 469 ss.

[90] Ai sensi dell'art. 1, lett. l), D.P.C.M. 131/2020 il "Servizio informatico" è «un servizio consistente interamente o prevalentemente nel trattamento di informazioni, per mezzo della rete e dei sistemi informativi, ivi incluso quello di cloud computing».

proprio possa comportare un pregiudizio per la sicurezza nazionale (art. 1, c. 1 e 2, Decreto Perimetro). I soggetti inclusi nel PSNC, individuati mediante criteri e procedure stabiliti dal D.P.C.M. 131/2020,[91] operano in settori strategici quali interno, difesa, energia, telecomunicazioni, trasporti, economia e finanza, spazio e aerospazio, tecnologie critiche e servizi digitali, enti previdenziali e del lavoro (art. 3, c. 1), e sono tenuti a predisporre e aggiornare periodicamente un inventario dettagliato delle reti, dei sistemi informativi e dei servizi ICT di propria pertinenza - come previsto dall'art.1, c. 2, lett. b), Decreto Perimetro[92] - comprensivo della relativa architettura e componentistica.[93] Tali elenchi assumono un ruolo centrale nella gestione del rischio, in quanto consentono l'identificazione degli *asset* critici da cui dipendono funzioni e servizi essenziali, nonché la valutazione delle vulnerabilità suscettibili di incidere sulla sicurezza nazionale. Tale obbligo si inserisce in una logica di gestione del rischio fondata sull'identificazione degli *asset* critici da cui dipendono funzioni e servizi essenziali e sulla valutazione delle possibili conseguenze derivanti da mal-

[91] Un soggetto è qualificato come rilevante, ai sensi dell'art. 2, c. 1, lett. a) e b), D.P.C.M. 131/2020, quando esercita una funzione essenziale dello Stato o fornisce un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali. Nel primo caso, si tratta di soggetti ai quali l'ordinamento attribuisce compiti volti a garantire la continuità dell'azione di Governo e degli organi costituzionali, nonché la tutela della sicurezza interna ed esterna, della difesa dello Stato, delle relazioni internazionali, dell'ordine e della sicurezza pubblica, dell'amministrazione della giustizia e del corretto funzionamento dei sistemi economico-finanziari e dei trasporti. Nel secondo caso, rientrano invece i soggetti che svolgono attività strumentali all'esercizio di tali funzioni, attività necessarie per l'esercizio e il godimento dei diritti fondamentali, per la continuità delle forniture e l'efficienza delle infrastrutture e della logistica, nonché attività di ricerca e produzione, in particolare nei settori ad alta tecnologia o in altri ambiti di rilevanza economica e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico . Tale duplice qualificazione assume rilievo centrale nella prospettiva della gestione del rischio, in quanto individua i soggetti la cui esposizione a vulnerabilità può tradursi in un impatto sistemico e, in ultima istanza, in un pregiudizio per la sicurezza nazionale. L'elenco dei soggetti inclusi è stato adottato con atto amministrativo del Presidente del Consiglio dei ministri, su proposta del Comitato Interministeriale per la Cybersicurezza. L'elenco viene aggiornato, ma non è soggetto a pubblicazione ed è sottratto al diritto di accesso, fermo restando l'obbligo di comunicazione individuale ai soggetti interessati.

[92] Il riferimento all'art. 1, c. 2, lett. b), Decreto Perimetro trova attuazione nell'art. 7 D.P.C.M. 131/2020, che disciplina i criteri e le modalità procedurali per la predisposizione e l'aggiornamento di tali elenchi.

[93] Per "Architettura e componentistica" l'art. 1, lett. n), D.P.C.M. 131/2020 intende «l'insieme delle architetture realizzate e dei componenti usati a livello di rete, dati e software, ivi inclusi la distribuzione su piattaforme di cloud computing, nonché le procedure e i flussi informativi per l'accesso, acquisizione, trasmissione, conservazione, elaborazione e recupero dei dati necessari all'espletamento dei servizi informatici».

funzionamenti o compromissioni.[94] In questo quadro, il PSNC introduce obblighi specifici di sicurezza e di notifica degli incidenti al CSIRT Italia,[95] nonché l'adozione di misure tecniche e organizzative volte a garantire un elevato livello di protezione, in linea con gli *standard* europei e internazionali. Tra questi, i soggetti Perimetro sono tenuti a permettere di effettuare uno «screening tecnologico degli approvvigionamenti ICT appartenenti a categorie specifiche destinati ai beni ICT perimetro».[96] Si tratta, di fatto, di un obbligo di notifica preventiva in relazione alle procedure di approvvigionamento di beni, sistemi e servizi ICT destinati a essere impiegati su *asset* strategici rientranti in specifiche categorie individuate dalla normativa di attuazione. In particolare, i soggetti devono comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN) l'intenzione di procedere all'affidamento, anche per il tramite di centrali di committenza, di forniture relative a beni, sistemi e servizi ICT rientranti nelle categorie individuate dal D.P.C.M. 15 giugno 2021, prima dell'avvio della procedura di gara o della conclusione del contratto.

Il CVCN, istituito presso l'ACN, ha, infatti, il compito di valutare preventivamente la sicurezza dei beni, sistemi e servizi ICT destinati ad essere impiegati nel Perimetro, verificando, in particolare, le caratteristiche di *security by design* e l'assenza di vulnerabilità note.[97] Tale obbligo si inserisce in una

[94] Nel PSNC la nozione di pregiudizio per la sicurezza nazionale è intesa come danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche che ne costituiscono il fondamento, nonché agli interessi politici, militari, economici, scientifici e industriali dello Stato, derivante dall'interruzione o dalla compromissione di una funzione essenziale o di un servizio essenziale. A tal fine, il concetto di compromissione è definito dall'art. 1, lett. f) e g), D.P.C.M. 131/2020 come la perdita di sicurezza o di efficacia nello svolgimento di tali funzioni o servizi, connessa al malfunzionamento, all'interruzione, anche parziale, o all'uso improprio di reti, sistemi informativi e servizi ICT. Tale definizione risulta particolarmente rilevante nella prospettiva della gestione del rischio *cyber*, in quanto esplicitano il nesso tra vulnerabilità tecnica, compromissione operativa e danno sistemico, contribuendo a qualificare il rischio non solo in termini economici-probabilistici, ma anche in relazione al suo impatto sugli interessi fondamentali dello Stato e sul prestigio della funzione pubblica.

[95] Per una panoramica in materia si rimanda a S. Mele, *Il perimetro di sicurezza nazionale cibernetica e il nuovo "golden power". Dalla compliance delle aziende e della pubblica amministrazione alla sicurezza nazionale*, in G. Cassano–S. Previti (a cura di), *Il diritto di Internet nell'era digitale*, Milano, 2020, 186.

[96] Per ulteriori chiarimenti e per l'evoluzione delle *policy* e della normativa *cyber* nazionale si veda Senato della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza* (riferita al 2020), Doc. XXXIII n. 3, 97 ss.

[97] Il CVCN definisce, inoltre, metodologie di test e verifica, contribuisce alla definizione delle misure di sicurezza e può imporre condizioni e prescrizioni specifiche per l'utilizzo dei prodotti, anche avvalendosi di laboratori accreditati. Si noti che si tratta di procedure complesse, anche composta da varie fasi di *assesment* del rischio *cyber* e delle vulnerabilità, per la quale si rimanda al D.P.R. 54/2021.

logica di gestione proattiva del rischio, consentendo al CVCN di effettuare valutazioni preliminari in ordine alla sicurezza delle soluzioni tecnologiche proposte, con particolare riferimento alla presenza di vulnerabilità e alla loro idoneità rispetto al contesto di impiego. In questo senso, la fase di *procurement* diviene un momento importante di controllo del rischio *cyber*, in cui la sicurezza dei prodotti e dei servizi ICT è verificata *ex ante*, contribuendo a prevenire l'introduzione di elementi vulnerabili all'interno di infrastrutture strategiche che possono annidarsi nelle *supply chain*.

Il PSNC, a livello domestico, è uno strumento di rafforzamento della sicurezza nazionale che integra, e in parte amplia, l'ambito applicativo della normativa unionale, includendo anche soggetti, prodotti e processi che non rientrano necessariamente nella sua disciplina. In molti casi, tuttavia, i soggetti NIS2 coincidono con quelli del Perimetro - nonché con quelli della l. 90/2024 - determinando una sovrapposizione funzionale tra i due regimi, soprattutto in relazione agli obblighi di gestione del rischio e di notifica degli incidenti al CSIRT Italia. Se la NIS2 opera sul piano della resilienza infrastrutturale e il CRA su quello della sicurezza del prodotto, il Perimetro introduce una dimensione strategico-nazionale, in cui la gestione del rischio è orientata alla tutela della sicurezza dello Stato. In tale prospettiva, emerge chiaramente come il prodotto digitale diventi un elemento critico anche all'interno dei sistemi inclusi nel PSNC: le fragilità *cyber* del singolo prodotto, infatti, possono mettere a rischio la sicurezza nazionale, confermando la centralità di un approccio integrato e proattivo alla *cybersecurity*, fondato sulla formazione, sulla valutazione continua del rischio e sulla gestione strutturata delle vulnerabilità. La *cybersecurity law* si inserisce, di conseguenza, in modo sempre più coerente e trasversale nel più ampio ecosistema normativo europeo e nazionale del digitale, contribuendo a completarlo, a rafforzare le discipline esistenti e ad assumere un ruolo progressivamente centrale, favorendo un'integrazione sistemica.

In particolare, il CRA si coordina direttamente con la regolazione dell'intelligenza artificiale, come emerge dall'art. 12, che prevede espressamente una presunzione di conformità dei prodotti digitali che sono anche sistemi di IA ad alto rischio ai sensi dell'AI Act. Attraverso tale disposizione, il legislatore europeo realizza un coordinamento che consente di integrare i requisiti di *cybersecurity* del CRA all'interno del più ampio *framework* di gestione del rischio dei sistemi di IA, confermando il ruolo del prodotto digitale quale nuovo *standard* tecnico[98] su cui si innestano i sistemi complessi. Ne deriva, pertanto, un modello regolatorio integrato e multilivello, in cui la sicurezza dei prodotti (ai sensi del CRA, che tutela altresì la protezione dei dati personali), la resilienza dei sistemi e dei servizi critici (ai sensi della

[98] Per maggiori chiarimenti, si veda I. Kamara-M. Bassini, *The cybersecurity and AI nexus in the EU digital acquis*, in questa *Rivista*, 1, 2025, 312 ss.

NIS2 e della normativa *cyber* nazionale) e la gestione del rischio nei sistemi di intelligenza artificiale (ai sensi dell'AI Act) operano in modo coordinato e interdipendente. Se il CRA stabilisce quali prodotti digitali sono tecnicamente conformi agli *standard* UE, la normativa in materia di intelligenza artificiale si concentra sui rischi per i diritti fondamentali e la sicurezza derivanti dall'uso di tali sistemi. L'AI Act organizza il quadro regolatorio secondo una struttura piramidale articolata in quattro livelli (inaccettabile, ad alto rischio, a rischio limitato e a rischio minimo), modulando gli obblighi in funzione della gravità del rischio connesso all'uso del sistema di AI e alle sue potenziali conseguenze. Il legislatore unionale ha ritenuto di dover vietare determinate pratiche inaccettabili, mentre ha stabilito requisiti specifici per i sistemi ad alto rischio (tra i quali quello di *cybersecurity*) e obblighi per gli operatori (cfr. considerando 26 AI Act). I principi di proporzionalità e trasparenza, coniugati con l'approccio basato sul rischio, garantiscono la tutela dei diritti fondamentali, senza ostacolare indebitamente i benefici che l'innovazione tecnologica può offrire.[99]

Sebbene sia la *cybersecurity* che l'AI adottino un paradigma regolatorio "*risk-based*", le modalità concrete di applicazione divergono: i sistemi di gestione del rischio consentono di tradurre in obblighi operativi un rischio che, a seconda delle finalità, dell'assetto decisionale del legislatore e della natura del rischio, può presentarsi come più o meno identificato.[100] In questo senso è fondamentale distinguere tra rischi e incertezze. Alcuni studiosi definiscono i rischi come "*known knowns*", ovvero eventi prevedibili per i quali è possibile stimare probabilità e impatti; le incertezze sono invece "*known unknowns*", situazioni note come ignote, non quantificabili, in quanto gli effetti di una specifica tecnologia non sono attualmente prevedibili. Vi è poi la dimensione degli "*unknown unknowns*", fenomeni dai quali non si sospettano, allo stato, neppure le possibili conseguenze avverse.[101]

Nel contesto della normativa *cyber* del macro-filone strategico (NIS2, CER, DORA), la responsabilità dell'identificazione e della valutazione del rischio è attribuita direttamente ai soggetti obbligati. Le organizzazioni, in quanto esperte del proprio assetto e contesto, sono chiamate a selezionare, prioritizzare e gestire i rischi in funzione della probabilità e dell'impatto. Nel CRA, questa libertà decisionale risulta notevolmente attenuata.[102]

---

[99] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, in *European Journal of Risk Regulation*, 16(2), 2025, 684 ss.

[100] A. Gullo, *Compliance*, cit., 1 ss.

[101] J. Black., *The role of risk in regulatory processes*, in R. Baldwin-M. Cave-M. Lodge (a cura di), *The Oxford Handbook of Regulation*, Oxford, 2010, 302 ss. e 310. Così anche M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[102] F. Teichmann-B.S. Sergi, *The EU Cyber Resilience Act: Hybrid governance, compliance, and cybersecurity regulation in the digital ecosystem*, in *Computer Law & Security Review*, 59, 2025,

Nell'AI Act, invece, per ogni sistema di AI ad alto rischio, il fornitore deve prevedere un sistema di gestione dei rischi che operi in modo «iterativo, pianificato e continuo» per l'intero ciclo di vita del sistema (dalla progettazione, allo sviluppo, al rilascio, all'aggiornamento e al ritiro), che tenga conto della finalità e del contesto dello stesso. Tale processo ha la finalità di identificare, stimare, valutare e mitigare non solo i rischi noti relativi all'uso conforme alla finalità prevista, ma anche i rischi derivanti da usi «impropri ragionevolmente prevedibili», ossia scenari conseguenti a comportamenti umani prevedibili in contesti reali.[103] In altre parole, questo vuol dire prevedere attaccanti o eventi *cyber* che possano usare il sistema di AI per scopi diversi o in modo errato, sebbene non esplicitato dalla normativa. Le decisioni del fornitore su quali misure di mitigazione adottare per i sistemi di AI ad alto rischio, e in quali casi accettare un rischio residuo, devono essere giustificate, documentate e, se appropriato, basate sul coinvolgimento di esperti o *stakeholder* esterni. Differentemente, il sistema di gestione del rischio previsto nella NIS2 tende alla verticalizzazione all'interno dell'organizzazione obbligata.

Le istruzioni per l'uso fornite dal fornitore di sistemi di AI ad alto rischio devono includere gli scenari di utilizzo improprio prevedibile, in modo che il *deployer* sia consapevole dei rischi potenziali. La normativa *cyber*, invece, prevede formazione del personale dell'organizzazione e l'aggiornamento continuo della sicurezza dei prodotti digitali. Le misure di mitigazione attuate nel contesto dell'AI Act devono riflettere lo stato dell'arte (normativo e tecnologico) e, in caso di rischi residui, non è richiesto che il fornitore eroghi formazione all'utenza o preveda addestramenti aggiuntivi al sistema stesso, benché tali accorgimenti siano incoraggiati, quando utili, per attenuare gli usi impropri ragionevolmente prevedibili. Il sistema di gestione dei rischi dei sistemi di AI ad alto rischio deve essere periodicamente riesaminato e aggiornato per garantirne costantemente l'efficacia, e ogni scelta significativa nel processo deve essere documentata, così da poter dimostrare conformità alle autorità regolatorie. I soggetti obbligati ai sensi dell'AI Act, dunque, non sono esenti da una valutazione del rischio: al contrario, essi devono effettuare una più complessa analisi di impatto[104] per tutti quei sistemi che potrebbero portare a lesioni dei diritti fondamentali e discriminazioni derivanti da decisioni automatizzate.[105]

A differenza del rischio *cyber*, di derivazione principalmente tecnocentrica,

106209 ss.

[103] Cfr. consideranda 64 e 65 e art. 9 AI Act.

[104] *Ibid.*

[105] O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali,* 43(3), 2023, 569 ss.; O. Pollicino-P. Dunn, P., *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Milano, 2024.

quello preso in considerazione in materia di AI è un rischio di derivazione antropocentrica. Nella normativa sulla *cybersecurity* l'attenzione è rivolta, tra l'altro, a vulnerabilità, attacchi all'integrità delle catene di fornitura, ai difetti infrastrutturali o dei sistemi, processi e prodotti ICT, alla difesa e resilienza delle componenti logiche e fisiche dei sistemi informativi e delle reti. Il legislatore interviene imponendo misure di sicurezza, obblighi di aggiornamento, *standard* tecnici, certificazioni e notifiche obbligatorie. Nel corso dei negoziati sull'AI Act, il legislatore europeo si è confrontato con la complessa individuazione dei criteri idonei a determinare quando un sistema di intelligenza artificiale possa essere considerato portatore di un rischio inaccettabile per gli individui, nonché con la definizione delle pratiche da vietare e delle categorie di sistemi da qualificare come "ad alto rischio" per la società, ammissibili solo a determinate condizioni. In tale contesto, è emersa una criticità degli approcci basati sul rischio, consistente nella difficoltà di raggiungere un consenso condiviso sia sull'individuazione dei rischi rilevanti sia sulla loro graduazione in termini di gravità. Questo processo ha alimentato un ampio dibattito a livello europeo, evidenziando le sfide connesse alla regolazione di una tecnologia in rapida evoluzione, ancora caratterizzata da limitate evidenze empiriche circa i suoi impatti sociali.[106]
L'AI Act e la Legge AI nazionale non lasciano il compito di valutare i punteggi di rischio ai soggetti obbligati, ma identificano e classificano direttamente le diverse categorie di rischio in modalità "*top-down*".[107]

2.1 Modalità di valutazione del rischio della normativa cyber e di intelligenza artificiale

La gestione del rischio *cyber* non riguarda la sola gestione del rischio tecnico. Nel 2025, il 95% degli attacchi *ransomware* ha colpito soggetti privi di particolari obblighi normativi o appartenenti a settori considerati a minore criticità, mentre solo il 5% ha interessato operatori soggetti a regimi normativi specifici.[108] Da questi dati si evince l'importanza della normativa *cyber*, che prevede un sistema di gestione adattabile al contesto, anche per quelle organizzazioni che, pur non essendo obbligate alla *compliance* normativa NIS2, e tantomeno al CRA o al PSNC, possono trovare nella *cybersecurity law* un sistema consolidato e integrato, basato sull'analisi com-

[106] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[107] G. De Gregorio-P. Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, cit.

[108] Quali il PSNC, la NIS, la normativa Telco, la l. 90/2024, il DORA e il CRA.

plessiva del rischio informatico.[109]
Per mitigare il rischio di compromissione dei sistemi informativi e di rete, la normativa NIS2 prevede un modello di gestione del rischio con obblighi di sicurezza calibrati sul livello di rischio effettivo al quale ciascun soggetto è esposto.[110] In particolare, il decreto NIS2 impone a soggetti essenziali e importanti[111] - individuati sulla base degli Allegati I-IV - di adottare misure tecniche, operative e organizzative adeguate e proporzionate per garantire la sicurezza delle reti e dei sistemi informativi utilizzati nello svolgimento delle proprie attività o nella fornitura dei loro servizi per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per gli altri.[112]
Tale obbligo risponde, ai sensi dell'art. 24, c. 1, decreto NIS2, a due principi: (*i*) il principio di adeguatezza, che richiede di considerare le «conoscenze più aggiornate e lo stato dell'arte» nell'individuazione delle misure di sicurezza - dunque tecnologie, normative e *standard* di riferimento[113] e (*ii*) il principio di proporzionalità, che impone alle organizzazioni di calibrare le misure «al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico».
La normativa impone, inoltre, precisi obblighi di comunicazione in caso di incidente significativo:[114] una pre-notifica al CSIRT Italia[115] entro 24 ore dalla conoscenza dell'evento, una notifica completa entro 72 ore, e la trasmissione di una relazione finale dettagliata che descriva causa, impatto e misure adottate (art. 25, Decreto NIS2). Tale valutazione si inserisce in una più ampia funzione di responsabilizzazione dei vertici e della *governance* dell'organizzazione (art. 23, Decreto NIS2), che sono chiamati non solo a deliberare l'adozione delle misure di gestione del rischio, ma anche a sorvegliare sull'attuazione e sul continuo aggiornamento delle stesse, raf-

[109] Si veda ACN, *Operational Summary del 1° semestre 2025*, cit.

[110] *Ibid.*

[111] La normativa si applica a diciotto settori critici suddivisi in due categorie: undici settori essenziali e sette settori importanti.

[112] Art. 24 d.lgs. 138/2024.

[113] *Ibid.*

[114] Per la normativa NIS2 deve trattarsi di incidenti significativi. Ai sensi dell'art. 25, c. 4, Decreto NIS2 un incidente è considerato significativo se: (*i*) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; (*ii*) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

[115] Il CSIRT Italia, in caso di incidenti *cyber* o notifiche di eventi, è l'interlocutore unico per tutti i soggetti pubblici e privati in quanto destinatario delle notifiche obbligatorie e segnalazioni volontarie previste dalla normativa *cyber*.

forzando così l'efficacia complessiva della sicurezza informatica dell'organizzazione.

La possibilità che le minacce informatiche[116] divengano incidenti si verifica quando viene sfruttata con successo una vulnerabilità dell'organizzazione. In un contesto di dipendenza dalle reti e sistemi informativi, eventi quali «l'accesso non autorizzato ai dati, la loro divulgazione senza consenso, la manipolazione o la distruzione costituiscono minacce concrete in grado di produrre conseguenze dannose non solo per la singola organizzazione, ma per l'intera società e l'economia del Paese, ad esempio in caso di blocco di servizi critici».[117]

Il rischio è «la combinazione dell'entità dell'impatto di un incidente[118], in termini di danno o di perturbazione, e della probabilità che esso si verifichi» (decreto NIS2).[119] In altre parole, è definito «dall'impatto della minaccia su un determinato bene, persona o valore, tenuto conto del grado della probabilità che tale evento si verifichi»:[120] una definizione, questa, riportata in termini analoghi dall'art. 3, par. 2, AI Act.

La formula concettuale Rischio = Probabilità × Impatto è coerente anche ai più comuni *standard* internazionali di settore quali la ISO e il *framework* NIST ed è un'utile formulazione del concetto ai sensi della normativa *cyber* e di AI nazionale ed unionale. Resta, tuttavia, un punto di partenza: la formula, infatti, deve essere letta in senso dinamico, potendo integrare pesi, fattori correttivi e ponderazioni che riflettano la specificità, ad esempio, del contesto organizzativo, della natura dei servizi e del livello di esposizione alle minacce.

A livello operativo, l'art. 24 Decreto NIS2 richiede che le misure di sicurezza siano adattate a fattori tecnologici (livello di interconnessione, dipendenze infrastrutturali), organizzativi (dimensioni, natura dei servizi

---

[116] Art. 2, lett. bb), d.lgs 138/ 2024, definizione di "minaccia informatica": «Qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone, così come definita dall'art. 2, punto 8), Regolamento (UE) 2019/881».

[117] ACN, *Domini della cybersicurezza - Event, Threat and Incident Management*, cit.

[118] Art. 2, par.1, lett. t), Decreto NIS. L'incidente è quell'«evento che compromette la disponibilità, autenticità, integrità o riservatezza dei dati o dei servizi offerti o accessibili tramite reti e sistemi informativi» e che la *cybersecurity* vuole evitare.

[119] Similmente, ai sensi dell'art. 3, par. 37, Regolamento (UE) 2024/2847 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (CRA) il rischio *cyber* è «la potenziale perdita o perturbazione causata da un incidente da esprimersi come combinazione dell'entità di tale perdita o perturbazione e della probabilità che si verifichi l'incidente».

[120] M.A. Rizzi-F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 6(2), 2024, 115 ss.

erogati) ed economico-sociali (impatto potenziale sulla collettività e sulla sicurezza nazionale). Sono questi fattori di contesto a riempire di significato - e successivamente a rendere calcolabile - le due variabili della "probabilità" e dell'"impatto".

In attuazione dell'art. 31, c.1, Decreto NIS,[121] la Determinazione di ACN n. 164179/2025 ha fornito una mappatura delle misure di sicurezza di base[122] - oltre che di incidenti significativi - e le tempistiche per la loro applicazione, distinguendo tra requisiti di natura organizzativa (es. processi di *risk assessment*, procedure di gestione degli incidenti, ruoli) e requisiti tecnologici (es. strumenti di monitoraggio, cifratura, autenticazione multifattore), ribadendo che nella *cybersecurity* occorre un adattamento al contesto specifico del soggetto obbligato[123]. La prevalenza di misure per i soggetti essenziali rispetto a quelli importanti è coerente con il principio di proporzionalità della NIS2. Il maggior numero di misure organizzative rispetto a quelle tecniche, rispondono anche all'esigenza di efficienza e contenimento dei costi. Le misure di base identificate da ACN rispondono ad un obbligo, ma allo stesso tempo supportano le organizzazioni offrendo una prima interpretazione nella predisposizione degli elementi di gestione del rischio previsti dalla normativa, quali, ad esempio: (*i*) l'applicazione di politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete; (*ii*) le misure di gestione degli incidenti, incluse le notifiche agli organi competenti; (*iii*) i piani di continuità operativa e *disaster recovery*; (*iv*) i requisiti di sicurezza per la *supply chain* e per l'acquisizione, lo sviluppo e manutenzione dei sistemi; pratiche di sicurezza di base e formazione del personale[124]. Infatti, se da un lato questa normativa offre il vantaggio di non richiedere una modalità specifica per la loro applicazione, dall'altro può risultare complessa a quelle organizzazioni con un livello di *cyberculture* non ancora maturo.[125]

Il rischio *cyber* si distingue per la rapidità con cui può produrre effetti negativi su *asset* e persone, per la capacità di propagazione su scala globale e per l'elevato grado di interconnessione che ne amplifica la portata. A ciò

[121] La disposizione prescrive che ACN debba «stabilire obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico».

[122] Si veda *Framework Nazionale per la Cybersecurity e la Data Protection - Edizione 2025 (v2.1)*, in *cybersecurityframework.it*.

[123] ACN, *Modalità e specifiche di base*, in *acn.gov.it*.

[124] Art. 24, c. 2, d.lgs. 138/2024.

[125] M.A. Adamu-M.I. Niemimaa-P. Spagnoletti, *Towards a Three-Tiered Framework for Fostering Organizational Cybersecurity Culture*, in M. Themistocleous-N. Bakas-G. Kokosalakis-M. Papadaki (a cura di), *Information Systems. EMCIS 2024. Lecture Notes in Business Information Processing, vol 536*, Cham, 2025, 313 ss.

si aggiunge l'elemento intenzionale, rappresentato da attori malevoli che possono sfruttare le vulnerabilità tecniche, le persone, le reti e i sistemi informativi per finalità illecite.
In questo senso la dottrina[126] parla di un approccio al rischio *cyber* multidimensionale, dinamico ed integrato che deve essere parte della cultura organizzativa, che supera la logica della *compliance checklist* per orientarsi verso una vera e propria *risk governance* adattiva, in grado di coniugare obblighi giuridici e valutazioni tecnico-organizzative in un quadro di responsabilità condivisa tra operatori, Autorità di settore e ACN dove il contesto organizzativo è la chiave per comprendere i rischi ai quali va incontro l'organizzazione.
L'AI Act parte da una prospettiva differente. Il Regolamento in parola valuta i rischi connessi all'uso dell'AI e li categorizza per gravità: "inaccettabile" (e quindi pratiche vietate), "rischio alto", "rischio limitato" e "minimo o nullo".
L'art. 5 AI Act elenca i sistemi di AI[127] che devono essere eliminati dal mercato in quanto ritenuti una minaccia alla sicurezza, ai diritti fondamentali e alla vita delle persone ai sensi della Carta dei diritti fondamentali dell'UE. In particolare, sono vietati quei sistemi di AI che mirano a manipolare, discriminare o sorvegliare gli individui in modi sistematici. Tra questi rientrano quelli che usano tecniche subliminali o ingannevoli per alterare decisioni consapevoli degli individui; che sfruttano vulnerabilità personali - per età, disabilità, status socio-economico - per influenzarne il comportamento; che valutano o classificano le persone sulla base del loro comportamento sociale o della personalità, anche mediante riconoscimento facciale (identificazione biometrica remota in tempo reale) o sono capaci di riconoscere le emozioni nei luoghi di lavoro ecc.
Al secondo livello della piramide di rischio si trovano i sistemi di AI ad alto rischio. Questi sistemi vengono utilizzati in settori considerati critici che, per finalità o per il loro impatto sistemico, possono incidere significativamente sui diritti fondamentali, sulla sicurezza o sulla salute pubblica. È il caso, ad esempio, dei sistemi usati per la diagnosi medica o per la guida autonoma dei veicoli.
Prima di immettere un sistema di AI ad alto rischio sul mercato UE o di farlo entrare in servizio, i fornitori dovranno dimostrare che il loro sistema è affidabile e conforme ai requisiti richiesti per l'AI in relazione a qualità

[126] A. Gullo, *Compliance*, cit., 1 ss.

[127] Il sistema di intelligenza artificiale, ai sensi dell'art. 3, par. 1, AI Act, è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

dei dati, documentazione e tracciabilità, obblighi di trasparenza, sorveglianza umana in ogni fase critica, accuratezza, *cybersecurity* e robustezza dei sistemi.[128]
Inoltre, l'art. 9, rubricato "Sistema di gestione dei rischi", impone ai fornitori di sistemi AI ad alto rischio di condurre una valutazione d'impatto comprendente l'identificazione e l'analisi dei rischi prevedibili per salute, sicurezza o diritti fondamentali e, sulla base di tale valutazione, di istituire un sistema di gestione del rischio che accompagni il sistema per tutto il ciclo di vita, mediante misure mirate a mitigare i rischi identificati. Mentre la valutazione del rischio riguarda l'identificazione, l'analisi e la valutazione dei rischi legati all'AI, l'analisi d'impatto comprende conseguenze più ampie, ad esempio, su diversi *stakeholder* - utenti, società - e ambientali.[129]
Per quanto riguarda i sistemi di AI che presentano rischi ridotti, come *chatbot* o strumenti che generano contenuti, questi sono soggetti a obblighi di trasparenza: gli utenti devono essere informati che i contenuti (ad esempio, audio e video) sono prodotti con l'ausilio dell'AI, così da poterne fruire consapevolmente.[130] In definitiva, nel contesto dell'AI per i soggetti obbligati assume rilievo innanzitutto la soglia preventiva del rischio: la normativa classifica *ex ante* i sistemi di AI in fasce di rischio, al di là del calcolo sull'impatto del singolo contesto,[131] con obblighi, vincoli o divieti differenziati. È la classificazione normativa a stabilire a priori quale livello di rigore applicativo un sistema di AI debba rispettare indipendentemente da quanto ogni singolo operatore o sviluppatore ritenga che i rischi possano sussistere.

3. Le intersezioni dell'intelligenza artificiale con la *cybersecurity* a tutela dell'ecosistema *cyber*

L'interazione tra sistemi di AI con la *cybersecurity* è un rapporto virtuoso, ampiamente descritto dalla letteratura tecnica[132,133], nonché un interesse

[128] Si veda Dipartimento per il programma di Governo, *Analisi del quadro normativo in materia di Intelligenza artificiale (D.D.L. IA e Regolamento UE su IA)*, in *programmagoverno.gov.it*.

[129] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[130] Si noti che giochi basati sull'AI o filtri antispam non comportano rischi rilevanti e non rientrano nell'ambito di applicazione del regolamento.

[131] *Ibid.*

[132] M. Ozkan-Okay-E. Akin-Ö Aslan-S. Kosunalp-T. Iliev-I. Stoyanov-I. Beloev, *A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions*, in *IEEE Access*, 12, 2024, 12229 ss.

[133] M. Pawlicki-A. Pawlicka-R. Kozik-M. Choraś, *Advanced insights through systematic analy-*

strategico emergente nell'ambito giuridico-istituzionale. Dai *report* tecnici[134] e dalla normativa di settore è possibile ricavare tre principali direttrici dall'interazione tra le discipline dell'AI e della *cybersecurity*: (*i*) l'AI per la *cybersecurity*: l'AI applicata alla *cybersecurity* agisce come leva strategica per sviluppare sistemi integrati di gestione del rischio, misure di sicurezza avanzate e strumenti ad alte prestazioni di difesa e risposta alle minacce, risultando particolarmente efficace nel contrasto di fenomeni patologici quali, ad esempio, il *cybercrime* e l'*information disorder*; (*ii*) la *cybersecurity* dell'AI: la *cybersecurity* è una *precondizione essenziale* per garantire un uso corretto, trasparente e responsabile dell'AI grazie alla sua capacità di garantire una maggiore robustezza dei sistemi e dei modelli di AI e di mitigarne le vulnerabilità; (*iii*) l'uso malevolo dell'AI, dunque utilizzata con l'intento di nuocere a persone e *asset* strategici. L'AI in termini tecnici è spesso descritta come "moltiplicatore di forze" in quanto è capace di ampliare la superfice d'attacco e amplificare l'attacco informatico, generando minacce avanzate e non convenzionali [135] [136]. L'utilizzo malevolo dell'AI è di particolare interesse per le normative che si occupano di *cybercrime, cyber threat intelligence, cyber defence*, anche nella prospettiva del diritto internazionale. Queste direttrici, pur non essendo concetti giuridici tipizzati, sono riscontrabili nei più recenti strumenti normativi europei e nazionali. Infatti, in un'ottica di protezione multilivello delle infrastrutture critiche e della gestione del rischio *cyber* nelle organizzazioni, della sicurezza dei prodotti digitali e della *supply chain*, nonché della tutela dei diritti degli utenti e delle altre persone, le intersezioni normative tra le due discipline assumono sempre più rilievo. Se da un lato sia l'AI Act sia la Legge AI[137] assegnano una dimensione chiave alla sicurezza informatica, confermando il ruolo trasversale della materia e il rapporto virtuoso e multidimensionale esistente tra le due,[138] dall'altro non mancano riferimenti all'uso dell'AI nel

sis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity, in *Neurocomputing*, 590, 2024, 127759.

[134] ENISA, *Report on Cybersecurity of AI and Standardization*, in *enisa.europa.eu*, marzo 2023; ENISA, *Securing Machine Learning Algorithms*, in *enisa.europa.eu*, dicembre 2021. NIST, *NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems*, in *nist.gov*, 4 gennaio 2024.

[135] G.F. Italiano-A. Martino-G. Piccardo, *Security and privacy in large language and foundation models: A survey on genai attacks*, in *International Conference on Distributed Computing and Intelligent Technology*, Cham, 2024, 1 ss.

[136] C. Nobles, *The weaponization of artificial intelligence in cybersecurity: A systematic review*, in *Procedia Computer Science*, 239, 2024, 547 ss.

[137] Per una panoramica della Legge AI nazionale, anche in connessione con altre normative digitali, si rimanda a G. Cassano-E. Prosperetti (a cura di), *Le regole dei dati e dell'intelligenza artificiale. Dal GDPR alla Legge 132/2025*, Santarcangelo di Romagna, 2025.

[138] ENISA, *Report on Cybersecurity of AI and Standardisation*, cit.

panorama normativo *cyber*.

3.1 L'intelligenza artificiale per la *cybersecurity*

La disciplina in materia di *cybersecurity* si caratterizza per un approccio di neutralità tecnologica, evitando di imporre l'adozione di tecnologie predeterminate e prescrivendo, piuttosto, che le misure di sicurezza implementate risultino proporzionate e adeguate ai rischi individuati. Nondimeno, le *policy* e le fonti normative di settore descrivono chiaramente il valore strategico delle *cybersecurity-enhancing technologies*, tra le quali l'AI, il cui impiego viene prospettato come elemento funzionale al rafforzamento complessivo della sicurezza dei sistemi informativi e di rete. In un'ottica di gestione del rischio integrata, i modelli di AI addestrati tramite tecniche di *machine learning*, [139] [140] [141] possono risultare particolarmente utili nella valutazione e nella classificazione del rischio all'interno delle reti per determinare la gravità di una vulnerabilità. Grazie alla capacità di analizzare grandi quantità di dati e di apprendere *pattern* complessi, queste tecnologie consentono di attribuire punteggi di rischio dinamici e contestualizzati, supportando le organizzazioni nel prioritizzare le azioni di mitigazione e migliorando la gestione complessiva del rischio *cyber*. A questo si aggiunga che, i modelli addestrati tramite tecniche di *machine learning*, consentono di identificare minacce e vulnerabilità con livelli di accuratezza e tempestività superiori rispetto agli approcci tradizionali.[142] Infine, i sistemi di AI migliorano le capacità delle organizzazioni nella predizione identificando *trend*, nonché nella risposta agli incidenti.[143]

La Strategia nazionale di *cybersicurezza* 2022-2026[144] considera lo sviluppo delle tecnologie di AI e di *machine learning* uno dei principali fattori abilitanti della crescita economica e della proiezione strategica del Paese. L'ACN, pur ricomprendendo tali tecnologie nell'ambito delle *Emerging and Disrup-*

[139] *Machine learning* (apprendimento automatico): disciplina scientifica, nell'ambito dell'intelligenza artificiale, che si pone l'obiettivo di sintetizzare modelli in grado di apprendere automaticamente da un insieme finito di dati tramite dedicati algoritmi di apprendimento.

[140] T. Mitchell, *Machine Learning*, New York, 1997.

[141] A.L. Samuel, *Some studies in machine learning using the game of checkers*, in *IBM Journal of research and development*, 3(3), 1959, 210 ss.

[142] ENISA, *Artificial intelligence and cybersecurity. ENISA Research and Innovation Brief*, in *enisa.europa.eu*, giugno 2023.

[143] A. Salvi-P. Spagnoletti-N.S Noori, *Cyber-resilience of Critical Cyber Infrastructures: integrating digital twins in the electric power ecosystem*, in *Computers & Security*, 112, 2022, 102507 ss.

[144] ACN, *Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026*, in *acn.gov.it*.

tive Technologies, evidenzia, al contempo, la necessità dualistica - difensiva e abilitante - di un impiego sinergico con la *cybersecurity*, come l'integrazione di questa tecnologia avanzata nei sistemi nazionali di monitoraggio e di analisi del rischio *cyber*, a supporto della sicurezza delle infrastrutture critiche nazionali.

Il Manuale operativo della Strategia di ACN[145] fornisce esempi concreti dell'applicazione di tali princìpi operativi: la gestione del rischio *cyber*, concepita in chiave preventiva e integrata su molteplici fonti di dati - comprese espressamente le tecnologie di AI e *machine learning* -, può supportare la *cybersecurity* nella funzione di «correlare e analizzare eventi di sicurezza di interesse».[146] L'impiego di strumenti integrati consentirebbe di creare una "super infrastruttura" ad alte prestazioni, con capacità elaborative sufficienti a «simulare, prevenire, scoprire, rispondere e predire gli impatti di attacchi *cyber* di natura sistemica».[147]

La normativa di derivazione unionale, come la Direttiva NIS2, invita i soggetti essenziali ed importanti a valutare l'impiego di tecnologie evolute, come l'AI e il *machine learning*, per il miglioramento delle proprie capacità e la sicurezza delle reti e dei sistemi informativi,[148] nel rispetto della protezione dei dati personali, dei principi di equità e trasparenza, e in combinazione con misure tecniche consolidate, quali la crittografia. Promuove, altresì, la ricerca e lo sviluppo in materia, sollecitando gli Stati membri a impiegare l'AI per potenziare le capacità di rilevamento delle minacce e prevenzione degli attacchi informatici[149]. Ciò può avvenire, ad esempio, tramite sistemi automatizzati o semiautomatizzati di rilevamento e di analisi predittiva delle minacce,[150] capaci di accrescere la rapidità della risposta e, conseguentemente, a mitigare gli effetti lesivi, siano essi di natura informatica o derivanti da altre forme di danno.

La normativa NIS2 lascia margine per un uso "mirato" dell'AI anche nello svolgimento delle competenze del CSIRT[151]. I CSIRT hanno, infatti, diverse possibilità per supportare le organizzazioni pubbliche e private,[152] e il gruppo italiano non fa eccezione, in quanto ha la facoltà di effettuare scan-

---

145 ACN, *Manuale operativo di attuazione della Misura 82. Piano di implementazione della Strategia Nazionale di Cybersicurezza 2022-2026*, su *acn.gov.it*.

146 Misura #30 in ACN, *Manuale operativo di attuazione della Misura 82*, cit.

147 Misura #32 in ACN, *Manuale operativo di attuazione della Misura 82*, cit.

148 Considerando 89, Direttiva NIS2.

149 Considerando 51, Direttiva NIS2.

150 G. Granato-A. Martino-A. Baiocchi-A. Rizzi, *Graph-based multi-label classification for WiFi network traffic analysis*. in *Applied Sciences*, 12(21), 2022, 11303 ss.

151 Art. 11, par. 3, lett. e), Direttiva NIS2.

152 I. Kamara-J. van den Boom, *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: Good practices*, 2022.

sioni proattive delle reti e dei sistemi informativi, su richiesta dei soggetti NIS italiani, per individuare vulnerabilità potenzialmente significative.[153] Si tratta di un'attività che potrebbe anche avvalersi di tecniche di AI e *machine learning*, sebbene la normativa non lo prescriva espressamente.[154]
L'Agenzia europea per la *cybersecurity* (ENISA) sintetizza le potenzialità dei sistemi basati sull'AI lungo tre direttrici: (*i*) la *detection*, ovvero l'identificazione di minacce e vulnerabilità; (*ii*) la *mitigation*, ossia la mitigazione delle minacce; (*iii*) la *prediction*, con riferimento alla capacità di anticipare rischi *cyber*[155].

3.2 La *cybersecurity* per l'intelligenza artificiale

La *cybersecurity* dell'AI è la direttrice con maggiori sviluppi paralleli sul piano tecnico e normativo. *Stricto sensu*, dal punto di vista tecnico, essa può essere intesa come l'insieme delle misure volte a garantire la protezione - in termini di riservatezza, integrità e disponibilità (c.d. triade CIA) - dei dati, dei modelli e dei processi che costituiscono un sistema di intelligenza artificiale lungo l'intero ciclo di vita. Tuttavia, il supporto della *cybersecurity* all'AI, non si esaurisce nella protezione dei sistemi AI da minacce ed attacchi, ma è la condizione preliminare per modelli e algoritmi di AI affidabili e sicuri, in quanto ne garantisce la robustezza, ne previene gli abusi e ne tutela l'affidabilità (*trustworthiness)*.
Affidabilità e robustezza sono due concetti interconnessi e la *cybersecurity* può garantirli entrambi. Un sistema di AI può dirsi robusto quando le sue prestazioni rimangono inalterate, nonostante una perturbazione da parte di un attaccante sui dati o su un modello di AI. Allo stesso tempo, un sistema di AI è affidabile quando, nel tempo, le sue prestazioni attese, corrispondono a quelle effettive.[156] Se attacchi *cyber* - come il *data poisoning*[157] e il *model poisoning*[158] - sono in grado di alterare le prestazioni del sistema, portandolo a comportamenti differenti da quelli attesi, la *cybersecurity* è in

[153] Art.15, par 3, lett. e), Decreto NIS2.

[154] I. Kamara-M. Bassini, *The cybersecurity and AI nexus in the EU digital acquis*, cit., 312 ss.

[155] ENISA, *Artificial intelligence and cybersecurity*, cit.

[156] L. Pupillo-S. Fantin-A. Ferreira-C. Polito, *Artificial intelligence and cybersecurity. Technology, Governance and Policy Challenges*, CEPS Task Force Report, maggio 2021.

[157] Protezione dei dati di addestramento da attaccanti malintenzionati che, qualora riuscissero a compromettere il *dataset*, potrebbero utilizzarlo come vettore di attacco verso il modello.

[158] Protezione del modello, una volta addestrato. I modelli sono composti da parametri che, se non opportunamente protetti, possono essere manipolati e compromessi da un attaccante con l'obiettivo di minare la sua affidabilità ed il suo potere predittivo. Si veda G.F. Italiano-A. Martino-G. Piccardo, *Security and privacy in large language and foundation models: A survey on genai attacks*, in *International Conference on Distributed Computing and Intelligent Technology*, cit.

grado di agire da scudo, ad esempio grazie all'utilizzo di misure di sicurezza quali la crittografia, capaci di rendere i dati intellegibili da chiunque (ad es. da chiunque agisca tramite un sistema informativo) e impenetrabili a tentativi di intrusione da parte di terzi non autorizzati. L'AI Act coglie questa capacità della sicurezza informatica - il testo conta oltre cinquanta riferimenti diretti – prevendendo un «obbligo di *cybersecurity*» come requisito necessario per i sistemi di AI ad alto rischio soggetti all'AI Act.[159] In particolare, l'art. 15 AI Act stabilisce che i sistemi di AI ad alto rischio debbano essere «progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e *cybersecurity* e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita». La medesima disposizione impone, inoltre, che tali sistemi siano resilienti a tentativi di terzi non autorizzati di alterarne l'uso o le prestazioni, attraverso misure quali ridondanza, piani di *fail-safe* e mitigazione dei rischi derivanti dai *feedback loops*. L'obbligo ad essere *cybersafe*, tuttavia, è circoscritto ai soli sistemi ad alto rischio.[160] D'altra parte, l'art. 12 CRA regolamenta i prodotti digitali che potrebbero incorporare sistemi di IA ad alto rischio, prevedendo una presunzione di conformità qualora ricorrano determinate condizioni.[161]
La *cybersecurity* è un principio cardine anche della Legge AI nazionale che la considera come una «precondizione essenziale» per garantire un uso corretto, trasparente e responsabile. I soggetti obbligati devono garantirla lungo l'intero ciclo di vita dei sistemi e modelli di AI per finalità generali, secondo un approccio proporzionato e basato sul rischio e l'adozione di adeguati controlli di sicurezza volti a garantire la resilienza dei sistemi e modelli di AI contro tentativi di manipolazione, alterazione delle prestazioni o modifiche delle impostazioni di sicurezza (art. 3, c. 6). La legge interviene, inoltre, sul piano istituzionale, ed in particolare sul d.l. 82/ 2021, convertito, con modificazioni, dalla l. 109/2021, ampliando le competenze di ACN, alla quale è affidato il compito di «promuovere e sviluppare ogni

[159] Cfr. art. 6 AI Act.

[160] Suscitando interrogativi circa l'assenza dell'obbligo di cybersecurity per gli altri sistemi di AI immessi sul mercato, come affermato da F. Bavetta-O. Pollicino, *Cybersecurity Requisiti tecnici e organizzativi solo per i sistemi ad alto rischio*, in *Il Sole 24 Ore*, 30 ottobre 2025.

[161] Il coordinamento tra CRA e AI Act emerge chiaramente dall'art. 12 CRA, che disciplina espressamente il rapporto tra prodotti con elementi digitali e sistemi di IA ad alto rischio. In particolare, la disposizione introduce una presunzione di conformità ai requisiti di *cybersecurity* di cui all'art. 15 AI Act per i prodotti che - rientrando nell'ambito di applicazione del CRA e qualificandosi come sistemi di IA ad alto rischio ai sensi dell'art. 6 AI Act - soddisfino i requisiti essenziali di *cybersecurity* previsti dal CRA. Tale presunzione opera al ricorrere di tre condizioni cumulative: (*i*) il rispetto dei requisiti essenziali di *cybersecurity* di cui all'allegato I, parte I, CRA; (*ii*) la conformità dei processi predisposti dal fabbricante ai requisiti di cui all'allegato I, parte II; (*iii*) la dimostrazione del livello di protezione richiesto dall'art. 15 AI Act mediante la dichiarazione di conformità rilasciata ai sensi del CRA.

iniziativa [...] volta a valorizzare l'intelligenza artificiale come risorsa per il rafforzamento della *cybersicurezza* nazionale» (art. 18). In questa dimensione, la *cybersecurity* svolge una funzione di supporto all'AI assumendo da un lato il suo tradizionale ruolo di *standard* tecnico, dall'altro evolvendosi per rispondere a sfide avanzate e contemporanee.
Le Linee guida per uno sviluppo sicuro dell'AI (2023),[162] promosse dal National Cyber Security Centre del Regno Unito, e sottoscritte da 23 Agenzie di diciotto Paesi, compresa l'ACN, evidenziano come i sistemi di AI - intese da questo strumento come le sole applicazioni di *machine learning* - siano soggetti a vulnerabilità nuove e peculiari, che si aggiungono a quelle tradizionali del dominio *cyber*, ad esempio l'*Adversarial Machine Learning* (AML): l'insieme delle tecniche che sfruttano le debolezze intrinseche dei modelli di apprendimento automatico - che possono riguardare sia componenti *hardware* e *software*, sia i flussi di lavoro e le catene di approvvigionamento - con l'obiettivo di indurre nei sistemi comportamenti non intenzionali o dannosi. I sistemi di AI sono, in fondo, sistemi informatici per questo ereditano tutti i rischi della sicurezza informatica connessi alle reti e ai sistemi informativi. Come la *cybersecurity*, anche l'AI sta evolvendo nel tempo ad una velocità molto rapida, tanto che l'attuale ecosistema AI è composto da una varietà di modelli e tecniche, con differenti livelli di maturità tecnologica: non tutti i modelli immessi sul mercato sono allo stesso stadio di sviluppo e non vengono utilizzati per gli stessi scopi.

4. Conclusioni

Le normative in materia di *cybersecurity* e intelligenza artificiale traducono il *risk management* in obblighi giuridici, orientando l'azione di soggetti pubblici e privati verso logiche proattive, proporzionate e anticipatorie del rischio.[163] Tuttavia, questo approccio si declina diversamente. La normativa *cyber* si fonda su un modello di gestione del rischio,[164] che valorizza la capacità del soggetto obbligato a valutarlo e gestirlo, nonché a identificare le vulnerabilità. L'AI Act opera, invece, una qualificazione normativa del rischio mediante una classificazione *ex ante* delle applicazioni di intelligenza artificiale in base al loro impatto sulla società, mantenendo una prospettiva esplicitamente antropocentrica a tutela dei diritti fondamentali e dell'autonomia umana.

---

[162] Si veda *Guidelines for secure AI system development*, in *acn.gov.it*.

[163] M.A. Rizzi-F. Serini, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, cit.

[164] Sia questo basato sull' approccio tecnico-organizzativo e flessibile (NIS2, DORA) oppure integrato *by security e by design* nei prodotti digitali (CRA e, con le dovute specificità, anche il PSNC, ad esempio in relazione ai meccanismi di *procurement*).

In entrambe le discipline, *cyber* e AI, la sicurezza non può assurgere all'assenza assoluta di rischio,[165] bensì alla sua gestione informata, continua e proporzionata.[166] Il fine ultimo è prevenire eventi avversi, proteggere persone, diritti, interessi giuridici, organizzazioni e *asset*.[167] [168]

In questa prospettiva, ci si può interrogare, se dall'interpretazione della *cybersecurity law* - alla luce dell'interezza della normativa, tanto di derivazione unionale quanto domestica - non si possa desumere una lettura ulteriore superando il mero lessico tecnico adottato in sede di formazione dell'atto, [169] [170] e ricondur-

[165] Sarebbe, d'altronde, un obiettivo irrealistico in un ecosistema digitale intrinsecamente esposto a diverse complessità.

[166] Permettendo al diritto di distinguere tra rischio tecnico (es. un guasto o malfunzionamento), oggettivamente misurabile, e il rischio percepito che è legato a valutazioni soggettive e sensibili al contesto. V. F. Nocifora, *Sociologia della sicurezza, rischio e legalità democratica*, in AA.VV. (a cura di), *Sicurezza e democrazia*, Napoli, 2010, 101 ss.

[167] P. Cichonski-T. Millar-T. Grance-K. Scarfone, *NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, agosto 2012.

[168] M. Ebers, *Truly risk-based regulation of artificial intelligence how to implement the EU's AI Act*, cit.

[169] Nell'analisi degli atti dell'Unione europea e della normativa derivata, occorre tener conto delle caratteristiche del processo legislativo e, in particolare, delle dinamiche negoziali che si sviluppano in seno al Consiglio dell'UE, nonché della composizione dei gruppi di lavoro, che incide sul risultato normativo. La rilevante prevalenza di esperti tecnici provenienti dai diversi Stati membri - quali ingegneri e specialisti della sicurezza informatica nel caso della *cybersecurity* - contribuisce alla produzione di testi nei quali il lessico operativo e il significato tecnico assumono un ruolo prevalente rispetto a quello propriamente giuridico. Ciò risulta ancor più evidente nelle fonti normative *cyber*, che tendono a mantenere una forte impronta tecnico-applicativa, sia sul piano concettuale sia su quello linguistico. Se, da un lato, tale impostazione favorisce un elevato grado di precisione operativa - come nel caso della nozione di "vulnerabilità" offerta dal CRA, dalla NIS2 e dal DORA - dall'altro richiede un'attività interpretativa volta a ricondurre tali concetti all'interno di un quadro giuridico più ampio, capace di coglierne le implicazioni nell'interezza del *framework*, e ricondurli a categorie giuridiche idonee a carpirne la rilevanza nel contesto della tutela dei diritti, della responsabilità e della regolazione del rischio nella società digitale. A titolo meramente esemplificativo e non esaustivo, si considerino il gruppo di lavoro orizzontale "Questioni riguardanti il ciberspazio" (*Horizontal Working Party on Cyber Issues – HWPCI),* istituito nel 2016, che coordina i lavori del Consiglio dell'Unione europea in materia di politiche e legislazione sulla *cybersecurity* e si riunisce con elevata frequenza - indicativamente più volte al mese -, e il gruppo orizzontale "Rafforzare la resilienza e contrastare le minacce ibride" (*Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats HWP ERCHT*) che si occupa di contrastare le minacce ibride, rafforzare la resilienza degli Stati e delle società a tali minacce e migliorare la comunicazione strategica e combattere la disinformazione. In tale contesto, ACN assicura un supporto soprattutto tecnico e strategico al Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI) e, in particolare, alla Rappresentanza Permanente d'Italia presso l'Unione europea (RappUE), contribuendo alla formazione della posizione italiana nei negoziati parte della procedura normativa, nonché contribuisce anche mediante «l'analisi di strumenti e opzioni operative». Si veda ACN, *Gruppo di Lavoro orizzontale sulle questioni cyber (HWPCI)* e *Hybrid e altri gruppi di lavoro UE*, in *acn.gov.it*.

[170] A tali criticità si aggiungono ulteriori fattori che contribuiscono ad accrescere la com-

la a categorie giuridiche idonee a coglierne la rilevanza nel contesto della tutela dei diritti, della responsabilità e della regolazione del rischio nella società digitale. Non si tratta di cristallizzare il lessico in costrutti rigidi, poco compatibili con la dinamicità e la complessità della materia, bensì di renderlo più adattivo e sensibile, tramite una lettura inferenziale, alle esigenze giuridiche, sociali e al contesto storico di riferimento, caratterizzato da una continua evoluzione tecnologica ed un'elevata produzione normativa sul digitale. In questo modo, sarebbe il diritto innanzitutto, e non la tecnica, a definire meglio gli spazi e i confini della materia stessa. A questa premessa segue la domanda se sia possibile ricavare una nozione di *cyber vulnerability*, che assume un significato peculiare per le normative considerate e che trascende la mera definizione normativo-nozionistica di "vulnerabilità" contenuta nella *cybersecurity law*[171].

La *cyber vulnerability* deve essere intesa come una condizione di potenziale esposizione che precede e struttura il rischio e ne consente la qualificazione. La consapevolezza delle vulnerabilità consente al soggetto obbligato, infatti, di individuare e prioritizzare gli *asset*, le funzioni e i diritti suscettibili di compromissione, permettendo una prima classificazione rilevante ai fini della loro tutela. In altre parole, assume una funzione ordinante in un ambito caratterizzato da multifattorialità ed elevata complessità tecnica.

In tal senso, la *cyber vulnerability* costituisce il presupposto logico-giuridico, non statico, dell'approccio *risk-based*, orientando le attività di *compliance* dei soggetti obbligati. Essa si manifesta come una condizione diffusa e sistemica, che attraversa l'intero ecosistema digitale, coinvolgendo le reti e i sistemi informativi. La compromissione dell'*availability* e dell'*integrity* delle infrastrutture critiche, così come delle condizioni di sicurezza dei prodotti digitali, può peraltro avere conseguenze sull'accesso a servizi essenziali.

Ne deriva che la *cybersecurity law* va oltre al mero obiettivo tecnico assumendo un ruolo funzionale, trasversale e complementare rispetto ad altri ambiti normativi – dalla protezione dei dati personali, alla regolazione dell'intelligenza artificiale – configurandosi, così, come uno *standard* da raggiungere per la tutela dei diritti dell'individuo nella società digitale.

Il tecnocentrismo della normativa *cyber* non è, dunque, fine a sé stesso: l'essere umano resta il soggetto esposto ai rischi derivanti dall'uso della tecnologia. Le minacce informatiche colpiscono primariamente componenti tecnologiche, ma incidono su aspetti fondamentali dell'esistenza dell'individuo (come

plessità, tra cui le traduzioni ufficiali degli atti normativi, che in alcuni casi divergono dal lessico adottato a livello domestico. Emblematico è il caso della pluralità terminologica utilizzata per indicare la cybersecurity - *cybersecurity*, *cibersecurity*, *sicurezza informatica*, *cybersicurezza*, *cibernetica*- che riflette non solo differenti scelte linguistiche, ma anche disallineamenti concettuali e interpretativi.

[171] Nozione di derivazione tecnica che rimanda alla debolezza di sistemi, prodotti o servizi ICT. Cfr. *supra*.

la sua vita privata, la sua attività lavorativa e imprenditoriale, l'accesso ai servizi pubblici digitali, la gestione della propria identità digitale, la sicurezza dei dati bancari e dei sistemi di pagamento, la continuità dei servizi essenziali, la partecipazione ai processi democratici, l'accesso all'istruzione, nonché la tutela della reputazione personale e professionale nell'ambiente informativo digitale). In tale prospettiva l'interesse protetto rimane eminentemente umano e sociale, poiché gli incidenti *cyber* possono tradursi in limitazioni concrete dell'autonomia individuale. La *cyber vulnerability*, in questo senso, non riguarda soltanto le debolezze tecniche e lo *human factor* (possibilità di commettere errori), ma comprende in modo sostanziale anche la vulnerabilità dell'essere umano, intesa come condizione soggettiva dell'esistenza, di esposizione al rischio. Nel discorso giuridico, invero, la vulnerabilità si configura come un concetto polisemico che dipende dal contesto. Più che indicare una condizione univoca e definita, essa assume una connotazione flessibile in quanto è utilizzata trasversalmente, in diversi ambiti del diritto, per evidenziare asimmetrie strutturali tra soggetti deboli e forti, richiamando una responsabilità giuridica di protezione.[172]

Nella *cybersecurity law*, tuttavia, la *cyber vulnerability* assume una dimensione peculiare, in quanto oltre che soggettiva è anche universale: tutti i soggetti risultano potenzialmente esposti innanzi al digitale e dunque vulnerabili. Il diritto, in questo caso, non è chiamato a proteggere solo determinate categorie specifiche di soggetti (es. i minori, i disabili)[173], ma a garantire condizioni di sicurezza per l'intera società.[174] In questa prospettiva, la tutela delle persone e della società dal rischio tecnologico – incluso quello *cyber* – costituisce l'orizzonte verso cui i sistemi di *risk governance*, delineati dalla normativa, devono convergere.

---

[172] F. Panuccio Dattola-T. Amodeo, *Vulnerabilità e diritti umani: strumenti e percorsi di tutela*, Milano, 2022.

[173] Cfr. l'art. 5 AI Act, il quale prevede il divieto di «immissione sul mercato, la messa in servizio o l'uso di un sistema di AI che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone», in quanto queste tecniche di manipolazione possono essere utilizzate per persuadere l'utilizzatore ad adottare comportamenti indesiderati o per indurre le persone a prendere decisioni con l'inganno, sovvertendone e pregiudicandone l'autonomia, il processo decisionale e la libera scelta. Il rischio individuato dalla normativa è quello di «causare danni significativi sulla salute fisica, psicologica o sugli interessi finanziari», ancor più se si tratta di persone ritenute particolarmente fragili, che il regolamento definisce indirettamente, come persone o gruppi di persone che «versano in condizione di vulnerabilità dovute all'età, a disabilità… o a una specifica situazione sociale o economica che potrebbe renderle più vulnerabili allo sfruttamento, come le persone che vivono in condizioni di povertà estrema e le minoranze etniche o religiose» (considerando 29).

[174] La consapevolezza di questa vulnerabilità universale «deve fondare l'attività legislativa e le istituzioni sociali, e cioè l'impegno della legalità, dell'organizzazione della società e delle sue leggi nel proteggere la società». T. Amodeo, *Tutela e protezione di soggetti vulnerabili. Un nuovo progetto di vita: il co-housing*, in *Judicium.it*, febbraio 2021.

Abstract

Il presente contributo ricostruisce e analizza la *governance* della *cybersecurity* nel quadro normativo europeo e nazionale, mettendo in luce le complementarità tra modelli integrati orientati alla sicurezza delle reti, dei sistemi e dei prodotti ICT. In tale contesto, si esamina la relazione virtuosa tra *cybersecurity* e intelligenza artificiale, sia nella prospettiva dell'AI per la *cybersecurity* quale strumento di prevenzione, rilevazione e risposta alle minacce, efficace soprattutto nel contrasto di fenomeni patologici, sia della *cybersecurity* per l'AI quale precondizione necessaria per garantire affidabilità, sicurezza e robustezza dei sistemi, mitigandone le vulnerabilità. Il contributo, infine, introduce il concetto di *cyber vulnerability* quale condizione di esposizione che precede e struttura il rischio. In tale prospettiva, la *cybersecurity law* emerge come strumento trasversale di tutela nella società digitale.

This paper examines and analyzes cybersecurity governance within the European and national regulatory frameworks, highlighting the complementary nature of integrated models focused on the security of networks, systems, and ICT products. In this context, it examines the virtuous relationship between cybersecurity and artificial intelligence, both from the perspective of AI for cybersecurity as a tool for prevention, detection, and response to threats - effective above all in combating malicious phenomena – as well as from the perspective of cybersecurity for AI as a necessary precondition for ensuring the reliability, security, and robustness of systems, thereby mitigating their vulnerabilities. Finally, this paper introduces the concept of cyber vulnerability as a condition of exposure that precedes and shapes risk. From this perspective, cybersecurity law emerges as a cross-cutting tool for protection in the digital society.

Keywords

cyber vulnerability - cybersecurity law - artificial intelligence regulation - risk-based approach - standard

Ricerca medica, fascicolo sanitario elettronico e IA: la direzione della legislazione italiana*

Vittorio Bachelet

Sommario

1. Premesse. – 2. Ricerca scientifica sanitaria e consenso degli interessati: inquadramento sistematico. – 3. *Segue*. Ricerca sanitaria senza consenso: l'evoluzione dell'art. 110 cod. privacy. – 4. Il declino del consenso nel c.d. fascicolo sanitario elettronico 2.0. 5. Il contributo della legge in materia di intelligenza artificiale. – 6. Riflessioni conclusive.

1. Premesse

Il tema della ricerca scientifica basata sui dati sanitari[1] fa capo, nell'ordi-

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

Il contributo, qui proposto con alcuni aggiornamenti e minime integrazioni, è stato originariamente pubblicato nel volume *Autodeterminazione, cura e ricerca nell'era digitale. Interessi antagonisti e modelli di bilanciamento* (a cura di C. De Menech e M. Foglia, Torino, 2026, 311 ss.), che raccoglie gli atti del convegno conclusivo del PRIN 2022 PNRR "*Medical Informed Consent, Artificial Intelligence and Law*", condotto dalle Università di Pavia e di Bergamo.

[1] In materia, senza pretesa di completezza, cfr. M. Faccioli, *Le condizioni di liceità del trattamento di dati sanitari per finalità di ricerca medica*, in *Pers. merc.,* 2025, 1115 ss.; G. Finocchiaro-L. Greco, *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, in *Dir. merc. tecn.*, 22 febbraio 2024, 1 ss.; P. Aurucci, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Napoli, 2022, *passim*; A. Bernes, *Dati e ricerca genetica. Dalla tutela individuale alla gestione procedurale*, in *Riv. biodir.*, 2022, 67 ss.

Più in generale, P. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, Trento, 2021, *passim*; A. Bernes, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove leggi civ. comm.*, 2020, 175 ss.; G.M. Uda, *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 557 ss.; C. Wiese Svanberg, *Article 89. Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*, in C. Kuner-L.A. Bygrave-C. Docksey (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020, 1240 ss.;

namento italiano, essenzialmente a tre fonti normative: la disciplina della "Ricerca medica, biomedica ed epidemiologica" di cui all'art. 110 cod. privacy, come da ultimo modificato dal d.l. 2 marzo 2024, n. 19, convertito con modificazioni dalla legge 29 aprile 2024, n. 56, il quale individua le condizioni alle quali si può svolgere la ricerca medica senza il consenso degli interessati; la disciplina del "Fascicolo sanitario elettronico 2.0", prevista dal decreto 7 settembre 2023 del Ministero della salute, adottato in attuazione del d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221, che ha istituito il fascicolo sanitario elettronico attribuendogli anche finalità di studio e di ricerca scientifica; e la recente disciplina di cui alla legge 23 settembre 2025, n. 132, contenente "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", che all'art. 8 si occupa di "Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario".

Il nesso tra i profili delineati emerge osservando che il c.d. fascicolo sanitario elettronico 2.0 intende costituire un rilevante bacino di dati sanitari[2] volto ad alimentare non solo la ricerca scientifica[3], ma altresì a supportare la sperimentazione e l'innovazione tecnologica mediante sistemi di intelligenza artificiale destinati alla prevenzione, alla diagnosi e alla cura, nonché allo sviluppo di terapie e dispositivi medici nel settore sanitario: ambiti che la recente normativa nazionale, in linea con quella europea, intende valorizzare e tutelare.

Prima di illustrare analiticamente tali ambiti di disciplina, va sottolineato come la loro evoluzione normativa rifletta, nel complesso, il passaggio da una prospettiva privatistica, incentrata sul consenso individuale – e, dunque, sull'autodeterminazione "informativa" dell'interessato[4] – a una concezione pubblicistica, che considera i dati sanitari quali risorse per la

A. Macinati, *Art. 89. Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in L. Bolognini-E. Pelino (a cura di), *Codice della disciplina privacy*, Milano, 2024, 429 ss.; R. Ducato, *Art. 89. Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021, 957 ss.

[2] A proposito di tale definizione, vedi A. Iuliani, *Gli incerti confini della nozione di "dati relativi alla salute"*, in *Autodeterminazione, cura e ricerca*, cit., 237 ss.; A. Bernes, *La nozione di «dati relativi alla salute» al vaglio della Corte di Giustizia: quali conseguenze per il commercio elettronico e la concorrenza?*, in *Nuova giur. civ. comm.,* 2025, 588 ss., e già P. Guarda, *I dati sanitari*, in *I dati personali nel diritto europeo*, cit., spec. 593 ss., e L.A. Bygrave-L. Tosoni, *Article 4(15) Data concerning health*, in *The EU General Data Protection Regulation (GDPR)*, cit., 217 ss.

[3] Su tale nozione, da intendersi in senso ampio ai sensi del considerando 159 del GDPR, si rinvia al contributo di C. Irti, *Il perimetro della nozione di "ricerca scientifica" nell'era digitale: profili problematici*, in *Autodeterminazione*, cit., 253 ss.

[4] Con riguardo all'ambito sanitario, v. da ultimo S. Corso, *Autodeterminazione e dati sanitari*, Torino, 2025, spec. 123 ss., e già C. De Menech, *Intelligenza artificiale e autodeterminazione in*

collettività, accessibili anche senza il consenso degli interessati ove trattati, tra l'altro, a fini di ricerca scientifica.
Questa evoluzione rispecchia una tendenza immanente nel regolamento (UE) 2016/679 sulla protezione dei dati personali, noto come GDPR[5] e rivolto, nel complesso, a favorire il trattamento dei dati sanitari per finalità di ricerca scientifica (secondo e terzo paragrafo), e in generale nel diritto dell'Unione, che ha dato impulso al potenziamento del Fascicolo sanitario elettronico attraverso il Piano nazionale di ripresa e resilienza nel quadro del regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari[6] (quarto paragrafo), e ha ispirato la legge italiana sull'intelligenza artificiale attraverso il regolamento (UE) 2024/1689, noto come "AI Act"[7] (quinto paragrafo).

2. Ricerca scientifica sanitaria e consenso degli interessati: inquadramento sistematico

Il punto di partenza dell'itinerario delineato è costituito dalla recente modifica dell'art. 110 cod. privacy, promossa da diverse società scientifiche italiane[8] e finalizzata ad agevolare le attività di ricerca medica, biomedica ed epidemiologica[9] che implicano il trattamento di dati relativi alla salute.

materia sanitaria, in *Riv. biodir.*, 2022, 181 ss.
Più in generale, in tema di autodeterminazione informativa (*informationelle Selbstbestimmung*) quale diritto a conoscere e a stabilire la sorte dei propri dati (art. 8 della Carta dei diritti fondamentali), distinto dal diritto alla riservatezza o *privacy* (art. 7 della Carta), cfr. O. Lynksey, *The Foundations of EU Data Protection Law*, Oxford, 2015, 89 ss.; nella dottrina italiana, S. Rodotà, *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2019, 9 ss.; G. Visintini, *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Dir. inf.*, 2019, 1 ss.; G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 2 ss.; V. Ricciuto, *L'equivoco della privacy. Persona* vs. *dato personale*, Napoli, 113 ss.; S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, *passim*.

[5] Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati).

[6] Regolamento (UE) 2025/327 dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari (c.d. *European Health Data Space* - EHDS).

[7] Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale).

[8] Raccolte nella Società Italiana di leadership e Management in Medicina: cfr. la *Proposta di revisione della normativa privacy in sanità*, Roma 20 febbraio 2024, consultabile all'indirizzo *medici-manager.it*, su cui v. M. Altini, *Ridefinire le norme Privacy*, in *Panorama sanità*, 4, 2024, 36 s.

[9] Su tali definizioni, si vedano L. Bolognini-E. Pelino, *Art. 110. Ricerca medica, biomedica ed*

L'evoluzione della norma si inserisce nel quadro dell'art. 9, par. 2, GDPR, che individua tassativamente le basi legali del trattamento di dati personali «particolari», come quelli sanitari[10], meritevoli di una specifica protezione in quanto particolarmente sensibili per la tutela dei diritti e delle libertà fondamentali (considerando 51 del GDPR).

Com'è noto, nell'architettura della disciplina europea, anche precedente al GDPR[11], il consenso dell'interessato non gode di una posizione di preminenza né fra le basi legali del trattamento dei dati appartenenti a categorie particolari, come quelli in esame, né di quelli c.d. comuni ai sensi dell'art. 6[12]. Esso risulta, peraltro, una base problematica per giustificare il trattamento dei dati sanitari a fini di ricerca scientifica, non solo a fronte della sua sempre libera revocabilità *ex* art. 7, par. 3, GDPR[13], ma soprattutto, come si vedrà, delle difficoltà di soddisfare i requisiti di specificità e di libertà stabiliti dall'art. 4, n. 11, affinché il consenso sia valido.

In primo luogo, il requisito di libertà del consenso, quale espressione effettiva dell'autodeterminazione informativa dell'interessato, impone un controllo più rigoroso di quello previsto in ambito negoziale, non limitato a riscontrare l'assenza dei tradizionali vizi del volere, ma esteso a ogni possibile forma di condizionamento[14]. Ciò si verifica tipicamente quando sussiste un evidente squilibrio tra l'interessato e il titolare del trattamento (considerando 43 del GDPR): una situazione spesso ricorrente nelle

epidemiologica, in *Codice della disciplina privacy*, cit., 568 s.

[10] Cfr. A. Thiene, *La regola e l'eccezione. Il ruolo del consenso in relazione al trattamento dei dati sanitari alla luce dell'art. 9 GDPR*, in Ead.-S. Corso (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, 2023, 9 ss., Id., *Il trattamento dei dati personali in ambito sanitario*, in *Riv. it. inf. dir.*, 2, 2025, 4 ss., e P. Guarda, *I dati sanitari*, cit., 598 ss.; più in generale L. Georgieve-C. Kuner, *Article 9. Processing of special categories of personal data*, in *The EU General Data Protection Regulation (GDPR)*, cit., 365 ss.

[11] Cfr. gli artt. 7 e 8 della direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; conf. Gruppo di lavoro Articolo 29 (WP29), Parere 6/2014, *Sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'art. 7 della direttiva 95/46/EC*, 9 aprile 2014, 12, e, in dottrina, F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, 384 s.

[12] V., tra gli altri, W. Kotschy, *Article 6. Lawfulness of processing*, in *The EU General Data Protection Regulation (GDPR)*, cit., spec. 329.

[13] Se esercitata, la revoca rende il trattamento illecito *ex nunc*, senza deroghe favorevoli per finalità di ricerca, obbligando il titolare del trattamento a interromperlo e, su richiesta dell'interessato, anche a cancellare i dati senza in ingiustificato ritardo ai sensi dell'art. 17, par. 1, lett. *b*), GDPR: cfr. F. Caggia, *Art. 7. Condizioni per il consenso*, in *Codice della privacy e data protection*, cit., spec. 223 ss.

[14] Sul punto, per tutti, S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, 517 ss.

sperimentazioni cliniche, nell'ambito delle quali i partecipanti potrebbero, ad esempio, versare in condizioni precarie di salute, appartenere a gruppi economicamente o socialmente svantaggiati, o trovarsi in situazioni di dipendenza istituzionale o gerarchica rispetto ai promotori della sperimentazione[15].

In secondo luogo, per esprimere autenticamente l'autodeterminazione dell'interessato, il consenso deve rispettare anche il requisito di specificità e riguardare il trattamento dei dati per una o più finalità specifiche[16]. Muovendo dalla constatazione che in molti casi è difficile precisare le finalità del trattamento a scopo di ricerca scientifica al momento della raccolta dei dati, il considerando 33 del GDPR ammette un consenso esteso in termini più ampi a «taluni settori» di ricerca, nel rispetto delle relative norme deontologiche (c.d. *broad consent*)[17]. Tale deroga, ritenuta eccezionale dal Comitato europeo di protezione dei dati e subordinata al fatto che il consenso generale sia seguito da un consenso specifico per ogni fase successiva della ricerca[18], non riesce tuttavia a risolvere le criticità della base consensuale dei trattamenti a fini scientifici, anche a fronte della sua eventuale revocabilità.

Pur così modulato, il requisito di specificità del consenso – agevole da soddisfare nelle classiche sperimentazioni cliniche, le cui finalità sono delineate sin dal momento dell'arruolamento dei partecipanti – resta difficile da rispettare negli studi più recenti di tipo "osservazionale retrospettivo"[19],

---

[15] Arg. *ex* considerando 31 del regolamento (UE) 2014/536 del 16 aprile 2014 sulla sperimentazione clinica di medicinali per uso umano (cui il GDPR rinvia al considerando 161), sebbene riferito al consenso alla partecipazione alla sperimentazione clinica, non al consenso quale base giuridica del trattamento: in tal senso, v. già Comitato europeo per la protezione dei dati personali (EDPB), *Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati*, 23 gennaio 2019, 7.

[16] A norma degli artt. 4, n. 11; 6, par. 1, lett. *a*); 9, par. 2, lett. *a*), GDPR: cfr. EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 4 maggio 2020, 15 s., e, in dottrina, S. Thobani *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 71 ss.

[17] Cfr. D. Sborlini, *Il "broad consent" come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in *Contr. impr.*, 2024, 223 ss., e, per ulteriori riferimenti e approfondimenti, M. Faccioli, *Le condizioni di liceità*, cit., 1124 ss.

[18] Cfr. EDPB, *Linee guida 5/2020 sul consenso*, cit., 33 ss., e la nt. precedente. V. ora, in senso parzialmente confermativo, ma con un'evoluzione verso modelli più flessibili di consenso – non necessariamente articolati in successive manifestazioni specifiche, e con un maggiore rilievo delle garanzie compensative – EDPB, *Guidelines 1/2026 on Processing of Personal Data for Scientific Research Purposes*, 15 aprile 2026, 22 ss.

[19] V., per tutti, P. Aurucci, *Il trattamento*, cit., 96 ss., spec. 101 ss., a cui si rinvia anche per la distinzione tra studi sperimentali e osservazionali (5 ss.).

che potrebbero analizzare *Big Data* sanitari mediante algoritmi di IA per scopi individuabili compiutamente solo a posteriori[20]. Il trattamento di tali dati, di norma raccolti per scopi diversi, di cura o per altri progetti di ricerca, configura un uso ulteriore, che il GDPR disciplina in senso favorevole alla ricerca scientifica[21]: il principio di limitazione della finalità *ex* art. 5, par. 1, lett. *b*), nell'esigere che i dati siano raccolti per scopi determinati, espliciti e legittimi – e in seguito trattati in modo non incompatibile con essi[22] – considera, infatti, non incompatibili i trattamenti ulteriori a fini di ricerca scientifica, purché siano rispettate le garanzie di cui all'art. 89, par. 1[23].
L'agevolazione per la ricerca risulta, tuttavia, attenuata dall'orientamento tradizionalmente restrittivo del Garante europeo della protezione dei dati, secondo cui non opererebbe una presunzione di non incompatibilità con le finalità iniziali del trattamento, quanto una mera attenuazione del rigore del giudizio di compatibilità, che dovrebbe comunque essere svolto caso per caso[24]. Accertata tale compatibilità, il titolare del trattamento non sarebbe peraltro dispensato dall'individuare un'autonoma base giudica per

[20] V., in generale, C. De Menech, *Intelligenza artificiale*, cit., 198, e V. Fusco, *Luci e ombre del GDPR nell'era dell'intelligenza artificiale*, in *Oss. dir. civ. comm*., 2025, 93 s., ove ulteriori riferimenti. L'espressione "*Big Data*" non evoca, del resto, soltanto grandi masse di dati, bensì una prospettiva di analisi che sostituisce il tradizionale approccio deterministico, volto a confermare ipotesi formulate *ex ante* circa possibili relazioni causa-effetto, con un approccio "*data-driven*" probabilistico, teso a ricavare *ex post* correlazioni "spontanee" (e imprevedibili) dall'esame di enormi volumi di dati eterogenei: cfr. V. Mayer-Schonberger-K. Cukier, *Big Data*, Milano, 2013, spec. 76 ss. c

[21] Sulla distinzione fra trattamento ulteriore e uso secondario, cfr. S. Thobani, *L'uso secondario dei dati sanitari*, in *Autodeterminazione*, cit., spec. 222 ss., alla quale si rinvia anche per l'analisi della norma nazionale relativa al trattamento ulteriore a fini di ricerca scientifica (art. 110-*bis* cod. privacy), con particolare riguardo ai controversi rapporti con l'art. 110: ivi, nt. 12.

[22] C. de Terwangne, *Article 5. Principles relating to processing of personal data*, in *The EU General Data Protection Regulation (GDPR)*, cit., spec. 315 ss. Sulla tensione tra principio di finalità e *Big Data*, v. ad es. G. Malgieri, *Art. 5. Principi applicabili al trattamento dei dati personali*, in R. D'Orazio-G. Finocchiaro-O. Pollicino-G. Resta (a cura di), *Codice della privacy e data protection*, cit., 185 ss.

[23] Che si traducono nella predisposizione di misure tecniche e organizzative adeguate a tutelare l'interessato – quali la pseudonimizzazione e l'anonimizzazione (cfr., *infra*, il § 5), volte in particolare a garantire il rispetto del principio di minimizzazione dei dati previsto dall'art. 5, par. 1, lett. *c*), GDPR – tra le quali possono ricomprendersi anche le garanzie individuate dal Garante privacy (cfr. la successiva nt. 39): si vedano, al riguardo, C. Wiese Svanberg, *Article 89*, cit., 1240 ss.; A. Macinati, *Art. 89*, cit., 429 ss.; e R. Ducato, *Art. 89*, cit., 957 ss.

[24] Alla luce dei criteri di cui all'art. 6, par. 4, GDPR: cfr. EDPS, *A Preliminary Opinion on Data Protection and Scientific Research*, 6 gennaio 2020, 23. V. tuttavia, in termini più favorevoli alla ricerca scientifica – con una più ampia valorizzazione della presunzione di compatibilità del trattamento ulteriore per finalità di ricerca – EDPB, *Guidelines 1/2026*, cit., 16 ss.

il trattamento ulteriore di dati particolari, come quelli sanitari, stando al rigoroso indirizzo del Comitato europeo di protezione dei dati personali, che circoscrive ai soli dati "comuni" il considerando 50 del GDPR, il quale esclude la necessità di una base giuridica separata per i trattamenti ulteriori[25].

Per tali ragioni, a cui si aggiunge la difficoltà pratica di contattare tutti i soggetti coinvolti in uno studio retrospettivo, che nel frattempo potrebbero essere deceduti o divenuti irraggiungibili[26], il consenso degli interessati costituisce un presupposto generalmente inadatto a giustificare il trattamento di dati sanitari a fini di ricerca scientifica[27].

3. *Segue*. Ricerca sanitaria senza consenso: l'evoluzione dell'art. 110 cod. privacy

Alla luce di quanto osservato, il consenso degli interessati costituisce una base giuridica di portata tendenzialmente limitata per il trattamento dei dati a fini di ricerca scientifica, in un quadro frammentato e non privo di incertezze applicative.

In tale contesto, il legislatore riserva ai trattamenti a scopo di ricerca scientifica[28] una base legale dedicata fra quelle relative ai dati appartenenti a categorie particolari, ai sensi dell'art. 9, par. 2, lett. *j*), del GDPR[29]. Essa trova applicazione quando il trattamento risulti «necessario» per la ricerca sulla base del diritto dell'Unione o nazionale, che sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate a tutelare l'interessato – in particolare quelle tecniche e organizzative previste dall'art. 89, par. 1, a cui la disposizione rinvia[30].

---

[25] EDPB, *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, 7 febbraio 2021, 7.

[26] Cfr. D. Fulco, *Modifica dell'art. 110 Codice privacy e il provvedimento del Garante del 9 maggio 2024*, in *Ius. amm.*, 4 giugno 2024. Si tenga presente che il GDPR non si applica al trattamento dei dati personali delle persone decedute; tuttavia, tale materia può essere regolata dagli Stati membri ai sensi del considerando 27.

[27] In tal senso, *ex multis*, A. Bernes, *La protezione dei dati personali nell'attività di ricerca scientifica*, cit., 192; L. Bolognini-E. Pelino, *Art. 110*, cit., 566; M. Faccioli, *Le condizioni di liceità*, cit., spec. 1122, 1129, 1132, 1136 e 1147; nonché EDPB, *Parere 3/2019 relativo alle domande e risposte*, cit., 7.

[28] O storica, a fini statistici o di archiviazione nel pubblico interesse.

[29] V., *ex multis*, G.M. Uda, *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, in *I dati personali nel diritto europeo*, cit., spec. 569 ss.; L. Georgieve-C. Kuner, *Article 9. Processing of special categories of personal data*, cit., 380 s.

[30] V. la precedente nota 23.

Altre basi giuridiche idonee a legittimare il trattamento di dati sanitari a fini di ricerca scientifica riguardano anzitutto, come si vedrà, i trattamenti necessari per motivi di interesse pubblico rilevante (lett. *g*), nonché i trattamenti necessari per motivi di interesse pubblico nel settore della sanità pubblica (lett. *i*)[31].

Come evidenziato, la portata di tali basi giuridiche è, tuttavia, ridotta dal fatto che esse coprono esclusivamente i trattamenti necessari agli scopi o per le ragioni indicate, non quelli meramente "utili"[32]. In particolare, quanto alla ricerca sanitaria, il requisito della necessità va riferito non tanto all'individuazione dei dati da trattare, la cui rilevanza è spesso conoscibile solo *ex post*, quanto alle operazioni effettuate sui dati, che risultano necessarie quando la ricerca riflette esattamente l'ipotesi oggetto di verifica – sicché potrebbero rivelarsi non necessari, ad esempio, i trattamenti svolti nell'ambito di ricerche sperimentali, destinati alla somministrazione di farmaci c.d. compassionevoli volti ad alleviare le sofferenze di pazienti in condizioni critiche[33].

Ogni qualvolta il trattamento non risulti necessario ai fini indicati, il consenso degli interessati resta, pertanto, la base legale di riferimento, pur con le criticità evidenziate nel paragrafo precedente.

In questa cornice, il legislatore italiano prevede, all'art. 110 cod. privacy, due ulteriori "eccezioni" all'impiego del consenso quale base giuridica del trattamento di dati sanitari a fini di ricerca medica, biomedica ed epidemiologica[34]. La prima si limita a richiamare l'art. 9, par. 2, lett. *j*), del GDPR, là dove consente i trattamenti necessari, tra l'altro, a fini di ricerca scientifica

---

[31] Su tali basi giuridiche, che comportano limitazioni al diritto alla cancellazione ai sensi dell'art. 17, par. 3, lett. *c-d*), del GDPR, si rinvia a M. Faccioli, *Le condizioni di liceità*, cit., 1132 ss..; A. Thiene, *La regola e l'eccezione*, cit., 15 ss.; P. Guarda, *I dati sanitari*, cit., 601 ss.

[32] Cfr., per tutti, L. Bolognini-E. Pelino, *Art. 110. Ricerca medica, biomedica ed epidemiologica*, in *Codice della disciplina privacy*, cit., 566 s.

[33] V. la nt. precedente.

[34] Non si tratta propriamente di eccezioni alla regola del consenso, benché questa appaia l'impostazione della norma in esame nel configurare ipotesi in cui il consenso dell'interessato «non è necessario…» (v., per tutti, P. Aurucci, *Il trattamento dei dati personali*, cit., 201). Tale impostazione "consenso-centrica", sulle cui ragioni si rinvia a F. Piraino, *Il regolamento generale*, cit., 383, permea invero la disciplina italiana di protezione dei dati, anche nelle sue parti ormai abrogate, come l'art. 23 cod. privacy, e già l'art. 11 della legge 31 dicembre 1996, n. 675 ("Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali").

Per contro, come già osservato nel paragrafo precedente, nel quadro direttamente applicabile e prevalente delineato dal GDPR – e, prima ancora, dalla direttiva 95/46/CE – il consenso degli interessati non rappresenta la base legale da adottare di regola: conf., nella dottrina più risalente, V. Cuffaro, *Il consenso dell'interessato*, in Id.-V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Torino, 1997, 204 (ulteriori riferimenti in V. Bachelet, *Il consenso oltre il consenso. Dati personali, contratto, mercato*, Pisa, 2023, 39).

sulla base del diritto dell'Unione o nazionale, precisando che quest'ultimo comprende tanto le disposizioni di legge quanto quelle regolamentari, e che la relativa fattispecie si estende anche alle ricerche biomediche o sanitarie incluse nella programmazione del Servizio sanitario nazionale ai sensi dell'art. 12-*bis* del d.lgs. n. 502 del 1992.

Profittando del potere di mantenere o introdurre condizioni e limitazioni ulteriori rispetto a quelle previste dal diritto dell'Unione per il trattamento di dati genetici, biometrici o sanitari in forza dell'art. 9, par. 4, del GDPR[35], la norma nazionale precisa che tali ricerche possono essere condotte senza il consenso degli interessati purché accompagnate da una valutazione d'impatto sulla protezione dei dati[36] resa pubblica. Per un'analisi più puntuale della disposizione, che riguarda la ricerca nel settore pubblico ed esula dalla più recente modifica dell'art. 110 cod. privacy, si rinvia agli studi specialistici sul tema[37].

Occorre, invece, focalizzare l'attenzione sulla seconda "eccezione" alla necessità del consenso prevista dall'art. 110 cod. privacy, che concerne la ricerca svolta al di fuori dalla programmazione pubblica ed è oggetto della novella legislativa in esame. Essa trova applicazione quando, «a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca»[38].

---

[35] Sui limiti che gli Stati membri incontrano nell'esercitare tale potere discrezionale, si vedano il considerando 53 del GDPR e le note seguenti.

[36] Disciplinata dall'art. 35 del GDPR: v. R. Torino, *La valutazione d'impatto (Data Protection Impact Assessment)*, in *I dati personali*, cit., 855 ss.

[37] V., *amplius*, M. Faccioli, *Le condizioni*, cit., 1137 ss.; in particolare, sul rapporto tra la previsione italiana e quella europea, P. Aurucci, *Il trattamento*, cit., 202 ss. Cfr., altresì, P. Guarda, *Art. 110. Ricerca medica, biomedica ed epidemiologica*, in *Codice della privacy*, cit., 1374 s.; L. Bolognini-E. Pelino, *Art. 110*, cit., 567 s.

[38] Il rapporto fra tale ipotesi e le basi legali del trattamento tassativamente previste dall'art. 9 del GDPR è meno agevole da definire rispetto alla prima ipotesi dell'art. 110 cod. privacy. Posto che la discrezionalità riconosciuta agli Stati membri dal par. 4 dell'art. 9 non è illimitata, ma va esercitata nel rispetto degli obiettivi indicati all'art. 1 del GDPR (ossia la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati: cfr. V. Bachelet, *Il consenso*, cit., 61 ss.), i legislatori nazionali non possono giungere a disapplicare le condizioni di legittimità del trattamento previste dal GDPR, come evidenzia P. Aurucci, *Il trattamento*, cit., 182 s., alla luce della giurisprudenza della Corte di giustizia.

Di conseguenza, la dottrina tende a ravvisare qui non tanto una – inammissibile – deroga alla base giuridica del consenso, quanto una mera deroga all'obbligo di informativa, ammessa dall'art. 14, par. 5, lett. *b*), GDPR, proprio nei casi elencati dall'art. 110 cod. privacy (Ead., ivi, 206 s.). Il limite di tale ricostruzione è, tuttavia, che l'art. 14 del GDPR si riferisce ai dati non raccolti presso l'interessato, mentre analoga deroga all'obbligo di informativa è assente qualora i dati vengano raccolti presso gli interessati ai sensi dell'art. 13 del GDPR, come accade quando il trattamento si fonda sul loro consenso: v., *amplius*,

Alla luce dei provvedimenti del Garante privacy, che hanno contribuito negli anni a concretizzare la delineata clausola generale[39], si deve trattare di casi "eccezionali" in cui sussistano difficoltà di ottenere il consenso dagli interessati, accuratamente documentate nel progetto di ricerca e riconducibili a due tipologie di fattori, tra loro alternativi: motivi *etici*, legati all'esigenza di non rivelare informazioni che potrebbero arrecare all'interessato un danno «materiale o psicologico» (ad esempio, la presenza di fattori premonitori di patologie incurabili)[40]; ovvero motivi *organizzativi*, quando ogni sforzo ragionevole per contattare gli interessati sia risultato infruttuoso[41], o – in ipotesi del tutto residuali – senza nemmeno tentare di contattarli, ove l'ampiezza del campione renderebbe lo sforzo sproporzionato. In ogni caso, purché risulti che la mancata raccolta dei dati relativi agli interessati non contattabili, considerato il numero complessivo dei soggetti coinvolti, pregiudicherebbe significativamente la qualità dei risultati della ricerca[42].
Come anticipato, la più recente novella dell'art. 110 cod. privacy, introdotta dal d.l. n. 19 del 2024, convertito con modificazioni dalla legge n. 56 del 2024, è stata promossa dalle società scientifiche interessate alla semplificazione della ricerca sanitaria. Essa mira, in effetti, a ricalibrare il bilanciamento tra autodeterminazione informativa, da un lato, e diritto alla salute – inteso quale interesse pubblico preminente – dall'altro.
Nella sua formulazione precedente, oltre ai presupposti sostanziali sui quali ci siamo da ultimo soffermati, la disposizione richiedeva, per legittimare il trattamento di dati sanitari a fini di ricerca medica, biomedica ed epidemiologica senza il consenso degli interessati: *i*) l'adozione di misure appropriate a tutelare l'interessato; *ii*) l'acquisizione del motivato parere fa-

L. Bolognini-E. Pelino, *Art. 110*, cit., 568.

[39] V., da ultimo, GPDP, *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice*, 9 maggio 2024, § 2, e già GPDP, *Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del d.lgs. 10 agosto 2018, n. 101*, 5 giugno 2019, § 5.3. Mette in luce alcune differenze tra i due provvedimenti M. Faccioli, *Le condizioni*, cit., 1139, nt. 89.

[40] Lo precisa GPDP, *Provvedimento recante le prescrizioni*, cit., § 5.3.

[41] GPDP, provv. 26 ottobre 2023, § 4.1, ha ritenuto proporzionati, nell'ambito di uno studio no profit, cinque tentativi di contatto telefonico.

[42] «[A]vuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti»: cfr., ancora, GPDP, *Regole deontologiche*, cit., e, per un esempio applicativo, GPDP, provv. 26 ottobre 2023, cit., § 1.
Intendendo l'impatto sulla qualità dei risultati della ricerca come un requisito cumulativo rispetto all'impossibilità o allo sforzo sproporzionato per informare gli interessati, il Garante sembra peraltro accogliere un'interpretazione restrittiva (*contra legem*) del passaggio dell'art. 110 cod. privacy riportato sopra nel testo, secondo cui il rischio di pregiudicare gravemente le finalità della ricerca costituisce, invece, una condizione alternativa.

vorevole sul programma di ricerca, reso dal comitato etico territorialmente competente; *iii*) nonché la sottoposizione dello stesso alla preventiva consultazione del Garante ai sensi dell'art. 36 del GDPR.

Quest'ultimo gravoso onere procedurale era stato introdotto dal legislatore italiano con il d.lgs. n. 101 del 2018[43], profittando dei margini consentiti dalla richiamata disposizione del GDPR che, mentre al primo paragrafo esige la consultazione preventiva del Garante per trattamenti a rischio elevato senza misure contenitive del rischio, al quinto paragrafo consente agli Stati membri di estendere tale onere a trattamenti finalizzati a compiti di interesse pubblico, tra cui quelli riguardanti la sanità pubblica, anche in assenza dei suddetti presupposti[44].

Avvalendosi di tale facoltà, l'art. 110 cod. privacy includeva dunque, quale ulteriore condizione di liceità del trattamento di dati sanitari destinati alla ricerca medico-sanitaria – oltre alle misure appropriate a tutela degli interessati e al parere positivo del comitato etico – anche la consultazione preventiva del Garante, indipendentemente dall'esito della valutazione d'impatto sulla protezione dei dati[45]. Secondo i critici, tale approccio tendeva a disincentivare la ricerca[46] e, al contempo, sovraccaricava l'attività

[43] 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)". Si veda, in particolare, l'art. 8, c. 2, lett. *r*).

Il requisito della preventiva consultazione del Garante aveva sostituito il previgente regime autorizzatorio, divenuto incoerente con l'impianto del GDPR fondato sul principio della responsabilizzazione (o *accountability*) dei titolari del trattamento, chiamati dall'art. 5, par. 2, a "rendere conto del loro operato", dimostrando di trattare i dati nel rispetto dei principi di cui al par. 1: cfr., per tutti, R. Caterina, *Novità e discontinuità nel Regolamento generale sulla protezione dei dati*, in Id. (a cura di), *GDPR tra novità e discontinuità*, in *Giur. it.*, 2019, 2777 ss. Il precedente regime autorizzatorio non riguardava, tuttavia, ogni singolo programma di ricerca: l'art. 110 cod. privacy, rinviando all'abrogato art. 40, consentiva infatti autorizzazioni generali per la ricerca scientifica, relative a determinate categorie di titolari e di trattamenti (cfr. GPDP, *Autorizzazione n. 9/2016 – Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica*, 15 dicembre 2016, che rinnova l'omologa *Autorizzazione n. 9/2012*, 13 dicembre 2012), tanto da delineare un regime per il trattamento dei dati sanitari destinati alla ricerca scientifica nei fatti più agile rispetto al meccanismo della specifica consultazione preventiva del Garante introdotto dal d.lgs. 101 del 2018.

[44] Lo segnala, ad es., D. Fulco, *Modifica dell'art. 110 Codice privacy*, cit.

[45] V. la precedente nt. 36.

[46] Anche alla luce dei termini previsti affinché il Garante renda un parere in merito alla richiesta: otto settimane, prorogabile di ulteriori sei in funzione della complessità del trattamento, ai sensi dell'art. 36, par. 2, del GDPR, secondo cui la decorrenza del termine massimo di quattordici settimane può, oltretutto, essere sospesa in caso di richieste di

dello stesso Garante, chiamato a pronunciarsi su ogni singolo programma di ricerca[47].

In questo senso, va pertanto accolto con favore lo snellimento apportato dalla l. 56/2024, che ha eliminato dalla disposizione in esame la necessità della preventiva consultazione del Garante, sostituendola con l'obbligo di osservare le garanzie individuate dallo stesso ai sensi dell'art. 106, cpv., lett. *d*), cod. privacy, da rispettare nei casi in cui si può prescindere dal consenso degli interessati. Tali garanzie comprendono, oltre ai già illustrati chiarimenti sui motivi etici o organizzativi che consentono di trattare i dati sanitari, anche l'obbligo di svolgere e pubblicare la valutazione d'impatto sulla protezione dei dati, dandone comunicazione al Garante[48].

All'esito dell'ultima novella, l'ordinamento italiano permette quindi, ove ricorrano le suddette condizioni sostanziali, il trattamento di dati sanitari a fini di ricerca medica, biomedica o epidemiologica, anche senza il consenso degli interessati, purché il relativo programma di ricerca sia stato approvato dal comitato etico e il titolare adotti misure appropriate a tutelare gli stessi, sulla base della valutazione d'impatto resa pubblica e comunicata al Garante. Non è, invece, più necessaria la sua consultazione preventiva, a meno che la valutazione d'impatto rilevi trattamenti a rischio elevato privi di misure contenitive, secondo le ordinarie regole di cui all'art. 36 del GDPR[49].

Il nuovo assetto normativo appare in definitiva idoneo, specie se adeguatamente integrato da future regole deontologiche chiare e organiche, a favorire un più equilibrato bilanciamento fra tutela dei diritti degli interessati e libera circolazione dei dati sanitari a fini di ricerca scientifica[50]. La delineata semplificazione non appare, peraltro, solo opportuna nella prospettiva de-

chiarimenti da parte del Garante. V., *amplius*, P. Aurucci, *Il trattamento*, cit., 208, testo e nt. 253.

[47] V., ancora, P. Aurucci, *Il trattamento*, cit., 208 s. Ulteriori riferimenti in Ead.-F. Di Tano, *Dati personali e ricerca medica: condizioni, incoerenze e prospettive giuridiche a fronte dell'evoluzione interpretative e applicativa del Garante per la protezione dei dati personali*, in *Riv. biodir.*, 2024, 324, nt. 36, ai quali si rinvia anche per una panoramica sui pareri resi dal Garante, a seguito della consultazione preventiva, in materia di programmi di ricerca (308 s., nt. 7, e 310 ss.).

[48] Così GPDP, *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*, cit., § 2, nelle more dell'adozione delle nuove regole deontologiche che l'art. 106, c. 1, cod. privacy impegna il Garante a promuovere, ai sensi dell'art. 2-*quater* cod. privacy (su cui v. L. Bolognini, *Art. 2-quater. Regole deontologiche*, in Id.-E. Pelino (a cura di), *Codice della disciplina privacy*, cit., 481 ss.), al fine di individuare le garanzie adeguate per i diritti e le libertà dell'interessato in conformità all'art. 89 del GDPR, che i soggetti pubblici e privati interessati al trattamento a fini statistici o di ricerca scientifica sono tenuti a rispettare: v., *amplius*, P. Aurucci-F. Di Tano, *Dati personali*, cit., 324 ss.

[49] Cfr. F. Cascini-M.A. Arcuri, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale*, in *Dir. inf.*, 2024, 869.

[50] Si vedano P. Aurucci-F. Di Tano, *Dati personali*, cit., 326, e la nt. precedente.

gli enti che svolgono la ricerca sanitaria, ma è anche coerente con il sistema del GDPR, che incoraggia tali trattamenti, come si è visto in precedenza, attraverso il temperamento del principio di limitazione della finalità di cui all'art. 5, par. 1, lett. *b*)[51] e la previsione di una base legale specifica per la ricerca scientifica ai sensi dell'art. 9, par. 2, lett. *j*).[52]

4. Il declino del consenso nel c.d. fascicolo sanitario elettronico 2.0

Dopo aver illustrato l'evoluzione della normativa italiana in materia di dati sanitari destinati alla ricerca scientifica, occorre ora soffermarsi sugli sforzi compiuti dal legislatore per l'attuazione del c.d. fascicolo sanitario elettronico, deputato istituzionalmente a raccogliere e contenere «l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alla prestazioni erogate al di fuori del Servizio sanitario nazionale»[53]. Una volta pienamente operativo e alimentato con informazioni sanitarie complete per tutti gli assistiti, esso costituirà, infatti, un enorme bacino di dati di straordinaria rilevanza per la ricerca scientifica.

In continuità con quanto già visto per l'art. 110 cod. privacy, anche la promozione di tale strumento passa attraverso un riassetto del bilanciamento tra autodeterminazione informativa e diritto alla salute, valorizzando quest'ultimo quale interesse pubblico prevalente e riducendo, di conseguenza, il ruolo del consenso individuale.

Come è noto, il fascicolo sanitario elettronico è stato introdotto dal d.l. 179 del 2012[54], per poi subire ben undici modifiche normative nel corso

[51] Si consideri, altresì, la derogabilità del principio di limitazione della conservazione di cui alla lett. *e*), che ammette la conservazione per periodi più estesi dei dati trattati esclusivamente a fini di ricerca scientifica, nel rispetto delle garanzie di cui all'art. 89, par. 1, del GDPR.

[52] Cfr. inoltre la derogabilità dell'obbligo di informativa stabilita all'art. 14, par. 5, lett. *b* (v. *supra* alla nt. 38); i limiti al diritto alla cancellazione di cui all'art. 17, par. 3, lett. *d* (v. *supra* alla nt. 31); la derogabilità di alcuni diritti dell'interessato ai sensi dell'art. 89, par. 2, del GDPR, nonché i considerando nn. 33 e 50 già richiamati nel testo: v. L. Bolognini-E. Pelino, *Art. 110*, cit., cit., 565 s., e G.M. Uda, *Il trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, cit., 557.

[53] Cfr. l'art. 12, c. 1, del d.l. 179/2012, come integrato, quanto alle prestazioni erogate al di fuori del SSN, dall'art. 11 del d.l. 34/2020. Per altre definizioni del fascicolo sanitario elettronico, elaborate dalla dottrina e dal Garante privacy, si rinvia a S. Corso, *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Nuove leggi civ. comm.*, 2024, 341.

[54] Convertito con modificazioni dalla legge n. 221 del 2012. Rilevante, ai nostri fini, è la sezione IV in materia di "Sanità digitale", e in particolare l'art. 12, rubricato "Fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità

del decennio successivo[55], intervallate da un'intensa attività del Garante privacy, in funzione sia di vigilanza che consultiva. L'obiettivo di tale strumento, basato su una «federazione [nazionale] di architetture regionali»[56], era, secondo le linee guida ministeriali del 2010, quello di rendere accessibili le informazioni sanitarie per finalità di cura della persona[57]. In tale prospettiva, risultava naturale subordinare sia la formazione del fascicolo sia l'inserimento dei singoli documenti alla volontà di ciascun assistito e, quindi, alla sua autodeterminazione individuale[58]: un consenso distinto da quello richiesto per la consultazione del fascicolo, il cui mancato rilascio non pregiudica il diritto alla prestazione sanitaria[59].

Nella sua configurazione iniziale, il fascicolo sanitario elettronico costituiva, dunque, essenzialmente un contenitore di documenti sanitari: parziale, a causa del segnalato vincolo del consenso individuale, ma anche della lentezza e della diversa capacità delle Regioni di implementarne l'uso[60]. Era inoltre un contenitore di documenti sanitari per lo più "non strutturati", limitati a scansioni degli originali cartacei: il risultato della mera digitalizzazione dell'analogico, senza ancora la conversione in dati – o "datizzazione"[61] – che rende possibili sia analisi automatizzate su larga scala sia l'addestramento di modelli di intelligenza artificiale.

---

digitale": cfr. P. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, 2011, *passim*. V. già l'art. 8 della legge regionale toscana 9 novembre 2009, n. 65, che introduce l'art. 76-*bis* ("Fascicolo sanitario elettronico") nella legge regionale del 24 febbraio 2005, n. 40, intitolata "Disciplina del servizio sanitario regionale".

[55] Per una elencazione delle quali, si rinvia a S. Corso, *Il trattamento dei dati personali in ambito sanitario*, cit., 11 s., nt. 56.

[56] L'efficace locuzione è di V. Peigné, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in *Riv. it. med. leg.*, 2011, 1522, la quale ricorda che la tutela della salute costituisce materia legislativa concorrente tra Stato e Regioni ai sensi dell'art. 117 Cost.: v., *amplius*, C. Silvano, *La digitalizzazione dei servizi sanitari alla luce del riparto di competenze tra Stato e Regioni. Il caso del Fascicolo Sanitario Elettronico*, in *Federalismi*, 26, 2023, 228 ss.

[57] Segnatamente di «prevenzione, diagnosi, cura e riabilitazione»: cfr. Min. Salute, *Il Fascicolo Sanitario Elettronico. Linee guida nazionali*, 11 novembre 2010, § 2.2.

[58] V. la nt. precedente e gli ulteriori riferimenti in S. Corso, *Il fascicolo sanitario elettronico*, cit., 339 s. La precisazione che il fascicolo è alimentato «esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti nel fascicolo medesimo», era contenuta nell'art. 12, c. 3-*bis*, del d.l. 179/2012, introdotto dalla legge di conversione 212/2012: v. *infra* nel testo.

[59] Art. 12, c. 5, del d.l. 179/2012: cfr. S. Faillace, *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS*, Milano, 2025, 20. Le finalità di consultazione per le quali è richiesto il consenso sono quelle di cui alle lett. a), a-*bis*), a-*ter*) della norma in esame: v. la successiva nt. 64 e, *amplius*, nel testo.

[60] S. Corso, *Il fascicolo sanitario elettronico 2.0*, cit., 342.

[61] Cfr. V. Mayer-Schonberger-K. Cukier, *Big Data*, cit., spec. 109.

Anche alla luce di tali limiti, il piano nazionale di ripresa e resilienza ha rilanciato lo strumento, dedicando alla c.d. missione 6, relativa alla "salute", interventi in materia di telemedicina e digitalizzazione della sanità[62]. Quale elemento chiave di tale processo di digitalizzazione, al fascicolo sanitario elettronico sono stati destinati ingenti finanziamenti e un programma di attuazione rigoroso il cui rispetto costituisce una delle condizioni per l'erogazione delle risorse stanziate[63].

Quanto qui interessa rilevare è che la finalità di ricerca scientifica, insieme a quella di efficiente governo del sistema sanitario – pur considerate sin dalla prima configurazione normativa del fascicolo sanitario elettronico nel 2012[64] – hanno assunto nel tempo un rilievo progressivamente più marcato. Il salto più evidente si registra, in particolare, con il «fascicolo sanitario elettronico 2.0», come delineato dal decreto del Ministero della Salute del 7 settembre 2023[65].

Tale evoluzione è stata preparata da una serie di interventi normativi[66], tra i quali si segnala il d.l. 34 del 2020[67], che ha eliminato il previo consenso dell'assistito quale requisito per la c.d. alimentazione del fascicolo sanitario[68], con ciò facendo venir meno anche la necessità, a monte, del consenso per la sua attivazione[69]. Tale previsione, fondamentale affinché tutti gli

[62] Vedi spec. 233 ss. del testo consultabile all'indirizzo *governo.it*.

[63] Vedi la nt. precedente e il portale istituzionale "PNRR Salute", sezione Missione 6 – Investimento 1.3 Rafforzamento dell'infrastruttura tecnologica e strumenti per la raccolta e l'analisi dei dati, consultabile all'indirizzo *pnrr.salute.gov.it*.

[64] Oltre alla finalità di prevenzione, diagnosi, cura e riabilitazione (lett. *a*), il testo originario dell'art. 12 del d.l. 179/2012, assegnava al fascicolo sanitario elettronico anche quella di «studio e ricerca scientifica in campo medico, biomedico ed epidemiologico» (lett. *b*), oltre a quelle di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria (lett. *c*). Successivamente, l'art. 21 del d.l. 4/2022, conv. in legge 34/2022, ha aggiunto anche le finalità di prevenzione (lett. a-*bis*) e di profilassi internazionale (lett. a-*ter*), l'art. 36 del d.lgs. 62/2024 quella di valutazioni e accertamenti sanitari per il riconoscimento di prestazioni assistenziali e previdenziali (lett. c-*bis*).

[65] Che ha in larga misura sostituito il precedente d.p.c.m. 29 settembre 2015, n. 178, intitolato "Regolamento in materia di fascicolo sanitario elettronico".

[66] S. Corso, *Il fascicolo sanitario elettronico*, cit., 344 ss.

[67] Convertito, con modificazioni, in legge 77 del 2020, con l'effetto di abrogare l'art. 12, c. 3-*bis*, del d.l. 179/2012.

[68] Con la conseguenza che il relativo trattamento si fonda ora sulla «necessità per finalità [...] di gestione dei sistemi e servizi sanitari o sociali sulla base del diritto [...] degli Stati membri», e deve essere eseguito da o sotto la responsabilità di un professionista sanitario soggetto al segreto professionale ai sensi dell'art. 9, par. 2, lett. *h*), e par. 3 del GDPR: v. GPDP, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7 marzo 2019, § 1.

[69] Cfr., per tutti, S. Faillace, *Prospettive civilistiche*, cit., 21, nt. 31 s., a cui si rinvia per ulteriori riferimenti.

assistiti siano dotati di un fascicolo sanitario elettronico tendenzialmente completo, va letta in raccordo con l'obbligo di inserire ogni prestazione sanitaria resa da operatori pubblici e privati accreditati o autorizzati entro cinque giorni dalla sua erogazione, introdotto successivamente dal d.l. 4 del 2022[70].

A seguito di tali interventi normativi e di una interlocuzione con il Garante privacy, è stato quindi emanato il decreto ministeriale 7 settembre 2023, recante il c.d. Fascicolo sanitario elettronico 2.0[71]. Esso ha, in primo luogo, contribuito a rafforzare il delineato obiettivo di costituire un ampio bacino di *Big Data* sanitari, idoneo anche alla ricerca scientifica, attraverso l'analitica individuazione dei soggetti tenuti ad alimentare il fascicolo sanitario e la previsione della loro responsabilità in caso di mancato, intempestivo o inesatto adempimento[72].

Divenuta automatica l'attivazione e l'alimentazione del fascicolo sanitario, il consenso rimane l'istituto attraverso cui l'assistito individua i soggetti autorizzati a consultarne i contenuti, a meno che ricorrano i presupposti del c.d. accesso in emergenza, nei casi di rischio grave, imminente e irreparabile per la salute o l'incolumità dell'interessato che, non avendo acconsentito alla consultazione del proprio fascicolo sanitario, si trovi nell'incapacità fisica o giuridica di esprimere il consenso[73].

L'autodeterminazione dell'assistito non viene meno, ma opera ormai "a valle" di un fascicolo sanitario alimentato a prescindere dal suo consenso. Il legislatore, peraltro, ne indirizza l'esercizio in chiave quasi paternalistica: in questa prospettiva, si comprende la disciplina che, da un lato, subordina alla manifestazione di un consenso "generale" dell'assistito la consultazione del suo fascicolo sanitario e, dall'altro, richiede un consenso ulteriore –

---

[70] Convertito, con modificazioni, in legge 25 del 2022, che ha integrato il testo dell'art. 12, c. 1, del d.l. 179/2012: cfr. S. Corso, *Il fascicolo*, cit., 345.

[71] Su cui v., in generale, I. Rapisarda, *Appunti sul fascicolo sanitario elettronico 2.0*, in *Resp. med.*, 2024, 57 ss.

[72] Sull'importanza di tale previsione, introdotta dall'art. 12, c. 3, del decreto ministeriale, si sofferma S. Corso, *Autodeterminazione e dati sanitari*, cit., 232, ricordando che essa tiene conto delle preoccupazioni espresse dal GPDP, *Parere al Ministero della Salute sullo schema del decreto, da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministero dell'economia e delle finanze, sul Fascicolo Sanitario Elettronico (FSE)*, 22 agosto 2022.

[73] A causa dell'impossibilità fisica, incapacità di agire, o di intendere o di volere: cfr. l'art. 20 del d.m. 7 settembre 2023, che in tali casi autorizza gli esercenti le professioni sanitarie e gli operatori del Servizio sanitario nazionale e dei servizi socio-sanitari regionali ad accedere prioritariamente al c.d. profilo sanitario sintetico dell'interessato (v. l'art. 4) e, ove necessario, agli ulteriori dati contenuti nel fascicolo sanitario elettronico, salvo quelli oscurati ai sensi dell'art. 9, per il tempo strettamente necessario ad assicurare all'assistito le cure indispensabili, fino a quando questi non sia nuovamente in grado di esprimere la propria volontà al riguardo.

esplicito, informato e specifico, da rendere al soggetto che eroga la prestazione – per autorizzare la consultazione dei dati sanitari "supersensibili", inerenti alla sfera della sessualità o concernenti situazioni particolarmente stigmatizzanti[74], i quali risultano di *default* visibili solo dall'interessato.
Quanto più importa rilevare è che, oltre a omettere il consenso affinché tali dati siano consultati, l'assistito può scegliere di ricevere le relative prestazioni in anonimato, con l'effetto di impedire addirittura l'alimentazione del fascicolo[75], limitando in via del tutto eccezionale il novero dei dati contenuti. Si tratta, a ben vedere, di un diritto distinto da quello all'oscuramento, che l'assistito può esercitare tramite specifica istanza resa al momento della prestazione ovvero in seguito[76] e sempre revocare[77], con l'effetto di nascondere un dato pur immesso nel fascicolo, senza che alcuno dei soggetti abilitati ad accedervi per finalità di cura, prevenzione e profilassi internazionale possa avvedersi dell'avvenuto oscuramento (c.d. oscuramento dell'oscuramento)[78].
Tale articolata disciplina mira evidentemente a bilanciare l'esigenza di garantire all'assistito un controllo sui propri dati con esigenze di carattere pubblicistico, non limitate alla tutela della salute in senso stretto – come mostra il c.d. accesso in emergenza al fascicolo sanitario – ma estese anche alla costituzione di un bacino di dati sanitari il più possibile completo, destinato, tra l'altro, a essere trattato a fini di ricerca scientifica. Nella prospettiva di questo studio, risulta pertanto decisivo chiarire a quali condizioni tale vasto bacino di dati possa essere utilizzato nella ricerca.
A questo proposito, occorre sottolineare che la delineata disciplina del consenso concerne la consultazione del fascicolo sanitario per finalità di diagnosi, cura, riabilitazione, prevenzione e profilassi internazionale[79]. Per quanto concerne, invece, le finalità di ricerca medica, biomedica ed epidemiologica, oltre che di *governance* sanitaria, già l'art. 12, c. 6, del d.l.

[74] Così, sotto la rubrica "Dati soggetti a maggiore tutela dell'anonimato", l'art. 6, c. 1, del d.m. 7 settembre 2023, sottopone a tale regime speciale i dati e i documenti sanitari e socio-sanitari disciplinati dalle disposizioni a tutela delle persone sieropositive, che abbiano subito atti di violenza sessuale o di pedofilia, che facciano uso di sostanze stupefacenti, psicotrope o alcoliche, delle donne che si sottopongano a un'interruzione volontaria di gravidanza o decidano di partorire in anonimato. Il regime speciale di protezione si applica, infine, a tutti i dati e documenti relativi ai servizi offerti dai consultori familiari.

[75] Art. 6, c. 3, del d.m. 7 settembre 2023.

[76] Art. 9, c. 3, del d.m. 7 settembre 2023.

[77] Con le medesime modalità previste per l'esercizio del diritto di oscuramento: v. l'art. 9, c. 5, del d.m. 7 settembre 2023.

[78] Cfr. S. Corso, *Il fascicolo sanitario elettronico*, cit., 357.

[79] Ai sensi dell'art. 12, commi secondo e quinto del d.l. 179 del 2012.

179/2012 autorizzava una serie di soggetti pubblici[80] a trattare i dati del fascicolo sanitario, nei limiti delle rispettive competenze e senza l'utilizzo degli identificativi degli assistiti, secondo modalità da definirsi con decreto ministeriale[81].

In seguito, il c. 1-*bis* dell'art. 2-*sexies* cod. privacy[82], introdotto dal d.l. 139/2021[83], ha inteso legittimare ulteriormente – riconducendoli nell'alveo dei trattamenti necessari per motivi di interesse pubblico rilevante ai sensi dell'art. 9, par. 2, lett. *g*), del GDPR – il trattamento dei dati sanitari pseudonimizzati[84] svolto nel rispetto delle rispettive finalità istituzionali, anche di ricerca scientifica[85], da un più ampio novero di soggetti pubblici[86] secondo le modalità individuate anche qui con decreto ministeriale[87]. Il c. 1-*ter* dell'art. 2-*sexies* cod. privacy ricomprende espressamente, tra tali trattamenti, anche quelli svolti mediante il fascicolo sanitario elettronico[88], che

[80] Quali le Regioni, il Ministero del lavoro e delle politiche sociali, il Ministero della salute, a cui si è aggiunta l'Agenzia nazionale per i servizi sanitari regionali (AGENAS), a opera dell'art. 42 del d.l. 19/2024, convertito in l. 56/2024.

[81] Decreto del Ministro della salute e del Ministro delegato per l'innovazione tecnologica – di concerto con il Ministro dell'economia e delle finanze, sentita la Conferenza permanente per i rapporti Stato-Regioni e acquisito il parere del Garante privacy – chiamato a definire, in particolare, livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti dallo stesso decreto, in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali: v. l'art. 12, c. 6 e 7, del d.l. 179/2012.

[82] Su cui v. E. Pelino, *Art. 2-sexies. Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*, in *Codice della disciplina privacy*, cit., 490. Per gli sviluppi più recenti nel quadro del c.d. EHDS, si rinvia a S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, in *Nuove leggi civ. comm.*, 2025, spec. 599 ss.

[83] Convertito, con modificazioni, in l. 205/2021.

[84] «Privi di elementi identificativi diretti» nel testo dell'allegato alla legge di conversione 205/2021, locuzione poi modificata in «pseudonimizzati» dall'art. 44 del d.l. 19/2024, conv. in l. 56/2024: v. la successiva nt. 99.

[85] Il trattamento a fini di ricerca scientifica, in particolare, resta soggetto alla disciplina regolamentare precedente (artt. da 15 a 17 del d.p.c.m. 29 settembre 2015, n. 178, "Regolamento in materia di fascicolo sanitario elettronico"), in attesa della sua sostituzione con la normativa secondaria attuativa del nuovo assetto del fascicolo sanitario elettronico: v., *amplius*, S. Corso, *Il fascicolo sanitario elettronico*, cit., 346.

[86] Segnatamente il Ministero della Salute, l'Istituto superiore di sanità (ISS), l'AGENAS, l'Agenzia italiana del farmaco (AIFA), l'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà (INMP), nonché le Regioni relativamente ai propri assistiti.

[87] Decreto del Ministro della salute, previo parere del Garante privacy: cfr. d.m. Salute 31 dicembre 2024, che ha istituito l'Ecosistema dei dati sanitari (EDS), spec. art. 17, intitolato "Accesso ai servizi dell'EDS per la finalità di studio e di ricerca scientifica".

[88] Tale riferimento è stato spostato dal c. 1-*bis* al c. 1-*ter* a opera del d.l. 19 del 2024, convertito con modificazioni in l. 56 del 2024.

possono così essere effettuati, in presenza delle condizioni previste, senza il previo consenso degli interessati.
Da ultimo, l'art. 12-*bis* del d.l. 179 del 2012, introdotto dall'art. 10 della legge 132 del 2025, alla quale è dedicato il paragrafo seguente, prevede l'utilizzo di soluzioni di intelligenza artificiale a supporto delle finalità perseguite dal fascicolo sanitario elettronico, incluse quelle di ricerca scientifica[89], demandando a decreti ministeriali l'individuazione dei soggetti che vi hanno accesso e delle relative modalità.
Nella sua più recente evoluzione, il c.d. fascicolo sanitario elettronico 2.0 si configura, dunque, come un contenitore di *Big Data* sanitari sempre più strutturato e completo, alimentato per lo più senza il consenso degli interessati e concepito quale risorsa collettiva da impiegare sia per la ricerca scientifica sia a supporto della sperimentazione e dell'innovazione tecnologica mediante sistemi di intelligenza artificiale.

5. Il contributo della legge in materia di intelligenza artificiale

In questo quadro, si inserisce ora l'art. 8 della legge 23 settembre 2025, n. 132, contenente "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", che rappresenta un ulteriore tassello dell'evoluzione normativa delineata. Tale disposizione, rubricata "Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario", conferma la rilevata tendenza a ridurre gli spazi riservati all'autodeterminazione individuale, valorizzando piuttosto l'interesse pubblico sotteso allo sviluppo di sistemi di intelligenza artificiale in ambito sanitario[90].
In tale prospettiva, il c. 1 dell'art. 8 stabilisce che i trattamenti di dati, anche personali, effettuati per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di IA destinati a una serie di finalità – di prevenzione, diagnosi e cura, incluso lo sviluppo di farmaci, terapie e tecnologie

[89] Per il supporto delle finalità di cura in particolare, la norma prevede l'istituzione di una piattaforma di intelligenza artificiale, affidata all'AGENAS e finalizzata a fornire servizi di supporto ai professionisti sanitari e agli utenti, specie nell'assistenza territoriale: v, *amplius*, l'art. 12-*bis*, c. 2, del d.l. 179 del 2012.

[90] Con riguardo alle possibili applicazioni dell'intelligenza artificiale, in particolare generativa, in ambito sanitario, cfr. D. Amram, *Governo dei dati, open AI e salute: profili introduttivi*, in *Riv. it. med. leg.*, 2023, 293 ss. In generale, in tema di intelligenza artificiale, si veda lo scritto pioneristico di A.M. Turing, *Computing Machinery and Intelligence*, in *Mind*, LIX, 1950, 433 ss. (ed. italiana: *Macchine calcolatrici e intelligenza*, D. Marconi (trad. it.), Torino, 2025).

riabilitative[91] – sono considerati di rilevante interesse pubblico in quanto necessari a costituire e utilizzare banche dati e modelli di base. La norma nazionale, che giustifica la sussistenza di un siffatto interesse pubblico alla luce degli artt. 32 e 33 Cost., in materia di tutela della salute e della libertà della scienza, riserva tale base giuridica a enti pubblici e privati non lucrativi, Istituti di ricovero e cura a carattere scientifico (IRCCS) ed enti sanitari privati coinvolti in progetti di ricerca cui partecipano i predetti soggetti[92]. Legittimando i trattamenti indicati ai sensi del più volte richiamato art. 9, par. 2, lett. *g*), del GDPR[93], la norma offre un significativo impulso allo sviluppo dei sistemi di IA i quali, come anticipato, tendono a definire le finalità nel corso del trattamento[94], rendendo difficoltoso rispettare i requisiti di predeterminazione e specificità delle finalità imposti dall'art. 5, par. 1, lett. *b*)[95] e, in particolare, garantire la specificità del consenso, ove questo dovesse invece operare quale base giuridica del trattamento[96].

Nella consapevolezza che lo sviluppo dei sistemi di IA richiede spesso l'impiego di dati già raccolti per altri scopi, ad esempio sanitari e di cura, il c. 2 dell'art. 8 della legge in esame estende la legittimazione degli stessi soggetti a eseguire trattamenti volti ai medesimi fini di ricerca nella realizzazione di sistemi di IA anche su dati inizialmente acquisiti a fini diversi (c.d. uso secondario)[97]. L'intento è quello di ammetterne il "riutilizzo" oltre quanto previsto dall'art. 5, par. 1, lett. *b*), del GDPR che, come osservato, già attenua il principio di limitazione della finalità ritenendo compatibili con le finalità iniziali i trattamenti ulteriori a scopo di ricerca scientifica, ma impone il rispetto di garanzie in concreto adeguate ai sensi dell'art. 89,

---

[91] Finalità «di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria nonché studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario».

[92] Cfr. anche V. Fusco, *Il trattamento di dati personali per l'addestramento di sistemi di intelligenza artificiale in ambito medico: criticità del consenso e basi giuridiche alternative*, in *Riv. it. med. leg.*, 2025, 95.

[93] V. *supra* la nt. 23 e di seguito nel testo.

[94] Vedi C. De Menech, *Intelligenza artificiale*, cit., 198, e gli ulteriori riferimenti di cui alla precedente nt. 20.

[95] In conformità al principio di limitazione della finalità: cfr. EDPB, *Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita*, 20 ottobre, 2020, § 72.

[96] Dell'art. 8, c. 1, come di una disciplina che rende possibile il trattamento dei dati in assenza del consenso individuale discorre F. Paoloucci, *La legge italiana sull'intelligenza artificiale: attuazione nazionale dell'AI Act e primi nodi applicativi*, in *Quad. cost.*, 2025, 966.

[97] Su tale nozione si rinvia a S. Thobani, *L'uso secondario dei dati sanitari*, in *Autodeterminazione, cura e ricerca nell'era digitale*, cit., 222 ss.

par. 1[98].

Preso atto della tendenziale incompatibilità dei sistemi di IA con il principio di finalità, la norma stabilisce *ex ante* la loro liceità per determinati soggetti e finalità secondarie, riducendo le garanzie alla sola pseudonimizzazione[99] (peraltro esclusa quando inevitabile o necessario a tutela della salute degli interessati) e semplificando gli obblighi informativi, ridotti a una comunicazione generale sul sito web del titolare del trattamento[100]. La portata innovativa della norma è apprezzata dalla dottrina, che tuttavia rileva l'assenza di alcune tutele, previste invece dal regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari, come i divieti di uso secondario e il diritto degli interessati di escludere l'uso secondario (c.d. *opt-out*), oltre alla mancata concretizzazione normativa del principio di minimizzazione di cui all'art. 5, par. 1, lett. *c*), del GDPR[101].

Nel complesso, la legge italiana intende quindi legittimare l'uso sia primario che secondario dei dati, anche particolari, per la ricerca scientifica e la sperimentazione nella realizzazione di sistemi di IA destinati alle indicate finalità medico-sanitarie, ove eseguiti da enti pubblici e privati non lucrativi, IRCCS o enti sanitari privati coinvolti in progetti di ricerca cui partecipano tali soggetti. La tecnica adoperata, come osservato, consiste nell'individuare il rilevante interesse pubblico alla base di tali trattamenti ai sensi dell'art. 9, par. 2, lett. *g*), del GDPR, il quale esige che essi siano pro-

---

98 V. *supra* il § 2.

99 Intendere il riferimento ai «dati privi di elementi identificativi diretti» alla stregua di dati pseudonimizzati, in linea con la proposta *de iure condendo* del GPDP, *Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale*, 2 agosto 2024 – oltre che con la discussa modifica apportata all'art. 2-*sexies*, c. 1-*bis*, cod. privacy dall'art. 44 del d.l. 19/2024, convertito in l. 56/2024 – risulta sistematicamente opportuno per concludere che la legge italiana non esclude, ma piuttosto specifica le garanzie minime previste per i trattamenti a fini di ricerca scientifica dall'art. 89, par. 1, GDPR.

Propende invece per la piena applicabilità della norma regolamentare, che la legge in esame intenderebbe derogare, il Garante nel citato parere, per cui l'uso secondario sarebbe legittimato pur sempre nei limiti della presunzione di non incompatibilità di cui all'art. 5, par. 1, lett. *b*), GDPR, con la previsione di garanzie adeguate ai sensi dell'art. 89, non limitate alla sola pseudonimizzazione (conf. V. Fusco, *Il trattamento di dati personali*, cit., 97, alla quale si rinvia per ulteriori spunti).

100 Sull'idoneità sostanziale della quale a informare gli interessati è scettico GPDP, *Parere su uno schema di disegno di legge*, cit. (v. anche G. Resta-G.M. Riccio, *Il ddl AI è legge: primi spunti di riflessione*, in *Altalex*, 18 settembre 2025); mentre S. Stefanelli, *Legge AI, ecco come cambia la ricerca scientifica in Sanità*, in *Agenda digitale*, 17 settembre 2025, si limita a criticare la norma nella parte in cui non prevede che la pubblicazione sul sito preceda l'inizio del trattamento di un termine congruo.

101 V., rispettivamente, gli artt. 54 ("Uso secondario vietato"), 71 ("Diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali per l'uso secondario") e 66 ("Minimizzazione dei dati e limitazione della finalità") del c.d. EHDS: cfr., per tali rilievi, G. Resta-G.M. Riccio, *Il ddl AI è legge*, cit.

porzionati alle finalità perseguite, salvaguardino l'essenza del diritto alla protezione dei dati e siano corredati da misure appropriate e specifiche a tutela dell'interessato[102].

Valorizzando i requisiti di determinatezza esplicitati dall'art. 2-*sexies*, c. 1, cod. privacy – che richiede norme indicanti i tipi di dati, le operazioni eseguibili e i motivi di interesse pubblico rilevante, nonché misure appropriate e specifiche per tutelare l'interessato – il Garante della privacy aveva evidenziato la necessità di integrare l'art. 8 della legge in esame affinché costituisca un valido presupposto di legittimazione del trattamento nella cornice regolamentare europea[103]. Alcuni aspetti sono invero chiariti dall'art. 9[104], che affida al decreto del Ministro della salute, sentito il Garante[105], il compito di disciplinare i trattamenti finalizzati alla ricerca e alla sperimentazione anche tramite sistemi di IA e *machine learning* – inclusa la costituzione e l'utilizzo di spazi speciali di sperimentazione a fini di ricerca (c.d. *regulatory sandbox*), anche mediante l'uso secondario dei dati personali – adottando il massimo delle modalità semplificate consentite dal GDPR[106]. Una volta esemplificate le operazioni eseguibili sui dati personali, anche particolari, nell'ambito delle finalità di cui all'art. 8, c. 1, resta tuttavia generico soprattutto il novero degli enti legittimati e, segnatamente, la categoria dei soggetti pubblici[107].

Sotto il profilo procedurale, per compensare il minor spazio riservato all'autodeterminazione degli interessati, l'uso primario e secondario dei dati per la ricerca nella realizzazione di sistemi di IA resta sottoposto a un maggiore controllo del Garante privacy[108], al quale tali trattamenti devono essere previamente comunicati ai sensi del c. 5 dell'art. 8, con l'indicazione,

---

[102] Presupposto, quest'ultimo, che non sarebbe derogabile dalla legge nazionale secondo l'orientamento del Garante riportato alle note precedenti.

[103] GPDP, *Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale*, 2 agosto 2024.

[104] V. Fusco, *Il trattamento di dati personali*, cit., 97; conf. M. Faccioli, *Le condizioni di liceità del trattamento di dati sanitari*, cit., 1146.

[105] Sentiti, altresì, gli enti di ricerca e i presidi sanitari, le autorità e gli operatori del settore; il che rende difficile da rispettare il termine di centoventi giorni dalla data di entrata in vigore della legge previsto per l'emanazione del decreto.

[106] Per il trattamento di dati personali a scopo di ricerca: v. *supra* la nt. 49 s. e il testo corrispondente.

[107] Vedi S. Stefanelli, *Legge AI, ecco come cambia la ricerca scientifica in Sanità*, cit., e, più in generale, G. Resta-G.M. Riccio, *Il ddl AI è legge*, cit.

[108] Che gli Stati membri possono introdurre ai sensi del già menzionato art. 9, par. 4, GDPR, come ricorda V. Fusco, *Il trattamento di dati personali per l'addestramento di sistemi di intelligenza artificiale in ambito medico*, cit., 98.

tra l'altro, della valutazione d'impatto sulla protezione dei dati[109]. Grazie al meccanismo di "silenzio-assenso" previsto dalla norma, i trattamenti possono tuttavia essere avviati decorsi trenta giorni dalla comunicazione, qualora non intervenga un provvedimento di blocco del Garante[110].
Sempre al fine di promuovere lo sviluppo dei sistemi di IA destinati alle finalità medico-sanitarie indicate dal c. 1 (nonché per le finalità di *governance* sanitaria di cui all'art. 2-*sexies*, c. 2, lett. *v*), cod. privacy), il c. 3 dell'art. 8 consente, infine, i trattamenti di anonimizzazione, pseudonimizzazione o sintetizzazione dei dati personali – inclusi quelli particolari – senza richiedere il consenso degli interessati, fermo restando l'obbligo generale di informativa. L'utilità della previsione si coglie considerando che tali operazioni, riducendo o eliminando il legame con l'identità degli interessati, favoriscono l'uso dei dati per l'addestramento dei modelli di intelligenza artificiale[111]. In particolare, l'anonimizzazione e la creazione di dati sintetici, escludendo in modo irreversibile l'identificabilità dell'interessato, generano dati "non personali" che sfuggono al perimetro applicativo del GDPR[112]. Linee guida per tali peculiari procedure possono essere adottate

[109] Disciplinata dall'art. 35 del GDPR (v. la precedente nt. 36). Meno chiaro, quanto alle informazioni da rendere al Garante, il rinvio agli artt. 24 ("Responsabilità del titolare del trattamento"), 25 ("*Data protection by design and by default*") e 32 ("Sicurezza del trattamento") del GDPR, che riguardano obblighi da rispettare anziché documenti da comunicare: cfr. S. Stefanelli, *Legge AI*, cit.,

[110] Con il rischio, segnalato da D. Corti, *Consenso (a fasi progressive), interesse pubblico per l'IA, opt-out per l'uso secondario: le nuove regole per la ricerca scientifica sui dati sanitari*, in *Riv. biodir.*, 1, 2025, 286, che il controllo del Garante risulti più apparente che reale, a fronte di un numero eccessivo di comunicazioni.

[111] A prescindere da tale finalità, l'art. 8, c. 3, consente altresì il trattamento di anonimizzazione, pseudonimizzazione o sintetizzazione dei dati finalizzato «allo studio e alla ricerca sui gesti atletici, sui movimenti e sulle prestazioni nell'attività sportiva in tutte le sue forme, nel rispetto dei principi generali di cui alla presente legge e dei diritti di sfruttamento economico dei dati relativi alle attività agonistiche che spettano a chi le organizza». Criticamente, sull'indeterminatezza della locuzione «attività sportiva in tutte le sue forme», si vedano, *amplius*, G. Resta-G.M. Riccio, *Il ddl AI è legge*, cit.

[112] Che concerne, come è noto, i dati personali definiti dall'art. 4, n. 1. La stessa pseudonimizzazione, che consente tramite informazioni aggiuntive di attribuire nuovamente il dato all'interessato (art. 4, n. 5, e considerando 26 GDPR: cfr. V. Janeček-G. Malgieri, *Data Extra Commercium*, in S. Lohsse-R. Schulze-D. Staudenmayer (eds.), *Data as Counter-Performance – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy V*, Baden Baden-Oxford, 2020, 110 s.), potrebbe peraltro rendere il dato non personale rispetto al soggetto privo delle informazioni aggiuntive che consentono la re-identificazione del dato: v., *amplius*, CGUE, 4 settembre 2025, caso C-413/23, *GEPD c. SRB*, in *Nuova giur. civ. comm.*, I, 2026, 80 ss. (con nota di E. Grillo, *Dati pseudonimizzati ma non anonimi: la Corte UE ridefinisce i confini di "dati personali"*), a partire dalle omologhe previsioni del regolamento (UE) 2018/1725. V. già C. Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020, 387.

e aggiornate, ai sensi del c. 4 dell'art. 8, dall'Agenzia nazionale per i servizi sanitari regionali (AGENAS), previo parere del Garante privacy, tenendo conto degli standard internazionali e dello stato dell'arte tecnologico.
Nel complesso, gli artt. 8 e 9 della legge italiana in materia di intelligenza artificiale sembrano, dunque, trasporre nel settore della ricerca scientifica e della sperimentazione sanitaria con sistemi di IA quella logica di "messa a disposizione regolata" del dato già collaudata con il c.d. fascicolo sanitario elettronico 2.0, accentuando la centralità delle garanzie rispetto al consenso degli interessati. In questa prospettiva il dato sanitario, nei limiti tipizzati dal legislatore nazionale ed europeo, viene valorizzato quale risorsa collettiva funzionale alla ricerca, all'innovazione e al miglioramento dell'assistenza sanitaria.

6. Riflessioni conclusive

A conclusione dell'itinerario tracciato sull'evoluzione normativa nazionale in materia di ricerca scientifica sui dati sanitari – con particolare riguardo alla disciplina della "Ricerca medica, biomedica ed epidemiologica" (art. 110 cod. privacy), del "Fascicolo sanitario elettronico 2.0" (d.m. 7 settembre 2023) e, da ultimo, della "Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario" (art. 8, l. 132/2025) – si possono svolgere alcune riflessioni d'insieme.
Storicamente è sempre stata ravvisabile una contrapposizione tra un modello di protezione dei dati personali di tipo soggettivo, incentrato sul consenso dell'interessato quale strumento di controllo e autotutela[113], e un modello di tipo oggettivo, fondato piuttosto sulla presenza di garanzie del trattamento a prescindere dal consenso[114]. Già evidenziata da Stefano Rodotà in uno scritto pioneristico degli anni Settanta del secolo scorso[115], tale contrapposizione ha trovato nella c.d. direttiva "madre" del 1995 prima[116] – e nel GDPR poi – un punto di equilibrio da cui è emerso un modello di

[113] Questa è l'impostazione originaria del cod. privacy italiano (d.lgs. 196/2003) e già della legge 675/1996, in materia di "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali": v. riferimenti nella precedente nt. 34, cui *adde* S. Corso, *Autodeterminazione e dati sanitari*, cit., 125.

[114] Modello accolto dal *Bundesdatenschutzgesetz* del 1977, nonché dalla *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, adottata dal Consiglio d'Europa il 28 gennaio 1981, n. 108: cfr. F. Caggia, *Art. 7. Condizioni per il consenso*, in *Codice della privacy*, cit., 208 s., ove ulteriori riferimenti.

[115] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973 (rist. anast., Napoli, 2018), spec. 44.

[116] Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

protezione dei dati ibrido, nel quale il consenso costituisce una base legittimante del trattamento, senza essere l'unica né la principale[117].

Ora, la delineata evoluzione della normativa nazionale mostra come la presenza di un interesse pubblico nella ricerca scientifica sui dati sanitari attenui ulteriormente la funzione del consenso quale baluardo della persona, che in questo contesto rischia di ridursi a mero capriccio individuale. I benefici che la ricerca, ormai anche tramite l'intelligenza artificiale, arreca alla salute dei singoli e della collettività inducono, infatti, a restringere gli spazi riservati all'autodeterminazione degli interessati e a privilegiare tutele oggettive, capaci di garantire un più adeguato bilanciamento tra libertà individuale e interesse collettivo.

È questa la direzione che il legislatore italiano sembra oggi voler seguire, conformemente agli auspici della dottrina[118], consolidando il favore per la ricerca scientifica già radicato nell'architettura del GDPR.

Resta tuttavia da verificare, sul piano applicativo, se tale assetto sia effettivamente in grado di garantire un equilibrio sostenibile tra valorizzazione dei dati sanitari come risorsa collettiva e tutela dei diritti degli interessati, alla luce di un quadro normativo che permane, sotto più profili, complesso e non sempre coerente: soprattutto in ordine ai requisiti di necessità del trattamento, all'individuazione dei soggetti legittimati e alla reale capacità delle garanzie, poste a presidio degli interessati, di compensare la progressiva marginalizzazione del consenso.

[117] Vedi *supra* il § 2.

[118] V., da ultimo, S. Thobani, *Il consenso nella regolazione della circolazione dei dati*, in *Pers. merc.*, 2025, spec. 486, e G. Calabrese, *La protezione dei dati personali tra individuo e società*, Milano, 2025, 309 ss., ove ulteriori riferimenti.

Abstract

L'articolo analizza l'evoluzione della disciplina italiana sul trattamento dei dati sanitari per la ricerca medica, il fascicolo sanitario elettronico e l'intelligenza artificiale, con particolare attenzione al declino del consenso quale base giuridica. Si esaminano, segnatamente, l'art. 110 cod. privacy, come modificato dal d.l. 19/2024, che disciplina la ricerca sanitaria "senza consenso"; il d.m. 7 settembre 2023 sul fascicolo sanitario elettronico "2.0", che configura un bacino di Big Data per la ricerca e l'intelligenza artificiale; nonché la l. 132/2025 sull'intelligenza artificiale, che all'art. 8 si occupa di "Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario".

This article examines the evolution of the Italian legal framework on the processing of health data for medical research, the Italian Electronic Health Record, and artificial intelligence, focusing on the declining role of consent as a legal basis. It discusses Article 110 of the Italian Privacy Code, as amended by Decree-Law No. 19/2024, governing medical research "without consent"; the Ministerial Decree of 7 September 2023 on the Italian Electronic Health Record ("Electronic Health Record 2.0"), establishing a Big Data infrastructure for research and artificial intelligence; and Law No. 132/2025 on artificial intelligence, whose Article 8 addresses scientific research and experimentation in the development of AI systems in the healthcare sector.

Keywords

health data – scientific research – legal bases for data processing – electronic health record 2.0 – artificial intelligence

Tra predizione e protezione dei dati: la pubblica amministrazione algoritmica al vaglio dei rischi e delle garanzie*

Riccardo Merli

Sommario

1. Premessa. - 2. Dalla digitalizzazione amministrativa alla *governance* algoritmica. - 3. Dati personali e nuove architetture informatiche: un'intersezione problematica. - 3.1. Opacità algoritmica e motivazione. - 3.2. Il consenso come base fragile. - 3.3. Responsabilità amministrativa e *accountability* progettuale. - 3.4. Profilazione, *bias* e principio di eguaglianza. - 4. L'art. 22 GDPR: decisioni automatizzate e diritto alla spiegazione. - 5. Conclusioni.

1. Premessa

Viviamo in una fase storica segnata da una rivoluzione informatica sistemica, in cui la Pubblica Amministrazione (PA) ha progressivamente abbandonato la dimensione meramente documentale per rivestire un ruolo strategico nell'adozione e nello sviluppo delle nuove tecnologie[1]. A ben vedere, infatti, la digitalizzazione, inizialmente limitata alla dematerializzazione dei procedimenti e alla costruzione della cittadinanza digitale, si è presto tradotta in forme più sofisticate di automazione e predizione, capaci di incidere in modo diretto sul rapporto tra amministrazione e cittadini[2]. In questo scenario complesso e in continua trasformazione, i giuristi sono

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

1 I. D'Elia Ciampi*, L'informatica e le banche dati*, in S. Cassese (a cura di), *Trattato di diritto amministrativo, Parte Speciale*, Milano, 2003, IV, 1632.

2 Per una ricostruzione sulle fasi della digitalizzazione e sulle principali disposizioni in materia *ex multis* vd. P. Rubechini, *Tecnologia blockchain e fiducia amministrativa*, Napoli, 2023; G. Pesce, *Digital first*, Napoli, 2018.

chiamati a confrontarsi con questioni in larga parte inedite ma ormai indifferibili. Ciò che emerge, infatti, non è un mero problema di modernizzazione tecnica della macchina amministrativa, bensì una sfida che investe principi costituzionali e categorie giuridiche consolidate che sono spinte a verificare la loro adattabilità alla tecnologia.

In altri termini, la progressiva introduzione di sistemi algoritmici[3] non si limita a ridefinire le modalità operative degli uffici ma, sostituendo la logica tradizionale del controllo *ex post* con quella del condizionamento *ex ante*, ha inciso sul terreno della legalità, della trasparenza, della responsabilità e, in special modo, dell'eguaglianza sostanziale nell'accesso ai diritti e alle prestazioni pubbliche[4].

Da questa prospettiva, l'efficienza algoritmica diviene una nuova forma di legittimazione dell'azione pubblica, ma – come si mostrerà nel prosieguo – essa non è neutra[5] né priva di tensioni con i principi costituzionali[6].

A partire da tali riflessioni, il percorso di ricerca che qui si inaugura si snoda lungo tre direttrici complementari che intendono ricostruire un quadro dogmatico unitario del rapporto tra predizione e protezione dei dati.

La prima direttrice riguarda la ricostruzione del mutamento concettuale che ha condotto dall'amministrazione digitale all'amministrazione predittiva, segnando il passaggio da un modello informativo a uno propriamente cognitivo, fondato sull'uso sistematico dei dati a fini decisionali.

La seconda, ragionando sul principio costituzionale di eguaglianza, analizza come *bias*, opacità e processi di profilazione possano tradursi in nuove forme di diseguaglianza sostanziale e, quindi, come la responsabilità amministrativa possa divenire una condizione di giustizia digitale, *id est* quale nuovo assetto di garanzie dell'azione amministrativa algoritmica.

La terza, infine, concerne l'esame delle garanzie previste dal quadro normativo europeo, con particolare attenzione all'art. 22 del Regolamento (UE) 2016/679, anche conosciuto come *General Data Protection Regulation*

[3] Per un inquadramento giuridico degli algoritmi nell'attività amministrativa si veda A. Sola, *Inquadramento giuridico degli algoritmi nell'attività amministrativa*, in *Federalismi.it*, 16, 2020, 332 ss.

[4] Non a caso, la dottrina ha da tempo messo in luce ritardi e disomogeneità, rilevando come l'assenza di standard uniformi dei servizi digitali rischi di compromettere l'eguaglianza sostanziale nell'accesso alle prestazioni pubbliche. Sul punto si veda M. Pietrangelo, *Sui "diritti di cittadinanza digitale". Note a margine di un opaco percorso normativo*, in *Federalismi.it*, 8, 2022, 130 ss.

[5] Tra i molti vd. A. C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, 107 ss.

[6] Tant'è vero che in dottrina, in materia di algoritmi, si è proposta una dottrina della "precauzione costituzionale". Così A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, spec. 86 e 87.

(GDPR)[7], e la loro interazione con gli obblighi di supervisione umana introdotti dal Regolamento (UE) 2024/1689, altresì noto come Regolamento sull'intelligenza artificiale (d'ora in poi, "AI Act"), al fine di verificare limiti e potenzialità nella disciplina delle decisioni automatizzate.
Ciò chiarito, occorre precisare che l'indagine è basata su approccio giuridico-dogmatico, che non ambisce a fornire risposte conclusive in grado di porre la parola "fine". Essa si propone, piuttosto, di offrire una ricostruzione critica volta ad alimentare il dibattito e a verificare se, e in quale misura, sia possibile coniugare innovazione tecnologica e tutela dei diritti fondamentali.

2. Dalla digitalizzazione amministrativa alla *governance* algoritmica

Appare doveroso chiarire che l'evoluzione digitale della PA non può essere ridotta a una sequenza lineare di fasi settoriali. Piuttosto, essa si è venuta a configurare come un processo di trasformazione complessiva che, tanto sul piano dogmatico quanto su quello descrittivo, segna il passaggio da una digitalizzazione debole a una digitalizzazione forte, capace di investire in profondità ogni processo e dimensione dell'agire pubblico[8].
La prima si concentra sull'estetica e sull'organizzazione dell'attività amministrativa, ossia su quell'insieme di interventi che attengono all'esteriorità del procedimento. Ne sono un esempio la dematerializzazione dei documenti e, con essa, l'interazione online con cittadini e imprese tramite moduli elettronici, firme digitali, portali, protocolli informatici e servizi di posta elettronica certificata.
Messi in chiaro questi profili, appare evidente che il passaggio da una PA cartacea a una "paperless"[9] rappresenta certamente un traguardo significativo, che però rimane pur sempre limitato ad una mera trasposizione in formato digitale di procedure e archivi analogici, senza incidere sul nucleo cognitivo dell'agire pubblico. Al contrario, la digitalizzazione forte rappresenta un'autentica ristrutturazione epistemica che ha segnato l'arrivo di un

[7] In relazione al quadro delineato dal GDPR in materia si vd. R. C. Perin-D. U. Galetta, *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, II, 2025, spec. 60 ss.

[8] G. Duni, *Amministrazione digitale*, in *Enciclopedia del diritto*, I, 2007, 17, invece, parla di passaggio da un «momento statico» a un «momento dinamico».

[9] In altri termini, la digitalizzazione implica il venir meno del legame tradizionale con il supporto cartaceo, che resta confinato a un ruolo meramente accessorio rispetto allo svolgimento dell'attività amministrativa. Cfr. G. Duni, *La amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica*, Milano, 2008, 14.

"nuovo paradigma amministrativo"[10].
In questa fase, la tecnologia non si limita più a svolgere un ruolo meramente ausiliario, ma diventa parte integrante e determinante dell'azione amministrativa, fino a incidere sulla sua stessa fisionomia. Ed è all'interno di questa nuova configurazione epistemica che trovano spazio strumenti di analisi avanzata e tecniche di *machine learning*; vale a dire, sistemi che non si limitano a riportare asetticamente la realtà, ma la producono e la orientano, modellando comportamenti e decisioni amministrative secondo logiche probabilistiche.
Sotto questa prospettiva, infatti, parte della dottrina ha parlato di una vera e propria "secessione amministrativa"[11], espressione che ben restituisce l'idea di una progressiva retrocessione del ruolo umano all'interno del procedimento; *scilicet*, il cittadino non è più destinatario del provvedimento ma oggetto di una classificazione probabilistica. Un processo che, come avremo modo di dire, ha reso presto evidente l'esigenza di nuove garanzie.
Per comprendere appieno la portata di tale fenomeno, è necessario chiarire che cosa significhi, in termini tecnici, "predire": elaborare inferenze basate su tecnologie statistiche e algoritmiche, in particolare mediante l'ausilio dell'intelligenza artificiale (IA), capaci di anticipare eventi futuri osservabili direttamente a partire dall'analisi di dati passati o presenti.
A ben vedere, pertanto, contrariamente ai metodi statistici tradizionali, i sistemi cognitivi non si affidano a una sequenza rigida di calcoli deterministici[12], né operano secondo regole predefinite che ne garantiscono la tracciabilità, ma utilizzano logiche più flessibili, talvolta *fuzzy*[13], più adatte a gestire l'incertezza e, proprio per questo, potenzialmente più accurate e stringenti. Esse si fondano, invero, su modelli di apprendimento automatico (appunto, *machine learning*) in grado di evolvere «in maniera proporzionale rispetto al numero di dati che vengono elaborati»[14] e che, processando

[10] G. Carullo, *La nozione di servizi digitali: un nuovo paradigma per la pubblica amministrazione autocertificazione e diritto dell'Unione europea*, in *Istituzioni del federalismo: rivista di studi giuridici e politici*, 2, 2023, 335 ss.

[11] Sul punto cfr. D. Diaco, *Amministrazione umana vs Amministrazione algoritmica: prolegomeni su un modello procedimentale a partecipazione successiva*, in *Judicium. Il processo civile in Italia e in Europa,* 2023.

[12] Francaviglia distingue tra "informatizzazione della P.A.", "elaborazione algoritmica – e dunque automatizzata – del provvedimento amministrativo" e "attività provvedimentale *data-driven*". Nello specifico, gli algoritmi predittivi rientrano principalmente nelle ultime due categorie. Così M. Francaglia, *L'intelligenza artificiale nell'attività amministrativa: principi e garanzie costituzionali nel passaggio dalla regula agendi alla regola algoritmica*, in *Federalismi.it*, 17, 2024, 114 ss.

[13] Per approfondire cfr. M. Veronesi-A. Visioli, *Logica fuzzy. Fondamenti teorici e applicazioni pratiche*, Milano, 2003.

[14] G. Alpa, *Diritto e intelligenza artificiale*, Pisa, 2020, 282.

tali grandi volumi informativi (*big data*[15]), sono in grado di individuare *pattern*, correlazioni e segnali all'interno del "rumore informativo", restituendo, così, un risultato probabilistico deduttivo scarsamente bisognoso di un mero assenso umano.

In buona sostanza, l'*ubi consistam* del sistema automatizzato, a differenza di quello tradizionale, limitato a riportare relazioni osservate nei dati storici, risiede nella sua capacità di applicare inferenze apprese in fase di addestramento a situazioni nuove e non perfettamente coincidenti con quelle già conosciute, dando luogo a un ragionamento probabilistico che, pur non assicurando esiti certi, consente di orientare l'azione amministrativa in scenari complessi e mutevoli, adeguando la risposta alle nuove variabili. Per comprendere appieno il funzionamento di tali strumenti, è forse utile osservare in quali procedimenti essi trovano oggi applicazione concreta nel dominio amministrativo; per esempio, essi vengono impiegati per valutare il rischio di evasione dei contribuenti, per stimare la probabilità di recidiva di un imputato, per il riconoscimento dei soggetti più esposti all'emarginazione sociale e per individuare i destinatari più appropriati di benefici o interventi pubblici.

Questa evoluzione mostra, infatti, come, nel tempo, il passaggio da un modello burocratico e reattivo a un'amministrazione che si configura come organismo cognitivo potenziato, ha di contro affermato un'autentica *governance* del dato[16]. Il dato stesso diviene il perno della vita amministrativa, trasformando le pubbliche amministrazioni in vere e proprie *data-driven organizations*[17], nelle quali gli strumenti per la raccolta, l'elaborazione e la gestione delle informazioni non ricoprono più un ruolo di mero supporto esterno all'*iter* amministrativo, ma tendono a diventare ontologicamente il processo stesso.

Lumeggiate la funzione e il fine di questi strumenti, nel prossimo paragrafo occorrerà constatare come la loro applicazione sollevi rilevanti profili problematici di ordine giuridico e costituzionale, imponendo di soffermarsi sui rischi connessi e sulle diverse forme di regolazione che il legislatore

---

15 *Ex multis* cfr. C. Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, in *Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino*, Torino, 2021.

16 Per un approfondimento sulla *data governance* e sulla sovranità digitale nella PA, cfr. V. Pagnanelli, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista Italiana dell'Informatica e del Diritto*, 1, 2021, 11 ss.

17 Cfr. A. Pentland, *Social Physics: how good ideas spread-the lessons from a new science,* New York, 2014; D. Kiron, *Lessons from becoming a data-driven organization*, in *MIT sloan management review*, 58-2, 2017; P. Korherr-D. K. Kanbach-S. Kraus-P. Mikalef, *From intuitive to data-driven decision-making in digital transformation: A framework of prevalent managerial archetypes*, in *Digital Business*, 2, 2022.

è chiamato ad approntare. La questione, infatti, non è se usare o meno algoritmi, ma a quali condizioni il loro impiego sia compatibile con i principi dell'azione amministrativa e con le tutele del GDPR.

3. Dati personali e nuove architetture informatiche: un'intersezione problematica

Nei paragrafi precedenti abbiamo avuto modo di constatare come all'inizio del XXI secolo si è affermato un fenomeno noto come *datafication*[18], alcuni hanno parlato persino di "datacrazia"[19], ossia la tendenza a trasformare ogni aspetto della realtà in dati quantificabili, capaci di guidare, influenzare o addirittura determinare le decisioni politiche, economiche, amministrative o sociali, spesso attraverso strumenti automatizzati come algoritmi e intelligenza artificiale.
In virtù di ciò, insomma, i dati sono oramai considerati una risorsa strategica a livello globale, tanto da essere spesso descritti come il "nuovo petrolio"[20]. Tuttavia, l'analogia è solo parziale. A differenza delle risorse naturali esauribili, i dati non si consumano, ma possono essere copiati, condivisi, riutilizzati indefinitamente e, persino, venduti (all'uopo, si tornerà più avanti sul caso *Weople*), mantenendo intatto il loro valore d'uso. Ciò che li rende realmente produttivi è, piuttosto, la loro organizzazione e trattamento; *in nuce*, come il greggio deve essere raffinato per diventare carburante, così i dati necessitano di essere raccolti, selezionati, correlati e analizzati.

---

[18] Secondo S. Calzolaio (*Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, 1, 2021, spec. 5) la *datafication* si fonda su tre elementi: la crescita esponenziale della produzione di dati, la capacità delle macchine di analizzarli ed estrarne conoscenza e, infine, l'utilizzo di tali informazioni nei processi decisionali tramite *algorithmic decision making*. Per un ulteriore approfondimento del tema, *ex multis*, si veda K. Cukier-V. Mayer-Schöenberger, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013; C. Sarra*, La datificazione della persona nella costruzione del Metaverso*, in *Journal of Ethics and Legal Technologies*, 6, 2024, 3 ss.

[19] S. Uggeri, *Il potere dei Big Data e la datacrazia della rete*, in *Confronti: mensile di fede, politica, vita quotidiana*, 1, 2018, 29 ss.; D. Gambetta (a cura di), *Datacrazia: Politica, cultura algoritmica e conflitti al tempo dei big data*, Roma, 2018; D. Talia, *Il rischio della Datacrazia nelle Smart Cities*, in G. F. Ferrari (a cura di), *Innovazione e sostenibilità per il futuro delle smart cities*, Milano, 2023, 793 ss.

[20] B. Ando, *Dati personali tra Costituzione e mercato: una prospettiva di diritto comparato*, in M. Mazzuca-M. Mauro (a cura di), *Sulle interrelazioni tra settori del sistema giuridico. Esperienze interdisciplinari*, Napoli, 2024, 61 ss.; V. Montozzi, *Le nuove sfide della regolazione dei dati: analisi di un modello a partire dall'intersezione tra protezione dei dati personali e concorrenza*, in *Rivista italiana di informatica e diritto*, 1, 2025, 501 ss.

In questa prospettiva, l'intelligenza artificiale, come già spiegato, svolge un ruolo decisivo, consentendo l'elaborazione di inferenze e previsioni che superano i limiti cognitivi dell'uomo. E, tuttavia, ridurre l'uso degli algoritmi a una dimensione salvifica significherebbe trascurarne le criticità e i rischi strutturali.

È indubbio, infatti, che la credibilità complessiva della ricostruzione qui delineata resta condizionata dal riconoscimento che l'algoritmo, allo stato attuale, non è in alcun modo qualificabile come un operatore o, peggio, come un giudice infallibile, bensì come un mero moltiplicatore di capacità classificatoria e predittive già presenti nei dati. Esso, invero, non sostituisce la razionalità umana, ma la moltiplica, offrendosi come strumento di elaborazione capace di ridurre i tempi procedimentali, favorire l'uniformità di trattamento, rendere misurabili le *performance* e tracciabili gli esiti. Eppure, è proprio in questo processo che si coglie la portata innovativa dei modelli computazionali, la cui attrattiva rimane innegabile.

Si badi. Il disquisito ecosistema digitale, pur tra le sue ambivalenze – che, per certi versi, richiama il chiaroscuro caravaggesco, ove la luce e l'ombra convivono in una tensione drammatica volta a guidare lo sguardo sui nuclei essenziali della scena –, non deve indurre in confusione. È doveroso, infatti, tener presente che la complessità del fenomeno, nella sua effettiva portata, impone al presente saggio un'alternanza di considerazioni di segno positivo e negativo, in un equilibrio instabile in cui non è agevole determinare l'inclinazione del piatto della bilancia.

In buona sostanza, se sul piano generale l'innovazione apre scenari di straordinaria portata, sul piano più concreto emergono con forza le problematiche connesse al rapporto tra dati personali e nuove architetture informatiche[21].

È noto, infatti, come anche la cronaca più recente abbia mostrato gli enormi rischi che si accompagnano alla centralità dei dati. Per fare qualche esempio, nel 2024 la Direzione Distrettuale Antimafia di Milano ha portato alla luce una rete di spionaggio informatico che, mediante accessi abusivi a banche dati pubbliche e private, metteva in commercio informazioni riservate di centinaia di migliaia di cittadini e imprese[22]. Pochi mesi più tardi, un'indagine parallela a Bari ha rivelato analoghe pratiche di intrusione sistematica ai danni dei correntisti da parte di un ex dipendente bancario,

[21] Sui profili di incompatibilità delle tecniche di polizia predittiva con la tutela di *privacy* e dati personali vd. A. Bonfanti, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Media Laws Rivista di diritto dei media*, 3, 2018, 1 ss.

[22] L'inchiesta milanese ha coinvolto la società investigativa *Equalize*, guidata dall'*ex* capo della Polizia Carmine Gallo, accusata di aver creato un vero e proprio mercato nero dei dati, attingendo abusivamente da banche dati come SDI, Serpico, INPS, ANPR e SIVA. Tra i clienti figuravano grandi imprese italiane ed estere, che pagavano somme tra i 1.000 e i 15.000 euro per l'ottenimento di informazioni riservate.

tra i quali figuravano anche esponenti delle massime istituzioni[23]. Questi episodi mettono in evidenza non solo l'esistenza di un vero e proprio mercato nero dei dati, ma soprattutto le carenze strutturali dei sistemi di protezione, con i rischi di furto, di alterazione e/o di distruzione dei dati (*computer crimes*[24]), nonché l'urgenza di una riforma normativa e tecnica[25].
Le questioni sin qui evidenziate consentono di delineare un primo quadro delle criticità connesse alla gestione del dato nell'attuale scenario digitale. Tuttavia, ulteriori problematiche si manifestano con particolare intensità in presenza delle nuove architetture informatiche – quali i *data lake*, i servizi in *cloud* e i sistemi di integrazione di banche dati eterogenee – che trovano nell'impiego dell'intelligenza artificiale a fini predittivi il loro principale punto di forza, ma al tempo stesso la loro area di maggiore vulnerabilità.
Le pagine che seguono approfondiscono i principali nodi critici dell'amministrazione algoritmica, esplorando i rischi derivanti dall'opacità dei modelli e dall'*automation bias*, le fragilità del consenso informato e della correlata questione del *consent bias*, le implicazioni culturali e organizzative, le ambiguità nelle responsabilità di trattamento e, infine, il tema centrale della profilazione.

3.1. Opacità algoritmica e motivazione

Con il diffondersi delle banche dati[26] e i primi scambi di informazioni tra archivi diversi – sovente in assenza di un quadro giuridico adeguato, circostanza che conferma il consueto ritardo del diritto rispetto al progresso tecnologico[27] – emerse con forza la richiesta di trasparenza e chiarezza nei trattamenti informativi. Gli interessati volevano sapere come sarebbero stati trattati i loro dati, accedervi e correggerli; in altre parole, nacque così

[23] L'indagine condotta a Bari ha accertato quasi 7.000 accessi non autorizzati da parte di un *ex* dipendente di Intesa Sanpaolo, con dati relativi a circa 3.500 clienti. Tra i soggetti spiati figuravano anche autorità politiche di vertice, come Giorgia Meloni e Ignazio La Russa, oltre a membri della magistratura e delle forze armate.

[24] Per una ricostruzione più puntuale cfr. M.G. Losano, *Scritti di informatica e diritto. Per una storia dell'informatica giuridica*, Milano, 2022, vol. 1.

[25] Sul tema della *cybersicurezza* nello specifico, vd. A. Contaldo-D. Mula (a cura di), *Cybersecurity law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020; S. Busetti-F. M. Scanni, *Pericoli Cyber. Un'analisi dei processi di istituzionalizzazione e di Policy Making della cybersicurezza nazionale*, in S. Busetti-A. Noto-R. Romani (a cura di), *Essere Digitali. Le scienze della politica allo studio dell'ultima rivoluzione*, Teramo, 2023, 67 ss.

[26] Cfr. R. Ridi, *Il mondo dei documenti: cosa sono, come valutarli e organizzarli*, Bari, 2014.

[27] E. D'Orlando, *Politica, tecnica e scienza: il sistema delle fonti difronte al dilemma della complessità*, in *Diritto amministrativo*, 4, 2021, spec. 723.

la rivendicazione di un vero e proprio «diritto alla buona amministrazione informatizzata»[28].
D'altronde, in un sistema giuridico fondato sul principio di legalità, la trasparenza dell'azione amministrativa non costituisce soltanto un valore etico, ma una condizione di validità e di legittimità del potere esercitato. L'amministrazione, infatti, è vincolata a fornire motivazioni comprensibili e verificabili, in modo che il cittadino possa esercitare il diritto di difesa e il giudice possa svolgere un controllo effettivo sulla correttezza del procedimento.
L'avvento delle decisioni algoritmiche ha tuttavia introdotto un elemento di radicale discontinuità. Nello specifico, l'opacità del processo decisionale automatizzato – che può derivare da una segretezza intenzionale da parte dei soggetti pubblici o privati che sviluppano o utilizzano gli algoritmi (*intentional corporate or state secrecy*), da una diffusa incompetenza tecnica o asimmetria informativa (*technical illiteracy*) oppure dalla complessità intrinseca dei sistemi di apprendimento automatico, che operano su scala e con modalità non pienamente intellegibili nemmeno ai loro creatori (*the way algorithms operate at the scale of application*)[29] – incrina la logica stessa della legalità amministrativa. Essa spezza, infatti, il nesso di imputazione tra decisione e decisore:

«[…] e ciò in quanto la correlazione tra dati che vale ad estrarre la "regola" su cui la decisione si fonda viene sviluppata dalla macchina, senza quindi che tale correlazione possa essere comprensibile o nota, nemmeno a chi l'algoritmo ha creato mediante la programmazione del relativo *software*»[30].

La questione, peraltro, diviene ancora più articolata se si considera la barriera aggiuntiva a questo oscurantismo che si presenta sotto forma di protezione della proprietà intellettuale, usata per giustificare la segretezza del codice sorgente o dei tipi di modelli matematici impiegati. Tale protezione, pur legittima sul piano economico, finisce per ostacolare ogni forma di ispezione, *audit* o controllo da parte degli *stakeholder* o delle autorità di regolamentazione, favorendo la creazione di quelle «*black boxes that even experts struggle to interpret, giving rise to an urgent need for transparency and interpretability to ensure accountability and trust*»[31]. Proprio per questo, la responsabilità del

[28] Cfr. R. C. Perin-D. U. Galetta, *Il Diritto*, cit., 77 ss.

[29] Così J. Burrel, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in *Big data & society*, 3, 2016, spec. 3, 4 e 5.

[30] G. F. Licata, *Intelligenza artificiale e contratti pubblici: problemi e prospettive*, in *CERIDAP Rivista Interdisciplinare sul diritto delle Amministrazioni Pubbliche*, 2, 2024, 30 ss.

[31] A. Adadi-M. Berrada, *Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)*, in *IEEE Access*, 6, 2018, spec. 52139. Sull'idea della *black box*, quale

decisore si estende anche alle fasi di *procurement* e di *outsourcing* tecnologico, imponendo una diligenza rafforzata nella selezione dei fornitori e nella definizione dei contratti di servizio. In tali contratti dovrebbero essere previste clausole di cooperazione, *audit* e accesso al codice o ai *log* decisionali, in coerenza con l'art. 30 del d.lgs. 36/2023 e con l'art. 14 dell'AI Act.

Ora, è doveroso riconoscere che la giurisprudenza europea e italiana conoscono bene i rischi derivanti dalla disquisita opacità.

La Corte distrettuale dell'Aia, nel caso *SyRI* (acronimo di *System Risk Indication*, il sistema algoritmico oggetto di causa), ha invalidato un sistema di sorveglianza predittiva proprio perché l'opacità sui dati e sulle regole di combinazione impediva un controllo effettivo e creava un rischio sproporzionato per i diritti. Sul versante interno, il Consiglio di Stato (sez. VI, 8 aprile 2019, n. 2270) in relazione all'assegnazione del personale scolastico e dei tirocinanti, ha chiarito che segreti industriali o vincoli contrattuali non possono precludere la conoscibilità dei criteri che incidono su posizioni soggettive. Analogo principio è stato ribadito in Francia nel caso *Parcoursup*, la piattaforma digitale utilizzata per gestire le candidature post-diploma: il *Conseil d'État* (12 giugno 2020, n. 418142) [32] ha affermato la necessità di rendere conoscibili i criteri di calcolo in nome dell'eguaglianza e della verificabilità amministrativa.

Pertanto, quando la decisione pubblica si appoggia a un punteggio o a una classificazione non intelligibile, la motivazione rischia di scivolare in una sorta di circolarità tautologica, riducendosi a formule del tipo "il modello ha restituito uno score di 0,78"[33] e "così è deciso" [34], che la rendono, in

metafora dell'opacità algoritmica, vd. F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, 2015.

[32] Sul punto cfr. L. Frouillou, *Parcoursup: quelles sélections à l'entrée dans le supérieur?*. In *Sélections, du système éducatif au marché du travail: 26 es Journées du Longitudinal. Céreq*, 2020, spec. 44-48

[33] I modelli di machine learning producono risultati espressi in termini di punteggi o probabilità, che rappresentano il grado di rischio o di appartenenza di un soggetto a una determinata categoria (ad esempio "alto rischio" o "potenziale recidiva"). Tuttavia, se tali score non sono accompagnati da una spiegazione dei criteri e delle variabili che li hanno generati, si riducono a meri enunciati tecnici, incapaci di assolvere alla funzione motivazionale che, nel diritto amministrativo, costituisce presidio imprescindibile di legalità e trasparenza. Sul punto, con particolare riguardo alle implicazioni in tema di trasparenza algoritmica e diritto alla spiegazione, tra gli altri, cfr. S. Wachter-B. Mittelstadt-C. Russell, *Counterfactual explanations without opening the black box: Automated decisions and the GDPR*, in *Harvard Journal of Law & Technology*, vol. 21, 2018, 841 ss.; J. Morley-A. Elhalal-F. Garcia-L. Kinsey-J. Mökander-L. Floridi, *Ethics as a service: a pragmatic operationalisation of AI ethics*, in *Minds and Machines*, 31, 2021, 239 ss.; J. Fehr-B. Citro-R. Malpani-C. Lippert-V. I. Madai, *A trustworthy AI reality-check: the lack of transparency of artificial intelligence products in healthcare*, in *Frontiers in Digital Health*, 2024, 1 ss.

[34] Sulla crescente delega delle decisioni ai sistemi automatizzati cfr. F. Marasà, *Intelligenza*

definitiva, «*not justifiable or legitimate*»[35].
Si tratta di una tautologia che riflette, come è stato osservato, la pretesa del mondo digitale di «essere letteralmente tautologico», in cui «nulla può avvenire che trascenda l'immanenza dell'informazione» e in cui «la legge algoritmica, la computabilità – per usare le parole di Fredkin – diventano la legge del tutto»[36]. In un simile scenario, la decisione automatizzata finisce per svuotare di significato quella "riserva di umanità"[37] a cui il sistema dovrebbe tendere attraverso il controllo del cittadino e del giudice. Tale svuotamento trova la sua espressione più evidente in quello che la letteratura definisce *automation bias*[38].
Addentrandoci su questa via, appare opportuno evidenziare che il cuore del problema rimane pur sempre il rapporto tra automazione e supervisione umana. In altri termini, se la retorica ufficiale insiste nel presentare l'algoritmo come un mero strumento di supporto al decisore, la prassi mostra spesso una realtà diversa: l'operatore tende a conformarsi all'*output* della macchina, specie quando manchi il tempo per un'istruttoria approfondita o quando l'autorevolezza tecnica del modello sembri incontestabile. In tali circostanze, la supervisione umana rischia di ridursi a una mera ratifica passiva[39], svuotando di significato i principi di legalità, motivazione e responsabilità.
Qui si colloca il nodo critico. La presenza dell'elemento umano non basta a neutralizzare l'effetto vincolante dello *score* o della classificazione derivante dalla sua apparente neutralità e precisione. Ne deriva una progressiva delegittimazione della funzione umana, la quale rischia di ridursi – se si consente la metafora – a un ruolo meramente protocollare, privo della capacità di incidere realmente sull'esito del procedimento.
L'*automation bias* non costituisce, dunque, un incidente marginale, bensì una conseguenza sistemica dell'automazione decisionale, che si alimenta

artificiale e tutela dei dati personali. Quali riflessi sulla giustizia predittiva?, in *Osservatorio del diritto civile e commerciale*, 1, 2023, 73 ss.

[35] A. Barredo Arrieta-N. Díaz-Rodríguez-J. Del Ser-A. Bennetot-S. Tabik-A. Barbado-S. Garcia-S. Gil-Lopez-D. Molina-R. Benjamins-R. Chatila-F. Herrera, *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI*, in *Information Fusion*, 58, 2020, spec. 83.

[36] G. De Ruvo, *Dio, l'evento e l'algoritmo: il tradimento di Leibniz nell'ontologia digitale e l'etica dell'istante*, in *Segni e Comprensione XXXVI*, 103, 2022, spec. 96.

[37] G. Gallone*, Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Milano, 2023.

[38] Il concetto è ampiamente studiato nelle scienze cognitive e nell'informatica applicata. Cfr. M. L. Cummings, *Automation bias in intelligent time critical decision support systems*, in D. Harris-W-C. Li (a cura di), *Decision making in aviation. Routledge*, 2017, 289 ss.

[39] B. Green*, The flaws of policies requiring human oversight of government algorithms*, in *Computer Law & Security Review*, 45, 2022, 1 ss.

di un duplice paradosso: da un lato, l'illusione di oggettività e neutralità dell'algoritmo che genera una fiducia acritica sulla sua presunta affidabilità; dall'altro, la riduzione della discrezionalità umana a funzione accessoria, incapace di ristabilire pienamente le garanzie di motivazione, proporzionalità e responsabilità proprie del diritto amministrativo.

Un ulteriore livello di opacità si manifesta, ancor prima che nei risultati dell'elaborazione algoritmica, nella fase di selezione e accumulo dei dati. L'esigenza di sviluppare modelli sempre più performanti alimenta infatti una raccolta massiva e spesso indiscriminata di informazioni[40], priva di un effettivo riscontro circa la loro pertinenza o necessarietà rispetto alle finalità del trattamento[41]. A ciò si aggiunge la tendenza a conservarle oltre il tempo strettamente necessario, nella prospettiva di riusi futuri, come l'addestramento di nuovi modelli predittivi. Ne deriva un circolo vizioso: l'espansione continua della base informativa, lungi dal migliorare la qualità dei risultati, finisce per amplificare le distorsioni già presenti e per rendere sempre più opaco il rapporto tra la finalità dichiarata e l'uso effettivo dei dati, compromettendo i principi di minimizzazione e di limitazione della conservazione e svuotando di significato il principio di finalità.

Questa dinamica mostra come la poca trasparenza algoritmica non si esaurisca nel momento decisionale, ma affondi le proprie radici nella costruzione stessa del sapere amministrativo. Ciò che diventa oscuro non è solo il risultato, ma il modo in cui si decide che cosa misurare, raccogliere e conservare. In tal senso, l'opacità è strutturale, riguarda il processo con cui la realtà viene tradotta in dati e trasformata in informazione utile al potere decisionale.

Essa solleva interrogativi profondi sulla compatibilità tra la logica dell'accumulo informativo e i principi di libertà e di autogoverno che fondano la democrazia. L'uso pervasivo dei sistemi di intelligenza artificiale rischia infatti di alimentare una democrazia predittiva, nella quale la partecipazione dei cittadini si riduce a una produzione costante di dati destinati ad alimentare modelli matematici e meccanismi di sorveglianza automatizzata[42].

In tale scenario, il richiamo del GDPR ai diritti fondamentali – dal diritto alla protezione dei dati sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea alla dignità intrinseca della persona (art. 1

---

[40] Cfr. European Union Angency for Fundamental Rights, *Data quality and artificial intelligence - mitigating bias and error to protect fundamental rights*, FRA Focus, in *fra.europa.eu*, 2019.

[41] Sul rapporto tra liceità e clausola di necessità cfr. B. Ponti, *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, Milano, 2023, spec. 31 ss.

[42] L.G. Sciannella, *Intelligenza artificiale, politica e democrazia: Artificial Intelligence, Politics and Democracy*, in *Diritto Pubblico Comparato ed Europeo online*, 1, 2022, spec. 337.

GDPR) – non appare più sufficiente. La sola tutela formale della riservatezza, infatti, non basta a fronte di rischi più sottili ma altrettanto invasivi, come la distorsione dell'identità personale e l'ampliamento progressivo della nozione stessa di dato personale, che assume un carattere dinamico e tendenzialmente onnicomprensivo[43].

In questa prospettiva, la trasparenza e la spiegabilità dei modelli non appaiono più come mere esigenze tecniche, ma come condizioni essenziali per preservare l'*accountability* e la fiducia pubblica nel processo decisionale automatizzato.

Certo, fondare la soluzione del problema su questi principi generale potrebbe rilevarsi insufficiente. Non può, infatti, essere trascurata anche la dimensione culturale del problema. L'amministrazione predittiva richiede nuove competenze non soltanto tecniche, ma anche analitiche e valutative. È necessaria, pertanto, un'adeguata alfabetizzazione ai dati da parte dei funzionari pubblici, una crescente capacità di leggere indicatori e risultati senza assumerli come verità oggettive, nonché una piena consapevolezza dei rischi di *bias*, *overfitting*, *drift* e *fairness*. Senza questo salto intellettivo, la promessa di un effettivo *human in the loop*[44] rimane nominale, e la retorica dell'innovazione rischia di prevalere sulla reale capacità di vigilanza.

L'analisi sin qui condotta mostra come l'opacità algoritmica non incida soltanto sul come si decide, ma anche sul modo in cui le decisioni vengono percepite e accettate da chi ne è destinatario. La medesima logica di deresponsabilizzazione che condiziona il decisore si riflette, infatti, sull'interessato, erodendo la consapevolezza e la libertà del consenso. L'automazione non altera solo il processo decisionale interno all'amministrazione, ma anche il modo in cui il cittadino "acconsente" ai trattamenti che lo riguardano, spesso senza comprenderne la portata né le implicazioni pratiche.

Diventa allora necessario interrogarsi sul valore effettivo del consenso nell'era predittiva: se esso rappresenti ancora uno strumento di autode-

---

[43] In dottrina si è evidenziato come la distinzione tra dato personale e dato non personale stia progressivamente perdendo chiarezza, poiché le pratiche di *data mining* e di profilazione rendono difficile, se non impossibile, una separazione netta tra le due categorie. La commistione di elementi identificativi e non identificativi nei *dataset* eterogenei e dinamici conduce, di fatto, a un'erosione della tradizionale dicotomia. Sul punto, vd. S. Torregiani, *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in *Rivista italiana di informatica e diritto*, 1, 2021, spec. 48 ss.; C. Bergonzini, *"Prova a prendermi". Ecosistema digitale e consapevolezza degli utenti: uno spazio per la regolazione nazionale*?, in G. Di Cosimo (a cura di), *Processi democratici e tecnologie digitali*, Torino, 2023, spec. 97. La sfumata (*blurred*) distinzione tra dati personali e non personali è stata constata anche da parte dell'European Parliamentary Research Service (EPRS), così M. D. M. Negreiro Achiaga, *Free flow of non-personal data in the European Union*, in *Briefing, EU Legislation in Progress*, 2019, 10.

[44] D. Martire, *Human in the loop. L'essere umano come fattore condizionante della–o condizionato dalla–intelligenza artificiale*, in *Rivista italiana di informatica e diritto*, 2, 2024, 1 ss.

terminazione o se, al contrario, stia divenendo una mera formalità, priva di reale capacità di controllo. A questo tema sarà dedicato il paragrafo successivo.

3.2. Il consenso come base fragile

Non meno problematico è il riflesso che la mancanza di trasparenza esercita sulla nozione di consenso informato, in particolare quando il trattamento dei dati avviene su base consensuale. In questo contesto, il diritto alla protezione dei dati personali non può essere più considerato solo una garanzia della riservatezza individuale, ma si configura come presidio fondamentale all'effettivo esercizio delle libertà nel contesto digitale[45]. Eppure, nemmeno il consenso del cittadino rappresenta una garanzia effettiva. La lettera del GDPR, infatti, consente il trattamento automatizzato fondato sul consenso esplicito dell'interessato (art. 22, par. 2, lett. c*)*), ma, anche quando tale consenso viene formalmente richiesto, non può qualificarsi come realmente libero e informato. Nessun utente è in grado di comprendere *ex ante* quali combinazioni di dati alimentino i modelli, quali riusi futuri siano possibili e quali conseguenze pratiche possano derivarne.
Ne consegue che, nei sistemi predittivi, la nozione stessa di consenso rischia di ridursi a una mera finzione giuridica, scarsamente utile alla protezione sostanziale della persona e, anzi, idonea a ostacolare una corretta allocazione della responsabilità in capo al titolare del trattamento.
Insomma, in questo senso, si può affermare che il consenso, pur formalmente acquisito, risulta sostanzialmente viziato da asimmetria informativa e asimmetria cognitiva: la volontà si forma su presupposti ignoti e l'autodeterminazione si svuota di contenuto. Com'è stato osservato:

«rimane oscuro come e a quali condizioni il funzionario umano possa legittimamente discostarsi dalle risultanze istruttorie algoritmiche, e come viceversa debba attivarsi per rilevare condotte atipiche e diverse o introdurre elementi di valutazione ulteriori che possono capovolgere il contenuto stesso della decisione finale»[46].

Sul piano dogmatico, ciò comporta un duplice rischio. Da un lato, l'amministrazione non è più in grado di valutare in modo trasparente se il

[45] S. De Luca, *Big Data, libertà e democrazia: tra utopia e distopia*, in S. Busetti-A. Noto-R. Romani (a cura di), *Essere Digitali*, cit., 27 ss.

[46] G. Avanzini*, Intelligenza artificiale, machine learning e istruttoria procedimentale: vantaggi, limiti ed esigenze di una specifica data governance*, in *Intelligenza artificiale e diritto: una rivoluzione?*, in *Quaderni ASTRID*, vol. 2, Bologna, 2022, spec. 92.

mezzo sia necessario e idoneo rispetto al fine, alterando così il principio di proporzionalità del trattamento. Dall'altro, la nozione di consenso come fondamento di liceità si svuota di significato, riducendosi a mera formalità priva di una effettiva capacità di garanzia. Ne risulta un meccanismo che deresponsabilizza la pubblica amministrazione più che garantire l'autodeterminazione individuale. La libertà del consenso evapora nella complessità epistemica del sistema.

A ben vedere, la problematica non è nuova ma ripropone, in chiave digitale, il tema classico dell'eterodeterminazione della volontà. Tuttavia, nel contesto algoritmico, l'eterodeterminazione non deriva più da un condizionamento esterno, bensì da una struttura epistemica opaca che confina il cittadino in una posizione di inconsapevolezza strutturale. La decisione amministrativa perde così il suo carattere dialogico[47], trasformandosi in un'interazione unidirezionale in cui la macchina determina i confini della partecipazione e della conoscenza.

Le criticità del consenso non si limitano però al piano soggettivo, ma si riflettono anche su quello sistemico.

Il cosiddetto *consent bias* – che si manifesta quando le analisi si basano solo sui soggetti che hanno prestato consenso al trattamento – introduce distorsioni che compromettono la rappresentatività dei campioni, generando discriminazioni di fatto. Tale rischio è particolarmente evidente in settori sensibili, come la sanità o la ricerca biomedica, dove motivi etici o personali riducono la disponibilità a condividere dati. In tali casi, quindi, il rispetto formale dell'autodeterminazione informativa può tradursi in risultati fuorvianti e potenzialmente iniqui.

Inoltre, il caso dell'applicazione *Weople*, che proponeva un modello di "economia dei dati" in cui gli utenti cedono informazioni personali in cambio di una remunerazione, mostra ulteriori limiti[48]. Il Garante per la protezione dei dati personali, già nel 2019, segnalò al Comitato europeo per la protezione dei dati (d'ora in avanti, EDPB) i rischi di tale pratica: da un lato, possibili duplicazioni e violazioni dei principi di integrità e minimizzazione; dall'altro, la trasformazione del consenso in merce negoziabile, in contrasto con la sua natura di atto libero e informato ai sensi dell'art. 7 GDPR. La stessa Autorità ha poi richiamato l'esigenza di vigilare sulla legittimità delle richieste di portabilità dei dati (art. 20 GDPR), sottolineando che solo i dati "forniti" dall'interessato e trattati con mezzi automatizzati possono essere trasferiti, non quelli derivati o inferiti[49].

---

[47] In dottrina si parla di "diritto all'interazione digitale" tra pubblica amministrazione e cittadini: cfr. E. Belisario, *La "nuova" Pubblica Amministrazione digitale*, Rimini, 2009.

[48] Sul caso *Weople*, cfr. F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 1, 2021, spec. 216-221.

[49] Art. 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for*

In definitiva, il consenso, lungi dal rappresentare una garanzia di libertà, si rivela oggi una base fragile. Esso appare sempre più come uno strumento formale, piuttosto che sostanziale, e finisce per operare più come meccanismo di deresponsabilizzazione che come effettiva tutela dell'interessato. La crisi del consenso, resa particolarmente evidente dall'opacità algoritmica, impone dunque di ripensare le modalità di legittimazione dei trattamenti automatizzati e di rafforzare i meccanismi di imputazione della responsabilità.
Questa fragilità non costituisce soltanto il sintomo di una crisi della libertà informativa. Essa rappresenta, più in profondità, il preludio a una crisi della responsabilità. Quando l'autodeterminazione dell'interessato risulta compromessa dall'opacità dei processi decisionali automatizzati, anche l'imputazione delle decisioni e dei loro effetti diventa incerta.
In tale prospettiva, il tema della responsabilità amministrativa emerge come il naturale sviluppo della riflessione, ponendo l'interrogativo su come attribuire, nel contesto automatizzato, la titolarità del potere e la conseguente rendicontabilità dell'azione pubblica.

3.3. Responsabilità amministrativa e *accountability* progettuale

La crisi del consenso come strumento di legittimazione dei trattamenti automatizzati, come appena anticipato, apre inevitabilmente la questione della responsabilità amministrativa. D'altra parte, se il cittadino non è più in grado di comprendere i processi decisionali fondati su algoritmi opachi, il problema non è solo garantire l'autodeterminazione informativa, ma assicurare che l'esercizio del potere resti imputabile e controllabile. In altri termini, la fragilità del consenso si traduce in una fragilità della responsabilità: là dove viene meno la comprensibilità della decisione, si affievolisce anche la possibilità di individuare chi debba risponderne.
È in questo passaggio che il tema dell'*accountability* si intreccia con quello della responsabilità amministrativa. Entrambi esprimono, seppur su piani differenti, l'esigenza che il potere resti tracciabile e giustificabile: l'*accountability* sul versante organizzativo e tecnico, la responsabilità su quello giuridico e personale. In questa prospettiva, il GDPR offre una prima traduzione normativa del principio, imponendo al titolare del trattamento di dimostrare la conformità delle operazioni ai criteri di liceità, correttezza e trasparenza. Tale obbligo, tuttavia, non esaurisce la questione sul piano sostanziale; non basta che il procedimento rispetti formalmente le prescri-

the purposes of Regulation 2016/679, adopted on 3 October 2017, revised on 6 February 2018, 19.

zioni regolamentari, è necessario che sia anche comprensibile, motivato e controllabile nella sua logica decisionale.

In questa prospettiva, nel contesto amministrativo, l'*accountability* si lega con il principio costituzionale di buon andamento (art. 97 Cost.) e con l'obbligo di motivazione, assumendo un significato più denso rispetto a quello meramente regolatorio. Essa diventa la misura della trasparenza del potere pubblico e della sua capacità di rendere conto delle scelte algoritmiche adottate.

Ciò posto, se la decisione è il frutto di un processo algoritmico non spiegabile, l'amministrazione si trova in una condizione di irresponsabilità strutturale, poiché non è più in grado di ricostruire la catena causale che conduce dall'*input* al risultato. In questa situazione, il potere pubblico rischia di trasformarsi in un potere "anonimo", in cui la decisione appare come un fatto tecnico piuttosto che come un atto imputabile. L'effetto, in termini di garanzie, è dirompente giacché si dissolve la possibilità stessa di individuare il responsabile, di motivare la decisione e di consentire al cittadino di contestarla efficacemente.

Da qui nasce l'esigenza di ripensare la responsabilità amministrativa nell'era della predizione: essa non può più limitarsi al piano soggettivo, ma deve essere ricostruita come responsabilità progettuale (o multilivello), che abbraccia l'intero ciclo di vita dell'algoritmo: dalla progettazione all'addestramento, fino all'utilizzo operativo. Non si tratta più soltanto di reagire a un danno *ex post*, ma di garantire, *ex ante*, che la tecnologia sia progettata e utilizzata secondo criteri di affidabilità, trasparenza e proporzionalità. Pertanto, essa coinvolge non solo i funzionari pubblici, ma anche i fornitori, le stazioni appaltanti e i soggetti esterni, secondo logiche di prevenzione e di governance ispirate all'art. 30 del d.lgs. 36/2023 e al modello di supervisione previsto dall'AI Act (art. 14)[50].

La logica sottostante è quella del principio di continuità della responsabilità, radicato nell'art. 28 Cost., secondo cui il potere decisionale, anche quando mediato da strumenti tecnologici, non può mai essere disgiunto dall'obbligo di comprensione, motivazione e controllo. Ne consegue che, anche in presenza di un sistema algoritmico, il funzionario è tenuto a rispondere delle conseguenze derivanti dall'uso di strumenti di cui non comprende pienamente il funzionamento, a meno che non abbia dimostrato di aver adottato tutte le misure necessarie per verificarne l'affidabilità e la correttezza.

L'uso di algoritmi predittivi non può essere considerato una delega neutra di funzioni tecniche; esso comporta, invece, l'assunzione di una responsabilità complessa, che si estende alla scelta, alla configurazione e alla va-

[50] Cfr. M. Barberio, *L'uso dell'intelligenza artificiale nell'art. 30 del d.lgs. 36/2023 alla prova dell'AI Act dell'Unione europea*, in *Rivista italiana di informatica e diritto*, 2, 2023, 253 ss.

lidazione del modello impiegato. In questa prospettiva, la responsabilità del decisore pubblico assume una dimensione *ex ante*, di prevenzione e controllo, e non più soltanto ex post, di sanzione o riparazione del danno. L'applicazione coerente di tale principio esige che l'amministrazione dimostri non solo di aver effettuato una corretta valutazione d'impatto sulla protezione dei dati (DPIA, ne riparleremo più avanti), ma anche di aver predisposto procedure interne di *audit* e supervisione. L'assenza di tali strumenti può integrare un vizio di *culpa in vigilando* o di *culpa in eligendo*, configurando una responsabilità amministrativa diretta in caso di danno ingiusto derivante dall'uso improprio del modello.

Sul versante europeo, la giurisprudenza della Corte di giustizia ha contribuito a definire questa esigenza di controllo effettivo. Nella causa *H.K. v. Prokuratuur* (C-746/18, 2021), la Corte ha stabilito che l'accesso ai dati di traffico e di localizzazione incide gravemente sui diritti fondamentali e può essere autorizzato solo previa verifica preventiva da parte di un giudice o di un'autorità indipendente e imparziale[51]. Sebbene la pronuncia maturi in ambito penale, la ratio del controllo effettivo (e non meramente simbolico) è estensibile anche al procedimento amministrativo automatizzato, in virtù del principio comune di proporzionalità e di effettiva tutela giurisdizionale.

L'AI Act recepisce questa impostazione introducendo un obbligo generale di supervisione umana effettiva per i sistemi di intelligenza artificiale ad alto rischio (art. 14). Tali sistemi devono essere progettati per consentire agli operatori di comprendere limiti e capacità del modello e restare consapevoli della sua influenza sul processo decisionale. La responsabilità si sposta così dal livello meramente giuridico a quello organizzativo e tecnico, imponendo la creazione di filtri istituzionali che assicurino tracciabilità e revisione delle decisioni automatizzate.

Quanto detto ci impone una riflessione sul significato della colpa algoritmica. Essa non coincide con l'errore del codice, ma con la mancata vigilanza, previsione o comprensione delle implicazioni derivanti dal suo uso. L'algoritmo, come strumento di esercizio del potere, non è mai un soggetto autonomo, bensì un mezzo; sicché, la sua imprevedibilità non elimina la colpa, ma la trasforma in colpa per difetto di vigilanza.

In questo senso, la responsabilità del decisore algoritmico si colloca tra la responsabilità da atto e la responsabilità da organizzazione, poiché ciò che

[51] Sul punto vd. I. Revolidis, *HK v Prokuratuur: On Balancing Crime Investigation and Data Protection*, in *European Data Protection Law Review*, 6, 2020, 319 ss.; S. Rovelli, *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers-A Journal on Law and Integration*, 1, 2021, 199 ss.; G. Formici, *La sentenza HK c. Prokuratuur e il difficile dialogo tra CGUE e Stati membri in materia di conservazione e accesso ai metadati per finalità securitarie: spunti di riflessione su una questione vecchia ma ancora irrisolta*, in *Quaderni di SIDIblog*, Napoli, 2021, 231 ss.

viene meno non è soltanto la correttezza dell'atto singolo, ma la capacità del sistema amministrativo di garantire un esercizio del potere conforme a diritto. Si direbbe che la vera sfida non sia adattare l'algoritmo al diritto, ma adattare il diritto a controllare l'algoritmo, nel solco della dottrina che propone di reinterpretare la legalità in chiave di "technological due process"[52].
Si comprende allora la necessità di ricercare un nuovo equilibrio tra fiducia tecnica e controllo giuridico: la sfida, in altri termini, consiste nel ricondurre la discrezionalità algoritmica entro i confini della discrezionalità amministrativa. L'amministrazione, infatti, non può limitarsi a utilizzare modelli predittivi: deve comprenderli, valutarli e saperne rendere conto. D'altronde, sembrerebbe essere lo stesso obiettivo del GDPR quello di «anteporre l'uomo alla macchina algoritmica, o se si vuole, porre la macchina in modalità servente all'uomo»[53], obiettivo che, tuttavia, resta in larga parte disatteso.
La riflessione sulla responsabilità amministrativa e sull'*accountability* progettuale segna dunque un passaggio decisivo nella comprensione del rapporto tra amministrazione e tecnologia. Quando trasparenza e motivazione vengono meno, si apre la strada a un potere algoritmico opaco, potenzialmente lesivo dell'eguaglianza e della fiducia pubblica.
È proprio su questo terreno che si colloca la successiva analisi: quella dei *bias* algoritmici e della profilazione predittiva, dove il problema non è più soltanto chi risponde della decisione, ma come le decisioni stesse possono produrre discriminazioni sistemiche, in contrasto con il principio costituzionale di eguaglianza.

3.4. Profilazione, *bias* e principio di eguaglianza

L'art. 4, par. 4, del GDPR definisce la profilazione come qualsiasi forma di trattamento automatizzato di dati personali finalizzata a valutare aspetti personali relativi a una persona fisica.
Nei sistemi predittivi essa costituisce, pertanto, il meccanismo tecnico che trasforma dati in inferenze e le inferenze in decisioni, classificando individui e gruppi in base a somiglianze statistiche e incidendo, così, sulla distribuzione di opportunità e oneri.
Ogni operazione di profilazione implica una scelta: quali caratteristiche contano e quali possono essere trascurate, quali variabili siano predittive e quali irrilevanti. In questo senso, la selezione delle variabili rappresenta

[52] M. C. Cavallaro-G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *Federalismi.it*, 16, 2019, spec. 17.

[53] S. Sassi, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi Giuridica dell'Economia*, 1, 2019, spec. 114.

un atto di discrezionalità pubblica, che deve restare tracciabile, motivata e sottoposta a controllo. Delegare tali decisioni al modello significa spostare il baricentro della responsabilità democratica verso un dominio opaco di scelte algoritmiche.

Nel quadro dell'amministrazione predittiva, la profilazione rappresenta, dunque, il punto di massima tensione tra efficienza algoritmica e principio di eguaglianza[54].

Come è stato osservato[55], infatti, l'idea di una *fairness* (equità) automatica è logicamente incoerente perché la giustizia distributiva, implicando un giudizio di valore, non può essere calcolata. Questa tensione non è soltanto tecnica ma giuridica e ontologica.

Il diritto dell'eguaglianza si fonda su comparazioni normative, su giudizi di rilevanza e di giustificazione delle differenze che dipendono dal fine pubblico perseguito. L'algoritmo, viceversa, ragiona per correlazioni e non per cause, e proprio per questo tende per sua natura a replicare e cristallizzare *pattern* di disuguaglianze sociali preesistenti. Le decisioni automatizzate, addestrate su archivi storici, finiscono così per creare nuovi *cluster* (*social sorting*[56]) fondati su comportamenti solo apparentemente neutri – come stili di vita o abitudini alimentari – generando discriminazioni personalizzate che il diritto dovrebbe contrastare, non legittimare. La discriminazione assume allora la forma di una ingiustizia distributiva automatizzata, che riduce l'eguaglianza sostanziale a una media statistica.

Ciò dimostra che i dati non sono meri strumenti di conoscenza, ma veicoli di costruzione sociale della realtà. E poiché ogni costruzione del reale è anche un atto di potere, il diritto dei dati non appartiene alla sfera della tecnica, ma a quella inevitabilmente politica dei rapporti che essa contribuisce a istituzionalizzare[57].

La *fairness* computazionale, pertanto, può offrire solo indicatori descrittivi di disuguaglianza, ma non può sostituire il giudizio giuridico, che resta un atto di ponderazione valoriale. L'idea di un ragionamento predittivo neutrale diviene, così, un'illusione, un mito tecnico e giuridico[58] che sbiadisce

---

[54] Cfr. G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2, 2019, 199 ss.

[55] S. Wachter-B. Mittelstadt-C. Russell, *Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI*, in *Computer Law & Security Review*, 41, 2021, 1 ss.

[56] Il sociologo David Lyon descrive efficacemente questo fenomeno: D. Lyon, *Surveillance as social sorting: Privacy, risk and automated discrimination*, Londra, 2005.

[57] M. Hildebrandt-A. De Bois, *Law for Computer Scientists*, in M. Chetouani-V. Dignum-P. Lukowicz-C. Sierra (a cura di), *In Human-centered artificial intelligence: Advanced lectures*, Svizzera, 2023, spec. 261.

[58] *Ex multis* vd. M. Airoldi-D. Gambetta, *Sul mito della neutralità algoritmica*, in A. Martella-E. Campo-L. Ciccarese (a cura di), *Gli algoritmi come costruzione sociale*, in *The Lab's Quarterly*, 4, 2018, 25-46; M. De Simone, *Oltre il tipping point dell'Intelligenza Artificiale*, in *For: rivista per*

il carattere normativo delle scelte algoritmiche e, in questa prospettiva, la profilazione diventa banco di prova della capacità del principio di eguaglianza sostanziale di agire anche nel dominio dei dati.
Sotto il profilo dell'eguaglianza, è emblematico il caso COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) negli Stati Uniti, in cui un algoritmo di *risk assessment* classificava sistematicamente come "ad alto rischio" soggetti afroamericani non recidivi. Nel caso *de qua*, la discriminazione deriva non da un'intenzione, ma da correlazioni spurie e variabili *proxy*. In termini giuridici, si tratta del cosiddetto *disparate impact*[59], una forma di discriminazione indiretta prodotta da regole apparentemente neutrali ma dagli effetti diseguali.
In questo quadro, sia il *disparate impact* statunitense sia la discriminazione indiretta del diritto europeo si fondano su una logica analoga: non punire l'intenzione soggettiva, ma valutare *ex post* la ragionevolezza del criterio utilizzato e i suoi effetti differenziali.
Ciò conferma la tesi che abbiamo via via delineato: l'eguaglianza non può essere tradotta in un'unica metrica di *fairness*, poiché la giustificazione delle differenze è sempre situata e dipendente dal contesto istituzionale e dal fine pubblico perseguito[60].
Il principio di eguaglianza, però, non è solo un limite, ma una condizione di legittimità della predizione amministrativa.
L'eguaglianza sostanziale, nella lettura offerta dall'art. 3, c. 2, Cost., impone di interrogare le metriche tecniche alla luce dei valori costituzionali.
Ogni soglia, ogni funzione di perdita, ogni parametro di accuratezza incorpora un giudizio di valore che deve essere giustificato in termini di proporzionalità e ragionevolezza. In questo senso, la *fairness* computazionale è uno strumento di evidenza, non criterio di giudizio.
Da qui discende l'esigenza di un diritto dell'algoritmo capace di integrare qualità dei dati e rappresentatività sociale. La qualità, in questa prospettiva, non coincide con l'accuratezza statistica, ma comprende la neutralità, la completezza e la capacità del *dataset* di rappresentare in modo proporzionato i gruppi interessati.
L'AI Act recepisce parzialmente questo paradigma, imponendo per i sistemi ad alto rischio obblighi di qualità e di *audit* periodico, ma il suo approc-

la formazione, 3, 2023, spec. 29.

[59] Per un approfondimento sulle due dottrine giuridiche dominanti "disparate treatment" e "disparate impact", e sulle più recenti proposte di ulteriori categorie, come il "disparate mistreatment" (disparità nei tassi di errore tra gruppi di individui), si veda D. E. Moore, *Disparate treatment versus disparate impact: A distinction without a difference*, in *Syracuse Law Review*, 41, 1990, 965 ss.; M. B. Zafar-I. Valera-M. Gomez Rodriguez-K. P. Gummadi, *Fairness beyond disparate treatment & disparate impact: Learning classification without disparate mistreatment*, in *Proceedings of the 26th international conference on world wide web*, 2017, 1171 ss.

[60] S. Wachter-B. Mittelstadt-C. Russell, *Why fairness cannot be automated*, cit., spec. 22-28.

cio resta prevalentemente procedurale. *Recta via*, manca un vero principio di "substantive equality by design", una progettazione orientata agli effetti distributivi delle decisioni automatizzate[61].

Una *governance* dell'algoritmo coerente con l'art. 3, c. 2, Cost. dovrebbe invece prevedere strumenti di valutazione dell'impatto sociale, in grado di misurare la capacità del sistema di promuovere l'inclusione e di prevenire discriminazioni indirette.

La difficoltà di eliminare *ex ante* o *ex post* i *bias* deriva dalla complessità tecnica dell'"unlearning", ossia dei procedimenti di disapprendimento dell'errore[62]. In tale contesto, la *protezione by design* rappresenta un approccio promettente: integrare misure di sicurezza e di equità sin dalla progettazione dei trattamenti consente di limitare gli errori di selezione[63] e garantire tutele generalizzate, indipendenti dal consenso individuale.

Le *Privacy Enhancing Techniques* (PETs), come la *Secure Multi-Party Computation*, i *commitment* crittografici, la *Homomorphic Encryption* e i metodi di *intersection,* costituiscono strumenti tecnologici maturi per proteggere i dati sensibili lungo tutto il ciclo di trattamento[64]. Le PETs rafforzano tanto la *input privacy* (confidenzialità dei dati di partenza) quanto la *output privacy* (protezione contro la rivelazione di informazioni nei risultati), riducendo il rischio di accessi indebiti e mitigando i *bias* sistemici.

Tuttavia, tali garanzie tecniche non bastano.

Devono essere accompagnate da un impegno giuridico e culturale nella supervisione umana. L'eguaglianza non si tutela solo con norme, ma con la formazione e la responsabilizzazione di chi utilizza gli algoritmi.

A ben vedere, infatti, la giurisprudenza amministrativa europea già si muove in questa direzione. Dalle decisioni italiane sull'algoritmo ministeriale per l'assegnazione dei docenti (Tar Lazio, sez. II-Bis, 7 agosto 2017, n.

---

[61] Cfr. S. Fredman, *Substantive equality revisited*, in *International Journal of Constitutional Law*, 14, 2016, 712 ss. L'autrice propone un approccio quadrimensionale alla *substantive equality* (riduzione dello svantaggio; contrasto a stigma e stereotipi; rafforzamento di voce/partecipazione; accomodamento della differenza e cambiamento strutturale), che qui assumiamo come base teorica per un principio di "substantive equality by design".

[62] U. Ruffolo-A. Amidei, *Diritto dell'intelligenza artificiale: Vol. 1: Responsabilità. Contratto. Regolazione. Veicoli autonomi*, Roma, 2024, spec. 21.

[63] L'eterogeneità non efficacemente governata può generare "allucinazioni statistiche", che occultano relazioni causali e compromettono la qualità delle scelte pubbliche. Per uno studio del fenomeno, soprattutto nei modelli linguistici di grandi dimensioni (LLM, *large language models*) si veda: A. Bruno-P. L. Mazzeo-A. Chetouani-M. Tliba-M. A. Kerkouri, *Insights into classifying and mitigating LLMs' hallucinations*, arXiv preprint arXiv:2311.08117, 2023; F. Wang, *LightHouse: A survey of AGI hallucination*, arXiv preprint arXiv:2401.06792, 2024; C. Novelli-F. Casolari-P. Hacker-G. Spedicato-L. Floridi, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, arXiv preprint arXiv:2401.07348, 2024.

[64] E. Belissario-G. Cassano, *Intelligenza artificiale per la pubblica amministrazione*, in *Diritto di Internet e tutele dei nuovi diritti*, Pisa, 2023, spec. 206 ss.

9230) a quelle francesi su *Parcoursup* e spagnole in materia di distribuzione assistenziale, emerge un principio comune: la legalità dell'automazione è subordinata alla spiegabilità sostanziale del processo, che deve consentire al giudice e all'interessato di ricostruire la catena causale tra dati, regole e decisione. In questa chiave, la trasparenza non è un accessorio tecnico, ma l'antitesi della "discriminazione silenziosa".

La *fairness* computazionale, dunque, può avere un ruolo importante come strumento di evidenza, non di giudizio. Modelli come il *Conditional Demographic Disparity*[65] possono fornire indicatori statistici di potenziali disparità, ma spetta al diritto (e alla giurisdizione) valutarne la legittimità alla luce dei principi costituzionali.

L'eguaglianza, dunque, non è automatizzabile, è un processo deliberativo, umano e pubblico, che richiede motivazione e confronto.

In conclusione, l'eguaglianza è la bussola normativa dell'amministrazione predittiva. Non frena l'innovazione, ma la orienta, imponendo che la predizione resti compatibile con la dignità della persona e che la tecnologia rimanga strumento, non soggetto, del potere pubblico. Solo una progettazione fondata su *fairness*, *accountability* e *human oversight* può impedire che l'efficienza si trasformi in arbitrio statistico.

Su questo terreno si innesta il quadro europeo in materia di decisioni automatizzate. Il punto di convergenza tra eguaglianza e responsabilità algoritmica è rappresentato dal GDPR, cardine dell'intero sistema di tutela. È proprio al GDPR – e in particolare al suo art. 22 – che occorre ora volgere l'attenzione, per comprendere come il diritto europeo cerchi di bilanciare innovazione tecnologica e controllo umano, evitando che la predizione si traduca in una forma di spossessamento della libertà individuale.

4. L'art. 22 GDPR: decisioni automatizzate e diritto alla spiegazione

Dopo aver esaminato le tensioni tra predizione, responsabilità e uguaglianza, il passo successivo è interrogarsi sul modo in cui il diritto europeo tenta di disciplinare queste dinamiche.

Il GDPR costituisce la risposta più compiuta a tale esigenza, e in particolare il suo art. 22, dedicato alle decisioni automatizzate, rappresenta il fulcro della tutela contro l'eccesso di automazione[66]. Tale disposizione è stata

[65] S. Wachter-B. Mittelstadt-C. Russell, *Why fairness cannot be automated*, cit., 24 ss.

[66] In Italia, il principale riferimento normativo in materia di protezione dei dati personali è il d.lgs. 196/2003 (Codice della Privacy), che — pur modificato più volte, da ultimo con il d.lgs. 101/2018 — continua a costituire il quadro di riferimento per il trattamento dei dati da parte delle pubbliche amministrazioni. Le successive riforme hanno progressivamente

sin dall'inizio una delle più dibattute e controverse, poiché tocca un nodo essenziale: fino a che punto è lecito affidare a un algoritmo, piuttosto che a un decisore umano, la valutazione di interessi che incidono significativamente sulla sfera giuridica e personale dei cittadini? La questione non è soltanto tecnica, ma investe direttamente la legittimazione dell'azione pubblica e la sua compatibilità con i principi costituzionali[67] e sovranazionali che tutelano la dignità, la libertà e l'eguaglianza.

Il par. 1 della norma *de qua* riconosce, infatti, all'individuo il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Si tratta, dunque, non di una semplice facoltà azionabile a richiesta, ma di un divieto generale imposto al titolare del trattamento, che opera *ex lege* e *by default*, senza necessità di una previa opposizione da parte dell'interessato.

Questa architettura, apparentemente lineare nella sua sintetica formulazione giuridica, cela però nodi interpretativi complessi.

Il primo riguarda la definizione di decisione unicamente automatizzata. Nella prassi amministrativa e organizzativa, raramente un processo decisionale si presenta come integralmente delegato a un algoritmo, senza alcuna forma di controllo umano. Più spesso si tratta di procedure ibride, in cui l'algoritmo produce uno *score*, un *alert* o una raccomandazione che poi viene confermata, più o meno criticamente, da un funzionario. Ciò chiarito, se si seguisse un'interpretazione letterale, si potrebbe ritenere che il semplice tocco umano sia sufficiente per sottrarre l'intera procedura all'applicazione dell'art. 22, con il rischio di svuotarne la portata. Proprio per evitare tale esito, l'EDPB, nelle sue Linee guida del 2018 su *automated decision-making* e profilazione, ha sottolineato che «per aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico»[68].

---

ampliato i poteri di trattamento e condivisione dei dati da parte delle PA, in nome di una governance più efficiente e interconnessa. Tuttavia, parte della dottrina (in particolare cfr. G. Carullo, *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in *Rivista Interdisciplinare sul diritto delle Amministrazioni Pubbliche*, 3, 2024, 37 ss.) osserva che tale estensione abbia finito per indebolire le garanzie originarie a tutela dell'individuo e per limitare l'efficacia del controllo europeo, lasciando agli Stati membri un'eccessiva autonomia nel disciplinare la materia.

[67] In materia, oltre ai già citati Autori, si rimanda a A. Vedder-L. Naudts, *Accountability for the use of algorithms in a big data environment*, in *International Review of Law, Computers & Technology*, 31, 2017, 206 ss.

[68] EDPB, *Article 29 data protection working party. Guidelines on Automated Individual Decision Making and Profiling for the Purposes of Regulation 2016/679*. 17/IT WP 251 rev.01, 2018,

A ben vedere, però, questa osservazione non scioglie il dubbio iniziale: sposta semplicemente la questione su un nuovo piano. Non si tratta più di stabilire quando una decisione sia automatizzata, ma quando il controllo umano possa dirsi realmente significativo e non meramente simbolico.
Come si è già visto a proposito dell'*automation bias* e del ruolo del funzionario, la presenza umana non è di per sé garanzia di consapevolezza o autonomia decisionale. Se il soggetto incaricato non dispone delle competenze necessarie per comprendere la logica del modello, del tempo per esaminare criticamente l'*output*, o dell'autorità per modificarlo, il suo intervento si riduce alla già paventata ratifica automatica.
Difatti, parte della dottrina più sensibile[69] ha sottolineato come questa supervisione apparente sia incompatibile con la *ratio* della norma, che mira invece a preservare uno spazio effettivo di valutazione critica umana come condizione essenziale per la tutela della persona. Ne consegue che la distinzione tra decisione automatizzata e decisione assistita dall'uomo diventa labile e che il vero criterio non può essere formale, ma sostanziale, richiedendo di verificare la qualità e l'effettività dell'intervento umano.
Le difficoltà interpretative in ordine alla possibilità di esercitare un controllo significativo da parte dell'uomo trovano un'eco, *mutatis mutandis*, anche nel secondo snodo cruciale dell'art. 22: la portata della clausola sugli "effetti giuridici" o "significativi". Mentre i primi sono relativamente facili da individuare – si pensi ad un atto che attribuisce o revoca un beneficio, concede o nega un titolo, irroga una sanzione – più complessa è la valutazione di ciò che può considerarsi effetti "significativi".
All'uopo, il considerando 71 del GDPR offre un primo orientamento, precisando che tali effetti sussistono quando l'automazione incide in modo rilevante sullo *status* giuridico o sulla condizione di vita del soggetto. Pur privo di valore vincolante, a ben vedere, questo chiarimento trova riscontro nelle FAQ della Commissione europea, secondo cui la disposizione si applica anche quando l'impatto del processo automatizzato non si traduce immediatamente in un effetto legale, ma altera in modo sostanziale le opportunità o le condizioni di vita dell'interessato.
Pensiamo a un algoritmo che classifica un contribuente come soggetto "ad alto rischio fiscale", il quale, pur non determinando direttamente un provvedimento, orienta la probabilità di controlli futuri, producendo effetti economici e psicologici non trascurabili. Analogamente, un sistema che attribuisce un *rating* negativo a un'impresa che intende partecipare a un appalto, non produce un effetto giuridico immediato, ma condiziona for-

spec. 23.

[69] Cfr. C. Colapietro-A. Moretti, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, *in BioLaw Journal-Rivista di BioDiritto*, 3, 2020, spec. 382-383.

temente le decisioni dei commissari e, di riflesso, le possibilità di successo dell'operatore economico.
La Corte di giustizia dell'Unione europea, nella recente causa *Schufa* (C-634/21, 2023)[70], ha confermato questa lettura estensiva, stabilendo che lo *score* creditizio elaborato da un'agenzia privata può configurare una decisione automatizzata ai sensi dell'art. 22 quando viene utilizzato in modo determinante da un terzo, come una banca, per concedere o negare un prestito.
Il principio affermato è di grande rilievo, poiché riconosce che anche valutazioni probabilistiche, se idonee a incidere concretamente sulle scelte che riguardano la persona, rientrano nella sfera di protezione della norma. L'impatto di questa pronuncia si riverbera direttamente sull'amministrazione predittiva, nella quale punteggi e classificazioni assumono un ruolo determinante nelle politiche di controllo, nell'erogazione di prestazioni e nella gestione delle risorse.
Nondimeno, pur alla luce del considerando 71, delle FAQ della Commissione europea e della giurisprudenza che ne hanno accolto la lettura estensiva, la nozione di effetti "significativi" continua a difettare di una definizione normativa precisa, lasciando irrisolta una tensione di fondo tra certezza del diritto e adattabilità tecnologica.
Chiarito ciò, se la giurisprudenza e la prassi interpretativa hanno contribuito ad ampliare l'ambito di tutela dell'art. 22, la disposizione non rimane sgombra da ulteriori complicazioni, mostrando, ancora una volta, il suo volto ambiguo. Essa si colloca, infatti, nel punto di frizione tra la razionalità tecnico-decisionale propria dei sistemi automatizzati e la logica garantistica che ispira il diritto europeo alla protezione dei dati personali.
Tale tensione emerge in modo evidente nel par. 2 che attenua il divieto di decisioni unicamente automatizzate introducendo tre ipotesi di deroga[71]: quando la decisione è necessaria per la conclusione o l'esecuzione di un contratto, quando è autorizzata dal diritto dell'Unione o degli Stati membri e quando si fonda sul consenso esplicito dell'interessato.
In linea teorica, la clausola di deroga mira a bilanciare esigenze di efficien-

[70] Sul tema del diritto alla spiegazione, cfr. ora anche CGUE, C-203/22, *Dun & Bradstreet Austria GmbH* (2025), che, nel solco di *Schufa* (C-634/21), ha precisato che l'interessato, in caso di decisione automatizzata, può pretendere una spiegazione "significativa, comprensibile e accessibile" circa la logica utilizzata e che il bilanciamento con eventuali segreti commerciali deve essere rimesso all'autorità di controllo o al giudice competente

[71] Per completezza, pur non costituendo il tema oggetto specifico della presente analisi, si richiama altresì l'ulteriore deroga prevista dall'art. 23 GDPR, che consente agli Stati membri di introdurre limitazioni per motivi di interesse pubblico rilevante. Tale disposizione è stata, ad esempio, applicata in Ungheria durante l'emergenza COVID-19, quando il diritto di opposizione alle decisioni automatizzate è stato temporaneamente sospeso per finalità emergenziali.

za e innovazione con la protezione dei diritti fondamentali. Tuttavia, nella pratica applicazione, la sua portata risulta ambigua e rischia di indebolire l'effettività della tutela.

Per comprendere meglio questa tensione, può essere utile soffermarsi sulla deroga più rilevante nel contesto amministrativo, ossia quella che consente agli Stati membri o al diritto dell'Unione di autorizzare decisioni automatizzate purché siano previste adeguate misure di salvaguardia. Da un lato, tale previsione permette di legittimare l'uso di algoritmi nei procedimenti fiscali, previdenziali o di polizia amministrativa; dall'altro, rischia di trasformarsi in una zona franca regolatoria, attraverso la quale si amplia la discrezionalità normativa senza che vi corrisponda un effettivo presidio garantistico.

Emergono, proprio in questo punto, alcune delle ricadute pratiche della difficile intersezione suggerite nei paragrafi precedenti. Le garanzie previste dall'art. 22, come il diritto all'intervento umano o la possibilità di contestare la decisione, restano infatti difficili da esercitare quando l'algoritmo è opaco e l'interessato non può accedere ai criteri che ne hanno determinato l'esito. Analogo discorso vale per la deroga fondata sul consenso esplicito, la cui effettiva libertà e consapevolezza sono state già messe in dubbio in ragione dell'asimmetria informativa e del condizionamento che caratterizzano l'interazione tra cittadino e amministrazione digitale.

È in questo contesto che si colloca l'altro nodo cruciale della disciplina, già tratteggiato nella riflessione sull'opacità algoritmica, ossia il cosiddetto "diritto alla spiegazione" (*right to explanation*) della decisione automatizzata, che rappresenta una logica derivazione delle problematiche emerse in materia di trasparenza, discrezionalità e accountability amministrativa.

Benché il GDPR non enunci espressamente un "diritto alla spiegazione", diversi autori hanno sostenuto che la migliore lettura sistematica degli artt. 13, 15 e 22 ne sorregge l'esistenza in termini positivi, come pretesa a ricevere «*meaningful information about the logic involved*»[72] nei processi automatizzati, idonea a garantire l'esercizio effettivo dei diritti e un controllo sostanziale dell'esito.

Tuttavia, le opinioni, al riguardo, risultano divise. Altri autori, infatti, in un'ottica più restrittiva, negano l'esistenza di un diritto alla spiegazione in senso sostanziale, osservando che il GDPR riconosce solo obblighi informativi generali e garanzie procedurali; pertanto, «*after a decision has been made [...] data subjects are granted additional safeguards to obtain human intervention, express views, or contest a decision (Article 22(3)), but not to obtain an explanation of the decision reached*»[73].

---

[72] A.D. Selbst-J. Powles, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 7-4, 2017, spec. 233 ss.

[73] S. Wachter-B. Mittelstadt-L. Floridi, *Why a Right to Explanation of Automated Decision-*

La questione ruota attorno al grado di comprensibilità della logica sottesa ai processi decisionali poiché informare non significa necessariamente spiegare e, in assenza di spiegazione, il diritto di difesa resta puramente formale.
In questo senso, secondo gli studiosi dell'*Oxford Internet Institute*[74], auditi nel 2018 alla Camera dei Comuni britannica, vi sarebbe una lacuna nel GDPR: pur essendo ampiamente affermato in dottrina che l'art. 22 riconosca un diritto alla spiegazione delle decisioni algoritmiche, di fatto tale diritto non è esplicitamente previsto dalla disposizione vincolante.
Il prefato considerando 71, appunto, fa riferimento al diritto dell'interessato di ottenere spiegazioni sulla logica sottesa al trattamento automatizzato. Tuttavia, come già spiegato, il considerando «oltre ad essere una previsione giuridicamente non vincolante, per alcuni versi sembra limitarsi alla fumosa informazione circa l'esistenza di un procedimento informatizzato»[75].
Sotto altra angolazione, si potrebbe sempre osservare che l'art. 22, par. 3, impone al titolare del trattamento di adottare misure adeguate a salvaguardare i diritti e le libertà dell'interessato, garantendo almeno l'intervento umano, la possibilità di esprimere il proprio punto di vista e di contestare la decisione, ma non permette di ottenere una spiegazione dell'esito raggiunto. Tuttavia, come evidenziato dall'Oxford Institute, queste garanzie rischiano di essere di scarsa utilità se non accompagnate da un diritto effettivo a comprendere come la decisione sia stata presa.
Insomma, per garantire una reale effettività, e seguendo l'impostazione delle Linee guida dell'EDPB già citate, la trasparenza non implica l'accesso al codice sorgente, ma la possibilità di conoscere i criteri decisionali essenziali e il peso attribuito ai dati e ai fattori che hanno determinato l'esito.
La questione assume una rilevanza ulteriore in chiave costituzionale; infatti, se manca la spiegabilità, viene meno la possibilità stessa di verificare l'uguaglianza di trattamento, poiché eventuali discriminazioni o *bias* rimangono invisibili e, quindi, incontestabili.
Come già evidenziato nei paragrafi precedenti, l'AI Act si inserisce in questa prospettiva di rafforzamento, introducendo un approccio basato sul rischio che integra il GDPR e ne colma, almeno in parte, le lacune in tema di trasparenza, qualità dei dati e supervisione umana effettiva. (→ semplifico la sintassi per migliorare la fluidità) Tuttavia, più che rappresentare un punto di svolta, il nuovo Regolamento può essere letto come un completamento del sistema europeo di protezione dei dati, che trova nel GDPR il suo perno e nella combinazione dei due testi la chiave per bilanciare

Making Does Not Exist in the GDPR, in *International Data Privacy Law*, 7-2, 2017, spec. 79.

[74] Cfr. F. S. di S. Ippolito-M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, spec. 270 ss.

[75] G. Alpa, *Diritto*, cit., 285.

innovazione tecnologica e tutela dei diritti fondamentali.
Come si è già avuto modo di osservare, questo equilibrio si realizza soprattutto attraverso gli strumenti di accountability previsti dal GDPR, i quali assumono un rilievo determinante nel governo delle decisioni automatizzate. Essi traducono in pratica i principi di trasparenza e controllo umano, configurando un sistema di governance fondato su una chiara attribuzione di ruoli, obblighi e responsabilità tra i soggetti coinvolti nel trattamento dei dati personali.
Al centro di tale architettura si colloca la figura del titolare del trattamento, definito all'art. 4, par. 7, come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina, da solo o congiuntamente ad altri, le finalità e i mezzi del trattamento. A questa figura compete la responsabilità primaria, anche quando le operazioni materiali siano delegate ad altri soggetti.
Ciò premesso, il principio di *accountability*, enunciato con chiarezza all'art. 5, par. 2, impone al titolare non solo di garantire la conformità alle disposizioni del GDPR, ma anche di poterne fornire prova concreta. Ne deriva un mutamento strutturale in cui non è più sufficiente "rispettare" il diritto, ma occorre dimostrare attivamente la conformità, attraverso strumenti organizzativi e procedurali che consentano la verifica ex post della correttezza delle operazioni di trattamento.
Tra gli strumenti di attuazione, la DPIA, prevista dall'art. 35, rappresenta il principale meccanismo di prevenzione dei rischi[76]. Essa impone al titolare un'attività anticipatorio di analisi e mitigazione, finalizzata a garantire trasparenza, proporzionalità e sicurezza.
In presenza di un rischio residuale elevato, il GDPR richiede, inoltre, una consultazione preventiva con l'autorità di controllo (art. 36), rafforzando l'impianto collaborativo e dinamico della protezione dei dati.
A fondamento della DPIA, e più in generale della responsabilità del titolare, si colloca il principio di liceità, correttezza e trasparenza (art. 5, par. 1, lett. a*)*), che impone una gestione chiara e leale dei dati fin dalle prime fasi del trattamento. Pertanto, ogni trattamento deve essere fondato su un presupposto giuridicamente legittimo, «conforme alle norme ad esso applicabili (liceità), nella prospettiva di assicurare un rapporto leale tra titolare e interessato (correttezza), avendo cura di raccogliere i dati per finalità

[76] Nel quadro dell'AI Act si individuano quattro categorie principali di rischio: inaccettabile, che implica il divieto assoluto di utilizzo dell'IA (cfr. art. 5 AI Act); alto, per il quale produttori e sviluppatori sono soggetti a rigorosi obblighi specifici che coprono l'intero ciclo di vita del sistema; basso; e, infine, una soglia specifica legata alla salvaguardia della trasparenza. Vd. M. C. Pollicino, *Gli effetti della "sommatoria" tra il GDPR e il nuovo Regolamento sulle intelligenze artificiali nell'ambito dell'attività amministrativa*, in *Rivista italiana di informatica e diritto*, 7, 2025, spec. 245 e 246.

determinate, esplicite e legittime (limitazione delle finalità)»[77].
A supporto dell'*accountability,* l'art. 30 prevede l'obbligo di tenuta di un registro delle attività di trattamento, redatto e aggiornato a cura del titolare (e, ove previsto, del responsabile). Questo registro ha la funzione di rendere tracciabili tutte le operazioni effettuate, indicando le finalità, le categorie di dati e di interessati, i destinatari, i termini di conservazione e le misure di sicurezza adottate. Esso costituisce uno strumento imprescindibile per facilitare i controlli da parte delle autorità garanti e per dimostrare la conformità ai principi del Regolamento.
In tale cornice, anche il principio della protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*), previsto all'art. 25, assume un ruolo strategico. La *privacy by design* impone l'integrazione strutturale della protezione dei dati nei processi aziendali e tecnologici, sin dalle fasi di progettazione dei sistemi e dei servizi. La *privacy by default* richiede invece che, per impostazione predefinita, siano trattati solo i dati strettamente necessari rispetto alle finalità perseguite. Entrambi i principi impongono una logica di prevenzione e contenimento del rischio, che risulta cruciale soprattutto nei trattamenti automatizzati, come quelli che impiegano algoritmi di intelligenza artificiale.
Infine, la complessità delle operazioni di trattamento rende necessaria la presenza del Responsabile della Protezione dei Dati (DPO), obbligatorio in determinati casi previsti dall'art. 37. Il DPO assume funzioni di sorveglianza, consulenza e interfaccia con le autorità di controllo, garantendo il rispetto delle norme e fungendo da presidio interno di legalità. La sua presenza è particolarmente rilevante nei contesti di trattamento ad alto rischio, dove la valutazione e la gestione del rischio devono essere svolte in modo indipendente, continuativo e professionale.
Per riepilogare ed avvicinarci alle conclusioni, la DPIA si configura come uno degli strumenti più rappresentativi del nuovo approccio proattivo e dinamico alla protezione dei dati personali: se da una parte, evidenzia l'effettività del GDPR di giocare sul terreno della valutazione *ex ante* dei rischi, rappresentando il fulcro di una cultura della protezione fondata sulla responsabilizzazione concreta dei soggetti coinvolti; dall'altra parte, essa esprime in modo paradigmatico il passaggio da una logica meramente autorizzativa a una responsabilità sostanziale, orientata alla prevenzione, alla trasparenza e alla rendicontazione.
Per queste ragioni, sempre più si discute della necessità di integrare la DPIA con valutazioni più ampie, orientate ai diritti fondamentali (FRIA), in grado di considerare anche gli impatti sociali e non strettamente *pri-*

[77] S. Franca, *Il trattamento dei dati nelle sperimentazioni di intelligenza artificiale riguardanti le Pubbliche Amministrazioni*, in *Intelligenza artificiale e diritto: una rivoluzione?*, in Quaderni *ASTRID*, vol. 2, Bologna, 2022, spec. 167.

vacy-related dei sistemi predittivi.
Le tecnologie di protezione della privacy (PETs), come la crittografia, la pseudonimizzazione, l'apprendimento federato e la *differential privacy*, offrono ulteriori strumenti per ridurre i rischi.
A questi si aggiungono gli *audit* indipendenti, che consentono di verificare nel tempo l'assenza di bias e la conformità del modello ai principi normativi, e i meccanismi di supervisione umana effettiva, che devono essere pensati non come mero presidio formale, ma come funzione organizzativa dotata di poteri reali di controllo e intervento.
In definitiva, l'art. 22 GDPR rappresenta una clausola di protezione essenziale, ma non autosufficiente. La sua efficacia dipende dall'interpretazione estensiva dei concetti chiave, dalla sostanza delle garanzie applicate nelle deroghe e dall'effettività del diritto alla spiegazione. La giurisprudenza recente, come il caso *Schufa*, indica un orientamento verso la massimizzazione della tutela, ma resta la necessità di strumenti ulteriori per rendere effettiva la protezione contro i rischi della predizione amministrativa.
L'AI Act e gli strumenti di accountability già previsti dal GDPR si collocano in questa prospettiva di rafforzamento, ma il loro successo dipenderà dalla capacità degli Stati membri di tradurli in pratiche organizzative solide e trasparenti.

5. Conclusioni

L'amministrazione predittiva non è illegittima per natura, ma lo diventa quando l'*output* sostituisce il giudizio, l'opacità erode la motivazione e l'imputabilità si dissolve in automatismi non verificabili. In questa prospettiva, una lettura sostanziale dell'art. 22 del GDPR, coordinata con i doveri di supervisione umana effettiva introdotti dall'AI Act, conduce a un esito nitido: la spiegabilità funzionale, intesa come condizione giuridica di legalità, diventa il punto di equilibrio tra potere e controllo, perché consente di comprendere i fattori determinanti della decisione e il loro peso "a misura di destinatario". Da ciò discende che il consenso non può fungere da base ordinaria nei procedimenti pubblici, essendo strutturalmente fragile in presenza di asimmetrie informative.
La garanzia deve, invece, collocarsi nel cuore dell'organizzazione amministrativa, attraverso un sistema di responsabilità progettuale e continuativa che renda verificabile ogni fase del ciclo algoritmico. Valutazioni d'impatto più ricche (DPIA e, ove opportuno, FRIA), *fairness testing*, *audit* indipendenti e tracciamento delle revisioni e delle eventuali disattese dell'*output* rappresentano, in questa logica, strumenti di imputabilità sostanziale prima ancora che di conformità formale.
Inoltre, poiché gli algoritmi apprendono correlazioni e tendono a cristal-

lizzare disuguaglianze sedimentate nei dati, la spiegabilità si salda naturalmente con il principio di eguaglianza sostanziale, che torna a svolgere la funzione di bussola delle scelte tecniche. L'eguaglianza, in tal senso, non si limita a correggere gli esiti della predizione, ma ne orienta la costruzione stessa, imponendo che le metriche di equità siano sottoposte a un controllo di proporzionalità e di ragionevolezza. Ne deriva una responsabilità amministrativa di tipo sistemico, che non si esaurisce nell'atto singolo, ma percorre l'intero ciclo di vita del modello, dalla progettazione all'uso operativo e alla sua revisione.

In questo quadro, la predizione non sostituisce la decisione, né l'efficienza algoritmica può surrogare la giustificazione pubblica: la tecnologia rimane strumento e l'esercizio del potere conserva il suo carattere umano, comprensibile e responsabile. Inoltre, l'eguaglianza, nell'era dell'intelligenza artificiale, non è un vincolo esterno ma la condizione che impedisce alla previsione di diventare destino; la legalità, per non ridursi a formula rituale, deve farsi sostanziale nella convergenza tra protezione dei dati, spiegabilità e imputabilità. Solo così l'amministrazione predittiva potrà dirsi, insieme, efficiente e giusta.

Abstract

Il contributo analizza le implicazioni giuridiche dell'impiego di sistemi predittivi nella pubblica amministrazione nel campo della protezione dei dati personali, mettendo in luce le tensioni che essi generano rispetto ai principi di legalità, trasparenza, responsabilità ed eguaglianza. Muovendo da una lettura sostanziale dell'art. 22 GDPR, integrata con gli obblighi di supervisione umana introdotti dall'AI Act, il saggio vuole dimostrare come l'automazione decisionale rimodelli il potere amministrativo e metta in discussione la sua intelligibilità e imputabilità. L'analisi, quindi, propone una ricostruzione dogmatica fondata sull'idea che la responsabilità organizzativa e il controllo umano costituiscano condizioni essenziali di una legalità algoritmica dell'azione amministrativa, nella quale la protezione dei dati e l'eguaglianza sostanziale convergono in un'unica architettura di garanzie.

The paper analyses the legal implications of the use of predictive systems within public administration in the field of personal data protection, highlighting the tensions they generate with regard to the principles of legality, transparency, accountability, and substantive equality. Building on a substantive reading of Article 22 of the GDPR, integrated with the human oversight obligations introduced by the AI Act, the study aims to demonstrate how automated decision-making reshapes administrative power and calls into question its intelligibility and imputability. The analysis therefore proposes a dogmatic reconstruction based on the idea that organisational accountability and human control constitute essential conditions for the algorithmic legality of administrative action, in which data protection and substantive equality converge within a single architecture of safeguards.

Keywords

algorithmic administration – Article 22 GDPR – AI Act – functional explainability – substantive equality

Un delicato equilibro di potere: le istituzioni religiose nella *governance* dei *social media*[*]

Nico Tonti

Sommario

1. Un nuovo tempo e un nuovo spazio: i pericoli di un carsico "laicismo digitale". – 2. Il potere dislocato della virtualità: istituzioni religiose e processi di legittimazione. – 3. L'eccedenza positiva del fenomeno religioso associato nella *governance* digitale. – 4. Le potenzialità (ancora inespresse) offerte dal diritto dell'Unione europea. – 5. *Quo itur*?

1. Un nuovo tempo e un nuovo spazio: i pericoli di un carsico "laicismo digitale"

È ormai ampiamente sedimentata nel *sensus communis* la consapevolezza per la quale l'esperienza giuridica contemporanea, così come l'insieme delle relazioni politiche, sociali e culturali che essa riflette, è costretta a misurarsi con un fenomeno di portata epocale, che ha profondamente segnato (e continuerà verosimilmente a farlo) le forme della convivenza civile: ovvero, l'incidenza dei *social media* sull'essere e sull'agire umano, tanto nella sua dimensione individuale quanto nelle sue plurime proiezioni collettive[1].

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

[1] Senza alcuna pretesa di esaustività si veda L. Floridi, *La quarta rivoluzione*, Milano, 2017; A. Biscaldi – V. Matera (a cura di), *Social Media and Politics of Identity*, Milano, 2024; K. Barker – O. Jurasz (a cura di), *Routledge Handbook of Social Media, Law and Society*, New York, 2025. Dall'angolazione prettamente giuridica, si è autorevolmente osservato che « solo chi è rimasto alla preistoria del diritto e si aggira ancora armato di clava cercando di inventare la ruota, non si rende conto del passaggio epocale che si è verificato nelle società evolute in questi anni: la possibilità di accedere sempre, dovunque a tutta la conoscenza racchiusa in testi digitali; la possibilità di comunicare sempre dovunque e a costi minimi con tutti; la possibilità di diffondere sempre e dovunque a tutto il mondo il proprio pensiero. E solo i cavernicoli non si accorgono del circuito inarrestabile fra accesso alle fonti di conoscenza, creazione di forme di scambio di esperienze, diffusione di nuove idee, e creazione di nuova conoscenza», V. Zeno Zencovich, *Perché occorre rifondare il significato della libertà di manifestazione del pensiero*, in *Percorsi Costituzionali*, 1, 2010, 71.

Segnatamente, l'analisi del rapporto tra fenomeno religioso associato ed ecosistema digitale esige, come premessa metodologica imprescindibile, il superamento di ogni residua concezione ingenuamente strumentale delle piattaforme *social*: intese, cioè, quali semplici supporti tecnico-materiali destinati a veicolare contenuti – per quel che qui interessa, religiosamente orientati – senza ripercussioni significanti sulle modalità di interazione tra utenti-cittadini[2]. La letteratura, già da tempo, segnala la necessità di riconoscere come il *cyberspazio* si sia configurato – e, invero si stia sempre più strutturando – con le caratteristiche proprie di un vero e proprio sistema normativo *in fieri*[3], ovvero un ambiente antropologico e giuridico dotato di specifiche logiche di funzionamento e portatore di un preciso *asset* valoriale, capace di influenzare le configurazioni con cui gli individui e le comunità – globalmente considerati come utenti – si autorappresentano, si organizzano e si legittimano[4]. Più precisamente la congerie di fonti che regola il vivere consociato sulle piattaforme *social* (*policies*, *standards*, condizioni d'utilizzo) può essere raffigurato come il riverbero di un ordinamento *in statu nascendi*[5], dotato di un potere regolativo[6] che, pur privo di legittimazione democratica, produce effetti giuridici immediati sulla vita degli utenti[7]. In altre parole, «occupiamo e viviamo realmente due mondi differenti, ognuno con regole e comportamenti consuetudinari propri e dotato

[2] Da ultimo, si rinvia a P. Annicchino*, Interazione tra diritto e religione nella transizione digitale*, Torino, 2025.

[3] In cui, per esempio, «Le regole pattizie elaborate da Facebook [come invero di tutte le piattaforme, n.d.r.], del tutto slegate dagli ordinamenti giuridici cui appartengono gli utenti della piattaforma, assumono [...] un ruolo preponderante nel decidere questioni che toccano quei diritti fondamentali su cui si basano le democrazie occidentali», S. Pelleriti, *La* governance *privata di* Facebook *e la presa di coscienza del regolatore europeo: qualcosa sta cambiando?*, in *Rivista della Regolazione dei mercati*, 2, 2021, 431.

[4] Cfr. in argomento, *ex plurimis*, J. Bayer, *Rights and Duties of Online Platforms*, in Ead. - B. Holznagel - P. Korpisaari - L. Woods (eds.), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe*, Baden-Baden, 2021, 25 ss.; K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Review*, 6, 2018, 1598 ss.; R.J. Hamilton, *Governing the Global Public Square*, in *Harvard International Law Journal*, 1, 2021,117 ss.

[5] In cui, cioè il «cyberspace is a distinct place for purposes of legal analysis by recognizing a legally significant border between cyberspace and the real world», divenendo così «*an important forum for the development of new connections between individuals and mechanism of self-governance*», D.R. Johnson – D. Post, *Law and Borders. The rise of Law in Cyberspace*, in *Standford Law Review*, 48, 1996, 1378.

[6] Sulla dicotomia potere-sovranità digitale, si veda la lucida analisi di G.D. Finocchiaro, *Sovranità digitale*, in *Diritto pubblico*, 3, 2022, 809 ss.

[7] Cfr. S. Theil, *Private censorship and structural dominance: why social media platforms should have obligations to their users under freedom of expression*, in *The Cambridge Law Journal*, 3, 2022, 645 ss.

di una logica e una percezione distinta di ciò che è lecito e ciò che non lo è»[8]: e, dunque, violare *policies* e condizioni d'utilizzo significa incorrere in sanzioni variabili che possono andare dalla semplice deindicizzazione di un contenuto *social* fino al *ban*[9]. Non si tratta, quindi, di agorà artificiali che si limitano a replicare dinamiche normo-giuridiche già sperimentate nella vita "*off line*" bensì di uno spazio che trasforma radicalmente le forme della coesistenza, ridefinendo i confini tra pubblico e privato, in cui i profili a cavallo tra la sfera istituzionale e informale finiscono per confondersi nella persuasiva (ma, invero, ingannevole) promessa di neutralità[10] ed equidistanza[11] che dovrebbero caratterizzare *policies*, *standards* e condizioni di utilizzo[12].

A ben vedere, infatti, l'autoregolamentazione dei *social* rappresenta tutti gli effetti una normazione privata che, *de facto*, assume caratteri para-statali[13]:

---

[8] Z. Bauman, *La vita tra reale e virtuale*, Milano, 2014, 29.

[9] A questo proposito, si rinvia a S. Martinelli, *La chiusura dell'account Facebook di un'associazione: quale tutela?* - (Nota a ordinanza Tribunale civile Trieste 27 novembre 2020, n. 2032), in *Giurisprudenza italiana*, 10, 2021, 2091 ss.

[10] In tempi non sospetti, M. Cuniberti, *Potere e libertà nella rete*, in questa *Rivista*, 3, 2018, 51, ammoniva che «parlare di libertà della rete appare non solo sbagliato, ma anche pericoloso, nel momento in cui è sempre più evidente che la rete è (anche) una enorme struttura di controllo sociale e di manipolazione, in cui gli utenti, mentre coltivano l'illusione di partecipare mettendo in rete pensieri, opinioni ed emozioni, vengono espropriati di sé stessi, e la loro identità viene messa a profitto e ridotta a merce; sicché, anche l'illusione dello «sviluppo della personalità» di cui si alimenta il richiamo all'art. 2 Cost. rischia di tradursi, neppure tanto paradossalmente, nella negazione della personalità stessa».

[11] Si vedano a proposito le pagine critiche di M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *La Rivista del Gruppo di Pisa*, 2, 2021, 12 ss. Sul punto cfr. anche M. Cuniberti, *Potere e libertà nella rete*, cit., 51 ss.

[12] Pur nella consapevolezza delle differenti denominazioni che le diverse piattaforme attribuiscono alle proprie *policies*, si è deliberatamente optato, al fine di garantire una maggiore fluidità e coerenza espositiva, per l'utilizzo di tali espressioni come termini equivalenti, intendendoli, cioè, quali designazioni di precetti atti a orientare comportamenti e processi decisionali all'interno di un determinato contesto operativo. Più in generale, si veda L. Torchia, *Poteri pubblici e poteri privati nel mondo digitale*, in *Il Mulino*, 1, 2024, 14 ss. Della stessa Autrice cfr. anche *Lo Stato digitale. Una introduzione*, Bologna, 2023.

[13] Non è questa la sede di illustrare i termini dell'ampia discussione in seno alla dottrina, a cui si rimanda per ulteriori approfondimenti: basti qui ricordare che le piattaforme non si limitano a fornire un servizio, bensì definiscono esse stesse le "regole del gioco", elaborano *policies* interne, stabiliscono procedure di reclamo, determinano criteri di accesso e permanenza nella *virtual life*, dispongono della capacità di oscurare, rimuovere, declassare, (o, per converso, promuovere) e silenziare singoli contenuti e interi *account*. In tal senso esse agiscono come organismi che detengono la potestà di emanare regolamentazioni, di eseguirle e di farle rispettare attraverso i meccanismi di moderazione: tutto ciò, giova precisarlo, senza che vi sia un controllo democratico effettivo né una rappresentanza pluralistica degli interessi in gioco. In effetti, tali caratteristiche non fanno altro che riflettere fedelmente le «dinamiche di funzionamento delle piattaforme digitali.

si legittima da sé e da sé trae tutti gli strumenti affinché venga applicata[14]. Ciò che accade è sotto gli occhi di tutti. Le grandi piattaforme su cui si dipana la vita di centinaia di milioni di utenti definiscono il dicibile, il visibile e financo il condivisibile, esercitando una forma di potere regolativo che non conosce confini territoriali[15] e non è soggetto ad alcun controllo democratico[16]: è quasi un'ovvietà ricordarlo ma occorre tenerlo presente poiché costituisce il punto di partenza di qualunque possibile ripensamento dell'attuale *status quo*.

Parallelamente, come già stato evidenziato da accorta dottrina, la pandemia da Covid-19, con la repentina trasposizione delle pratiche cultuali e delle preoccupazioni *lato sensu* pastorali nella virtualità, ha reso tangibile anche per le confessioni l'esigenza di questo processo di transizione digitale[17]. Tale trasmigrazione si è dimostrata invero almeno parzialmente

---

Questi soggetti sono, infatti, veri e propri poteri privati in competizione col potere pubblico, che esprimono ordinamenti giuridici alternativi agli Stati-nazione, fondati sulla coincidenza tra ordinamento (*Ordnung*) e localizzazione territoriale (*Ortung*). Il pluralismo giuridico e la differenziazione sociale che caratterizzano la società globale, l'esistenza cioè di una pluralità di organizzazioni private che operano su scala transazionale secondo regole autonome, funzionali alla soddisfazione dei rispettivi interessi settoriali, hanno sollecitato la teorizzazione delle costituzioni civili o societarie, sistemi normativi sorti dall'incontro tra fonti di autonormazione di istituzioni globali private o para-pubbliche e decisioni paragiurisdizionali di soggetti impolitici (quali corpi arbitrali, comitati etici etc.)», C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quaderni costituzionali*, 3, 2023, 553.

[14] Cfr. M. Monti, *Privatizzazione della censura e Internet platforms: la libertà di espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e diritto*, 1, 2019, 35 ss. Sui processi di *content moderation*, *ex plurimis*, B. Farrand, H. Carrapico, *Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators*, in *Journal of Information Technology & Politics*, 2013, 357 ss.; K. Klonick, *The new governors: the people, rules, and processes governing online speech*, cit., 1599 ss.; G. De Gregorio, *Democratising online content moderation: A constitutional framework*, in *Computer Law & Security Review*, 2019, 1 ss.; A.P. Heldt, *Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum*, in *Mitchell Hamline Law Review*, 5, 2020, 997 ss.

[15] Cfr. ampiamente le considerazioni di M.R. Burnstein, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, in *Vanderbilt Journal of Transnational Law*, 1, 1996, 75 ss. L'autore svolge le sue teorizzazioni sul *web* generalmente inteso, ma considerazioni analoghe posso essere svolte senza significativi scarti di significato pure in relazione alle infrastrutture digitali.

[16] *Ex plurimis*, si rinvia a C.R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media*, Princeton, 2017; J.A. van Dijk - K.L. Hacker, *Internet and Democracy in the Network Society*, New York, 2018; M. Monti, *Le* Internet platforms*, il discorso pubblico e la democrazia*, in *Quaderni costituzionali*, 4, 2019, 811 ss.

[17] In argomento la dottrina è sterminata, *ex multis*, cfr. G. Boni, *Il fondamentale diritto dei fedeli ai sacramenti*, Centro Studi Rosario Livatino, 7 maggio 2020 in *centrostudilivatino.it*; C. Giraudo, *La vita sacramentale in tempo di pandemia*, in L. Alici – G. de Simone – P. Grassi (a cura di), *Quaderni di dialoghi. Speciale 2020. La fede e il contagio nel tempo della pandemia*,

reversibile ma, al contempo, ha dato prova di inedite modalità di vivere la propria appartenenza fideistica *uti singoli* e *in societas* nell'ecosistema virtuale. Solo a titolo meramente esemplificativo, si ricordino, a questo proposito, il profluvio di celebrazioni religiose di vario tipo officiate a distanza, incontri catechetici mediati da strumenti telematici e colloqui spirituali affidati a mezzi di comunicazione istantanea: ciò, a ben vedere, se può essere letto come un fenomeno contingente e "di reazione" rispetto all'emergenza pandemica, ha altresì inequivocabilmente dimostrato che la dimensione religiosa non è rimasta ai margini della trasformazione tecnologica ma è stata da essa profondamente rimodellata, sino a divenire parte integrante dell'esperienza digitale.

In tale scenario, appare forse riduttivo pensare le confessioni religiose, e le articolazioni operative che da esse germinano, come a soggetti-utenti che semplicemente trasferiscono nell'ambiente virtuale attività da sempre esercitate nello spazio fisico: come, in verità, fino ad ora è stato fatto. Occorrerebbe forse investigare opzioni differenti che, anzitutto, valorizzino, attraverso gli strumenti – ancora limitati – messi a disposizione dal diritto dell'Unione europea, il loro potenziale ruolo di *policy makers*, il quale – in prospettiva – potrebbe determinare positive e significanti ripercussioni nel perimetro normativo segnato delle *policies* elaborate dai *providers*[18]. È infatti fin da subito opportuno sottolineare che le confessioni incarnano un patrimonio simbolico e normativo, talvolta sedimentatosi lungo secoli di storia, che ha contribuito a sagomare la fisionomia delle istituzioni giuridiche secolari e le strutture socio-culturali delle collettività contemporanee: peraltro, il processo osmotico tra istituzioni religiose e società civile è un tema ampiamente dissodato in letteratura e, proprio dalle concrezioni dottrinali in argomento, si può tracciare più di una pista d'indagine funzionale

Roma, 2020, 53 ss. Sui limiti all'esercizio del culto durante l'emergenza pandemica, cfr. N. Colaianni, *La libertà di culto al tempo del coronavirus*, in *Stato, Chiese e pluralismo confessionale*, 7, 2020, 25 ss.; T. Di Iorio, *La quarantena dell'anima del* civis-fdelis. *L'esercizio del culto nell'emergenza sanitaria da Covid-19 in Italia*, in *Stato, Chiese e pluralismo confessionale*, 11, 2020, 36 ss.; A. Fuccillo, M. Abu Salem, L. Decimo, *Fede interdetta? L'esercizio della libertà religiosa collettiva durante l'emergenza Covid-19: attualità e prospettive*, in *Calumet*, 2020, 87 ss.; M. Ganarin, *Specificità e potenzialità del diritto canonico al tempo della crisi epidemica in Italia*, in *Ius canonicum*, 2021, 199 ss..; G. Macrì, *La libertà religiosa alla prova del Covid-19. Asimmetrie giuridiche nello stato di emergenza e nuove opportunità pratiche di socialità*, in *Stato, Chiese e pluralismo confessionale*, 9, 2020, 23 ss.. Più di recente, è tornato sul tema M. Toscano, *Emergenza sanitaria e libertà di religione*, Torino, 2024.

[18] Nel solco delle riflessioni di R. Caplan, *Networked Platform Governance: The Construction of the Democratic Platform*, in *International Journal of Communication*, 17, 2023, 3451 ss., per il quale ancora le piattaforme mantengono un controllo centrale e utilizzano la "network governance" come strumento retorico e organizzativo per distribuire solo simbolicamente la responsabilità, non escludendo però in futuro una diversa ripartizione del potere effettivo sulle (e nelle) piattaforme.

a coniugare il portato storico degli aggregati confessionali con le nuove tendenze in tema di *governance* digitale[19]. Rimanendo confinati nell'ambito dei tre monoteismi di matrice abramitica è fuori di dubbio che la loro azione non si sia limitata alla "produzione di contenuti" religiosi ma, parallelamente, abbia espresso una capacità regolativa in grado di disciplinare rapporti complessi, costruire comunità coese e comporre tensioni sociali fortemente polarizzate. La trasposizione di tale funzione nell'universo digitale non costituisce, pertanto, un'opzione residuale quanto piuttosto una possibile condizione per scongiurare il rischio che la *governance* dei *social media* resti manovrata da grandi *players* tecnologici e monopolizzata dalle logiche utilitaristiche e performative: logiche, queste ultime, che tendono a ignorare la profondità e la complessità simbolica e valoriale della dimensione religiosa perché orientate, in definitiva, al profitto.

Se si accetta che una futura cittadinanza digitale[20] non debba esaurirsi in un insieme di interazioni governate da codici comportamentali espressione di una volontà unilaterale (quella delle piattaforme)[21], diviene evidente che le molteplici espressioni che compongono la società civile, tra cui le confessioni religiose, devono essere riconosciute come interlocutori qualificati e necessari[22]. La loro voce, qualora non si riduca a sterili rivendicazioni

[19] Sull'influenza delle istituzioni religiose nella formazione di una cultura giuridica comune nel nostro Paese, per tutti, si veda C. Cardia, *Ordinamenti religiosi e ordinamenti dello Stato. Profili giurisdizionali*, Bologna, 2003.

[20] Intesa nell'accezione proposta da M. Di Felice*, La cittadinanza digitale*, Milano, 2019.

[21] Peraltro, come già ricordato, attraverso processi tecnici pilotati da interessi economici come illustrato da M. Hindman, *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy*, Princeton, 2018.

[22] In questo senso, sono infatti diversi gli esempi che potrebbero essere offerti. Per quel che qui interessa, ci si limita a ricordare il ruolo svolto dalla Chiesa cattolica che già da tempo ha avviato una riflessione sul piano pastorale (ma non solo) relativa alle intersezioni tra l'esperienza di fede e la cultura digitale. A tal proposito, è da rammentare – già più di vent'anni fa – la Lettera apostolica *Il rapido sviluppo* del 24 gennaio 2005 (in *Acta Apostolicae Sedis*, 97, 2005), 265 ss.), in cui l'allora pontefice regnante Giovanni Paolo II insisteva sull'attenzione che la Chiesa doveva riservare al proliferare delle nuove tecnologie digitali. Nel medesimo solco si è posto Benedetto XVI: quest'ultimo nell'enciclica *Caritas in veritate*, in *Acta Apostolicae Sedis*, 101, 2009, n. 73, chiarisce che il «senso e la finalizzazione dei media vanno ricercati nel fondamento antropologico. Ciò vuol dire che essi possono divenire occasione di umanizzazione non solo quando, grazie allo sviluppo tecnologico, offrono maggiori possibilità di comunicazione e di informazione, ma soprattutto quando sono organizzati e orientati alla luce di un'immagine della persona e del bene comune che ne rispecchi le valenze universali. I mezzi di comunicazione sociale non favoriscono la libertà né globalizzano lo sviluppo e la democrazia per tutti, semplicemente perché moltiplicano le possibilità di interconnessione e di circolazione delle idee. Per raggiungere simili obiettivi bisogna che essi siano centrati sulla promozione della dignità delle persone e dei popoli, siano espressamente animati dalla carità e siano posti al servizio della verità, del bene e della fraternità naturale e soprannaturale. Infatti, nell'umanità la

settoriali, contribuisce infatti a mantenere viva la consapevolezza che la salvaguardia delle libertà (segnatamente quella religiosa) non si riduce ad accessorio del vivere comune ma, se opportunatamente valorizzata, costituisce il presupposto imprescindibile che connota la qualità e la profondità valoriale di un ordinamento *lato sensu* inteso, anche quando questo assume le forme inedite – e, invero, ancora incerte – del *cyberspazio*[23]. E dunque, la partecipazione delle istituzioni confessionali alla definizione di quel coacervo di autoregolamentazioni elaborate dalle grandi piattaforme che si potrebbero definire – per semplicità – *lex digitalis*, non raffigura un beneficio discrezionale concesso dai *providers* quanto piuttosto un'esigenza strutturale affinché lo spazio virtuale non si impoverisca di senso e non cada preda di un rinnovato laicismo che riduca la professione di fede a dato personalissimo e, quindi, irrilevante nella dimensione pubblica[24]. Nel perimetro di questa premessa, come si tenterà di dimostrare, le fedi religiose non sono chiamate solo a difendere i diritti delle comunità che rappresentano, ma, auspicabilmente, responsabilizzate nel conferire dispositivi semantici nella costruzione di un "ordine virtuale" più pluralista e inclusivo, capace di restituire dignità e riconoscimento a tutte le identità che ne popolano l'orizzonte.

2. Il potere dislocato della virtualità: le istituzioni

libertà è intrinsecamente collegata con questi valori superiori». Da ultimo, poi, si veda anche Francesco, *Messaggio per la 53ma Giornata Mondiale delle Comunicazioni Sociali*, "Siamo membra gli uni degli altri" (Ef. 4,25). *Dalle* social network comunities *alla comunità umana*, 24 gennaio 2019 (consultabile sul sito *vatican.va*). Sul punto si rinvia a M. Martini, *The Catholic Church and the Media: A Text Mining Analysis of Vatican Documents from 1967 to 2020*, in *Journal of Media and Religion*, 3, 2022, pp. 155-173. Invero, pure altre realtà religiose hanno dimostrato di poter offrire un contributo alla riflessione sul digitale ai propri fedeli ma pure alla società civile. Su quest'ultimo tema cfr. R. Santoro - F. Gravino, *Internet, culture e religioni. Spunti di riflessione per un web interculturale*, in *Stato, Chiese e pluralismo confessionale*, 20, 2020, 99 ss., spec. 108 ss. F. Balsamo, Apps *religiose e intelligenza artificiale generativa: problematiche giuridiche*, in *Diritto e religioni*, 2, 2023, 116 ss.

[23] In argomento si veda S. Rodotà, *Una Costituzione per Internet?*, in *Politica del diritto*, 3, 2010, 337 ss.

[24] Sulla tensione tra la dimensione pubblica e quella privata dell'appartenenza religiosa e sui risvolti giuridici prodotti da tale dicotomia, per tutti si rinvia a C. Cardia, *Le sfide della laicità. Etica, multiculturalismo, islam*, Cinisello Balsamo, 2007. In aggiunta, sui processi di frammentizzazione sociale che accadono nel *web*, il rimando è d'obbligo a J. Habermas, *Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere*, in *Theory, Culture & Society*, 4, 153 ss.

religiose e i processi di legittimazione

L'evoluzione del diritto di libertà religiosa, tradizionalmente garantito attraverso il riconoscimento costituzionale e la protezione del diritto internazionale, incontra nel contesto digitale una serie di ostacoli che rischiano di comprometterne l'effettività, giacché le dinamiche innescate dall'utilizzo delle infrastutture *social*, anziché porsi come prosecuzione lineare dello spazio fisico, introducono nuove forme di esercizio del potere che sfuggono ai canoni classici della sovranità statale, intaccando conseguentemente la tenuta dei diritti fondamentali[25]. L'argomento, come noto, è stato ampiamente dissodato dalla dottrina[26]: in estrema sintesi e nell'alveo di quanto qui rileva, la *vexata quaestio* è la seguente. Le *social media platforms*, operando mediante processi *data driven* e sistemi di regolazione interna, esercitano un'autorità che, pur non perfettamente assimilabile a ordinamenti di matrice statualistica, possiede effetti diretti sulla possibilità di esprimere e condividere le manifestazioni del proprio pensiero, anche religioso[27]. È dunque evidente che ci si trovi dinanzi «a soggetti nuovi che dettano regole in un modo nuovo, diversamente da quanto accadeva nell'ordinamento giuridico dominato dallo Stato nazionale»[28]: non che in passato i poteri privati non rivendicassero spazi di libertà (e quindi, in qualche misura, di potere), i quali tuttavia venivano accordati all'interno di precise coordinate fissate dall'autorità pubblica[29]. Questo cambio di paradigma, come evidente, è problematico per (almeno) due ordini di ragioni.

Anzitutto, si è concretamente determinato un fenomeno inedito, e per certi versi preoccupante, che investe la garanzia di diritti di primaria rilevanza in relazione alla cosiddetta normazione privata: quest'ultima – vista l'ampiezza e la transnazionalità delle piattaforme – sembra assumere caratteri sempre più pervasivi e, attraverso l'autoregolamentazione sulla modera-

[25] Sulla dialettica tutela dei diritti e potere privato si vedano le riflessioni risalenti ma, invero, ancora attuali di G. Lombardi, *Potere privato e diritti fondamentali*, Torino, 1970. Più di recente, invece si rinvia a F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Napoli, 2022.

[26] Per tutti, cfr. G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in questa *Rivista*, 1, 2018, 20 ss. Pure più di recente, M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in questa *Rivista*, 2, 2021, 67 ss.

[27] Da una prospettiva più ampia si veda G. Cassano – A. Contaldo, *Internet e tutela della libertà di espressione*, Milano, 2009; M. Betzu, *Regolare Internet. Le libertà di informazione e di comunicazione nell'era digitale*, Torino, 2012.

[28] G. D. Finocchiaro, *Sovranità digitale*, cit., 816.

[29] Cfr. per tutti, C.M. Bianca, *Le autorità private*, Napoli, 1977. Sulle riflessioni del grande giurista catanese, sono ritornati più di recente P. Sirena – A. Zoppini (a cura di), *I poteri privati e il diritto della regolazione. A quarant'anni da* «*Le autorità private*» *di C.M. Bianca*, Roma, 2018.

zione dei contenuti (nonché, sulle procedure di segnalazione e sui meccanismi di deindicizzazione) condiziona in maniera incisiva la fruibilità dei messaggi a sfondo religioso[30]. Il nesso (apparentemente) consequenziale per il quale alcuni diritti consolidati nella vita "reale" – solennemente e unanimemente suggellati nelle costituzioni europee, tra i quali ovviamente rientra la libertà religiosa – sarebbero parimenti salvaguardati in rete è, in verità, solo un sinolo apparente: il *web*, e specificatamente le *community online*, configurano a tutti gli effetti modulazioni privatistiche con propri codici comportamentali e un apparato di "precetti" da rispettare, talvolta in maniera minuziosa, per non essere ostracizzati dalla *community*.

In seconda battuta è doveroso ricordare l'intrinseco *deficit* di democraticità che connota i *social media*: l'illusione della sconfinata libertà e della neutralità della rete si è scontrata, in verità fin dalla sua origine, con l'esigenza di fissare alcune regole per una possibile convivenza e, conseguentemente, di sanzionare l'eventuale trasgressore[31]. Tale disciplina, tuttavia, non si legittima – come già detto – né sulla base di processi democratici né, peraltro, in forza dei capricci dispotici di un soggetto individuabile, quanto, piuttosto, dal volere di attori economici privati, il cui obiettivo primario – almeno attualmente – resta la massimizzazione del profitto e la stabilità dei modelli di *business* applicati. In questo magmatico contesto, la libertà religiosa, pur proclamata in astratto nelle *policies* come valore da perseguire, si è trasformata in un diritto vulnerabile[32]. Sebbene infatti la professione di fede non sia apertamente avversata e programmaticamente esclusa dal catalogo di "beni" che le *policies* delle piattaforme *social* intendono salvaguardare, essa al contempo è quotidianamente oggetto di bilanciamenti (e inevitabili compressioni) attraverso decisioni tecniche spesso automatizzate la quali, nonostante si presentino come neutre, riflettono inevitabilmente *bias* culturali o, ancor peggio, valutazioni arbitrarie[33].

---

[30] Non a caso, peraltro, la giurisprudenza si è già confrontata «con la difficoltà di stabilire il confine oltre il quale l'autonomia privata (di cui il contratto che regola il servizio di social network è, pur sempre, espressione), esiga invece una peculiare forma di eteroregolazione funzionale alla garanzia dei diritti e delle libertà incise da questi contratti», F. Resta, *Le piattaforme e la visibilità del potere*, in P. Stanzione (a cura di), *I poteri privati delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, 372.

[31] Cfr. G. De Minico, *Libertà in Rete. Libertà dalla Rete*, Torino, 2020.

[32] Cfr. per tutti le ampie riflessioni di O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Londra, 2021. Considerazioni in questo senso, relativamente alla libertà di espressione, sono rinvenibili in C. Caruso, *I custodi di silicio. Protezione della democrazia e libertà di espressione nell'era dei social network*, in Liber Amicorum *per Pasquale Costanzo*, III, Collana di studi di Consulta on-line, 2020, 1 ss.

[33] Evidentemente, ciò può avvenire anche nelle aule giudiziarie ma il rischio di valutazioni *data driven* che incidano così pesantemente sulla possibilità di manifestare esternamente la propria identità è immediatamente percepibile.

L'etichettatura di taluni contenuti religiosi come "sensibili", l'oscuramento di immagini sacre bollate come inappropriate in base a criteri standardizzati, la sospensione di *account* che diffondono messaggi confessionali giudicati divisivi da parametri spesso opachi, sono esempi di un incedere quantomeno opinabile che, nella sostanziale latitanza di un robusto intervento "correttivo" statale, corre il serio pericolo di incrinare irreversibilmente la possibilità di manifestare liberamente la propria aderenza fideistica nello spazio virtuale[34]. A questo proposito, risalta immediatamente uno snodo di natura squisitamente giuridica non di poco momento: in che misura l'autonomia regolativa delle piattaforme può legittimamente prevalere sul godimento di libertà fondamentali, e fino a che punto è ammissibile che tali prerogative siano delegate a soggetti che non rispondono ad alcun principio democratico di rappresentanza della comunità degli utenti?
Il diritto positivo, a livello tanto nazionale quanto sovranazionale, non solo stenta nella rincorsa dei fulminei transiti che "accadono" sui *social* ma soprattutto fatica a adattare le proprie categorie giuridiche a questo originale e proteiforme scenario[35]. D'altronde, come noto, i tradizionali strumenti di tutela e i presidi di salvaguardia dei diritti risultano calibrati su rapporti tra individui, collettività e Stato, non sulle relazioni fra individui e colossi privati, peraltro dotati di leve finanziarie non indifferenti, che operano su scala planetaria. In questo riquadro dai contorni così frastagliati ci si potrebbe chiedere quale ruolo potrebbero rivestire le istituzioni confessionali in un torno di tempo in cui neppure l'autorità statuale riesce a fornire convincenti alternative né, tantomeno, strumenti di controllo e vigilanza davvero efficaci. Se si restringe il campo d'osservazione alle discipline giuridiche del fenomeno religioso, è proprio in questo vuoto[36], qualcuno direbbe voluto, di responsabilità pubblica che si profila un'occasione irripetibile per gli aggregati confessionali *lato sensu* intesi[37].

---

[34] Il tema, da una visuale prospettica più ampia, è stato recentemente scandagliato da P. Annicchino*, L'interazione tra diritto e religione nella transizione digitale*, cit., 22 ss.

[35] In effetti, «L'ascesa dei giganti della tecnologia come Facebook è stata senz'altro facilitata, tra le altre cose, dalla loro capacità di vanificare le regole giuridiche tradizionali e di amplificare il fenomeno della de-regolazione digitale. Facebook si è attentamente costruita nel tempo un sistema di auto-regolazione che ancora oggi fa vacillare la *governance* pubblica, che a fatica sta cercando una via per riaffermare il proprio ruolo nella regolazione del mondo digitale», S. Pelleriti, *La governance privata di Facebook e la presa di coscienza del regolatore europeo: qualcosa sta cambiando?*, cit., 441. Sempre in argomento si rinvia pure a L. Ammannati, *I "signori" dell'era dell'algoritmo*, in *Diritto pubblico*, 2, 2021, 383.

[36] A questo proposito, si è perfino sostenuto, un poco laconicamente, che «il *code* sostituisce il diritto», E. Maestri, Lex informatica *e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars interpretandi*, 1, 2017, 16.

[37] Di recente ha sviluppato una coerente riflessione sull'argomento, in ispecie nel rapporto tra appartenenza confessionale associata e la pervasiva diffusione dell'intelligenza

Considerato che la matrice religiosa ha inciso in modo determinante nella formazione dell'assetto socio-normativo delle moderne società post-secolari, non è irragionevole ipotizzare che un'influenza analoga possa oggi esercitarsi su grandi infrastutture digitali, anche attraverso strumenti di cooperazione e partecipazione nella definizione delle *policies* e delle condizioni di erogazione dei servizi da parte dei *provider*[38]. Segnatamente, il coinvolgimento delle comunità religiose nei processi di regolazione appare essenziale per scongiurare il rischio che il *cyberspazio* diventi un ambiente esclusivamente governato da logiche di mercato e pilotato da sterili parametri economici[39]. Segnatamente, la loro partecipazione non deve essere intesa come una forma di privilegio confessionale, francamente ormai dal tutto anacronistica, bensì come strumento per un possibile riequilibrio volto tanto alla concertazione delle modalità di autoregolamentazione privata quanto alla restituzione della centralità a un principio cardine della civiltà giuridica occidentale: ovvero, la libertà di coscienza e di religione considerata quale fondamento irrinunciabile di ogni ordine sociale autenticamente plurale[40]. Peraltro, a voler ritenere diversamente, qualora la libertà religiosa venisse considerata alla stregua di una variabile dipendente dalle strategie commerciali delle *big tech*, verrebbe compromessa la stessa sopravvivenza del pluralismo, con la diretta e immediata conseguenza di ridurre lo spazio digitale a un orizzonte privo di senso e incapace di riflettere la complessità della dimensione sociologica dell'appartenenza confessionale[41]. Detto

artificiale, F. Balsamo, *La tutela del diritto di libertà religiosa nell'era dell'intelligenza artificiale*, Cosenza, 2025.

[38] Effettivamente, dal punto di vista potere pubblico-potere privato, è stato giustamente osservato che «La co-regolazione non implica affatto di dover porre sul medesimo identico piano i poteri pubblici e i poteri privati differente, infatti, è, anzitutto e soprattutto, il fine da essi perseguito: mentre i primi sono istituzionalmente preordinati a curare l'interesse pubblico (cura che costituisce, al fondo, l'essenza e la giustificazione della loro stessa istituzione), i secondi sono legittimamente dediti al conseguimento del proprio interesse egoistico», L. Ricci, *Per una nuova teorica della regolazione "forte" delle piattaforme digitali tra (necessario) intervento pubblico e tutela (necessaria) della libertà di espressione*, in questa *Rivista*, numero speciale, 2024, 258.

[39] I pericoli che si profilano sono variegati, «dalla manipolazione delle reti sociali a uso politico, all'assenza di piena responsabilità da parte degli intermediari, fino al trionfo della governance privata, senza che alcuno strumento giuridico potesse anche soltanto impensierire la condotta delle piattaforme di turno», A. Renda, *L'Unione europea e l'insostenibile leggerezza del* Web, in *Rivista della regolazione dei mercati*, 1, 2021, 7 ss.

[40] Cfr. per tutti, G. Dalla Torre, *Libertà religiosa e secolarismo*, in *Stato, Chiese e pluralismo confessionale*, 10, 2018, 1 ss.; P.A. d'Avack, *Trattato di diritto ecclesiastico italiano*. Parte generale, 2ª ed., Milano, 1978, 415 ss.

[41] Sotto il profilo squisitamente giuridico, si è correttamente osservato che «La *lex digitalis*, ispirata all'efficientismo tecnico e modellata sugli interessi delle piattaforme, ha una dimensione teleologica autonoma, potenzialmente antagonista al valore della persona

altrimenti, un dialogo strutturato tra piattaforme digitali e fedi religiose, mediato da soggetti pubblici istituzionali, può produrre un incremento qualitativo della densità etica insita nei codici di condotta che regolano la vita *online*, disancorando le *policies* da una prospettiva eminentemente funzionale e dunque incapace di contemplare la profondità antropologica che pure connota l'esperienza digitale.
A scanso di equivoci occorre preliminarmente fugare ogni dubbio: incorporare la visuale "religiosa" nelle *policies* non significa cedere a una eteronomia confessionale, ma piuttosto arricchire la dimensione regolativa privata con fondamenti etici e trans-storici, capaci di orientare le decisioni delle *social media platforms* in scenari delicati in cui l'appartenenza confessionale degli utenti possiede ancora un peso specifico rilevante: basti pensare, solo per fare qualche esempio, all'*hate speech*, alla tutela dei minori e alle (presunte) dinamiche *online* di manipolazione delle coscienze. In tal senso, dunque, la partecipazione delle istituzioni religiose può contribuire a colmare il divario tra l'efficientismo tecnico-giuridico proprio dell'autoregolamentazione privata con la sensibilità delle comunità globali che vivono gli spazi digitali. Tuttavia, ancor prima di addentrarsi nello scandaglio degli strumenti giuridici messi a disposizione dal legislatore europeo, occorre forse domandarsi perché proprio le confessioni, e loro articolazione operative, possono essere una risorsa impareggiabile per la gestione della pluridiversità *online*.

3. L'eccedenza positiva del fenomeno religioso associato nei processi di *governance* digitale

L'analisi dell'incidenza delle istituzioni confessionali nella *governance* digitale non può prescindere da una considerazione storica, poiché proprio la lunga esperienza maturata dalle religioni nella gestione della complessità sociale[42] costituisce la base sulla quale fondare una loro possibile legittimazione nel *cyberspazio*. Infatti, le tradizioni religiose, attraverso secoli di sedimentazione giuridico-normativa, hanno fornito un repertorio di principi etico-morali poi trasfusi in strumenti concreti di regolazione dei conflitti, modelli di mediazione fra interessi contrapposti e forme di organizzazione

umana e alle modalità di funzionamento dei sistemi democratici», C. Caruso*, Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, cit., 553.

[42] Una complessità che dipende dal numero dei soggetti che compongono il sistema sociale, dall'articolazione delle regole e delle istituzioni che ne presidiano il funzionamento, dalla pluralità dei ruoli, delle culture, delle condizioni economiche e dei rapporti di potere che lo attraversano e, infine, come tutte queste parti interagiscono tra loro. Cfr. a questo proposito, T. Whalen, *Complexity, Society and Social Transactions. Developing a Comprehensive Social Theory*, Londra, 2018.

comunitaria che hanno plasmato interi ordinamenti giuridici: e ciò sorprendentemente, se calato in prospettiva diacronica, è avvenuto a tutte le latitudini[43]. Chiese, comunità e istituzioni spiritual-religiose in senso lato oltre a custodire gelosamente verità dottrinali e precetti dogmatici hanno altresì agito come soggetti di diritto capaci di produrre norme, di regolare la vita dei consociati mediante l'elaborazione di articolati sistemi che hanno influenzato la giurisprudenza, la legislazione e la prassi amministrativa degli Stati nazionali[44]. Trasporre questa funzione "socialmente accreditata" nello spazio digitale significa riconoscere che tali soggetti possono contribuire alla definizione di *policies* non tanto per difendere i propri "interessi" di parte ma, soprattutto, per arricchire l'ecosistema virtuale con un patrimonio di competenze variegato, idoneo a preservare – se messo oculatamente a frutto – la coesione sociale e il pluralismo *online*[45].

Questo portato storico, lungi dall'essere una mera testimonianza di un passato ormai definitivamente tramontato, rappresenta un'inestimabile ricchezza per affrontare le sfide del presente: infatti, le istituzioni religiose hanno fronteggiato momenti di conflitto e proficue collaborazioni con l'autorità civile, sanguinose guerre intestine, processi di secolarizzazione d'intensità variabile, confronti (e scontri) con regimi assolutistici e con ordinamenti democratici[46], sviluppando un'intrinseca elasticità che consente loro di adattarsi a contesti mutevoli senza tuttavia rinunciare al nucleo essenziale del proprio messaggio. Tale capacità di "resilienza istituzionale", tradotta oggi nel complesso rapporto con le grandi infrastrutture *social*, potrebbe consentire di proporre modelli alternativi di *governance*, in cui la logica dell'efficienza tecnica non obliteri (o, ancor peggio, soppianti) la tutela dei diritti fondamentali e la salvaguardia delle identità culturali[47].

---

[43] Pur senza esaurire la complessità del tema, cfr. G. Guerra, *L'umano e la legge: una teologia politica dell'ebraismo*, in *Democrazia e diritto*, 3-4, 2008, 1 ss.; M. Campanini, *Islam e politica*, Bologna, 1999; Id., *Ideologia e politica nell'Islam*, Bologna, 2008; K. Adeney, *Hindu Nationalists and Federal Structures in an Era of Regionalism*, in Ead. - L. Sáez (eds.) *Coalition Politics and Hindu Nationalism*, New York, 2005, 97 ss. Per una visione sinottica tra varie appartenenze confessionali rispetto all'influenza della matrice religiosa nella costruzione della comunità politica, anche in prospettiva diacronica, si rinvia ai contributi contenuti in J. Haynes (ed.), *Routledge Handbook of Religion and Politics*, Londra, 2023.

[44] Relativamente al cristianesimo, per tutti si rinvia a J. Le Goff, *L'imaginaire médiéval*, Parigi, 1985. Da visuale prospettica del giurista, si veda l'insuperato studio di F. Calasso, *L'unità giuridica dell'Europa*, Soveria Mannelli, 1985, 142 ss.

[45] Sul punto si vedano le lucide considerazioni di C. Sunstein, #*Republic: Divided Democracy in the Age of Social Media*, Princeton, 2017.

[46] Ancora una volta, relativamente al cristianesimo in Europa, il rimando è d'obbligo a J. Le Goff, *La civilisation de l'Occident médiéval*, Parigi, 1964.

[47] Tali possibili derive sono state illustrate da A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 63 ss.

Gli aggregati confessionali hanno inoltre la possibilità di influenzare positivamente una nuova cultura digitale attraverso la formulazione di messaggi che non si limitino a aderire acriticamente alle logiche commerciali, ma che sappiano offrire ai propri fedeli – ma, pure, alla società civile – una prassi discorsiva alternativa. Nel solco di queste considerazioni, le istituzioni religiose possono mostrare modalità diverse di abitare il *cyberspazio*, sforzandosi di non cedere all'immediatezza e alla superficialità (nonché, talvolta, all'aggressività) che spesso caratterizzano i flussi comunicativi online[48]: potrebbero, cioè, proporre narrazioni che valorizzino il rispetto, la solidarietà e la cura reciproca, contribuendo così a materializzare un umanesimo digitale che, al di là di roboanti retoriche, diviene una concreta pratica di convivenza sulle piattaforme *social*[49].

Ulteriormente, i collettivi religiosi spesso si caratterizzano per una vocazione intrinsecamente transazionale: a differenza, dunque, di altre realtà *lato sensu* associative presenti nella società civile, essi potrebbero contribuire proattivamente, qualora "incorporati" in processi decisionali di ampio respiro (come quelli per l'elaborazione di *standards* e *policies*), nel raccogliere esigenze e istanze di un numero cospicuo di soggetti-utenti. Di più, proprio in forza della loro natura (spesso) universalistica, essi sono attori di primaria rilevanza nella costruzione di reti globali che travalicano i confini geografici e culturali, in grado dunque di offrire un paradigma di *governance* cooperativa multilivello che potrebbe influenzare le dinamiche digitali ben oltre la cerchia dei fedeli che rappresentano[50]. In un contesto in cui il potere delle *big tech* si esercita a livello planetario[51], la voce concertata degli ag-

[48] Tale possibile sviluppo si potrebbe innestare proprio sulla base di meccanismi normo-giuridici endoconfessionali, i quali – vista la natura dei diritti a base religiosa – incidono direttamente sulla coscienza dei fedeli. Quanto alla Chiesa cattolica, da una prospettiva più ampia, circa la diffusione dell'AI si rinvia alla *Antiqua et nova* (Nota sul rapporto tra intelligenza artificiale e intelligenza umana) del Dicastero per la dottrina della fede e del dicastero per la cultura e l'educazione (28 gennaio 2025). Ancora prima, cfr. Dicastero per la dottrina della fede, *Dichiarazione* Dignitas infinita *circa la dignità umana*, 2 aprile 2024, n. 61, in cui si specifica che «il progresso delle tecnologie digitali, che pure offrono molte possibilità per promuovere la dignità umana, inclina sempre più alla creazione di un mondo in cui crescono lo sfruttamento, l'esclusione e la violenza, che possono arrivare a ledere la dignità della persona umana».

[49] Sull'ipotesi di una co-regolamentazione si veda P. Bonini, *L'autoregolamentazione dei principali Social Network. Una prima ricognizione delle regole sui contenuti politici*, in *Federalismi*, 11, 2020, 264 ss.

[50] Cfr. sulla *networked governance*, D. Levi-Faur*, Regulatory networks and regulatory agencification: Towards a single European regulatory space*, in *Journal of European Public Policy*, 6, 2011, 810 ss.; L. Lim, *Networked governance: Why it is different and how it can* work, in *Ethos*, 14, 2011, 19 ss.

[51] Sul punto è da segnalare la difficoltà di individuare esattamente quali siano i centri che effettivamente detengono il potere decisionale in seno a grandi corporate, quali sono le piattaforme *social*. In questo senso si è correttamente parlato di neointermediazione, in

gregati confessionali può costituire un contrappeso significativo, capace di influenzare tanto il dibattito politico quanto le scelte regolative delle stesse *corporates* proprietarie dei *social:* in altre parole, si potrebbero individuare vere e proprie forme di *advocacy* indirizzate non solo nei confronti dei decisori politici ma altresì pure dei soggetti privati[52]. Le diverse appartenenze religiose, se considerate nella loro peculiare specificità storico-giuridica e nella funzione di agenti interpretativi di principi assiologici che hanno forgiato la nostra società[53], possono assumere una significativa incidenza nei processi di elaborazione, miglioramento e revisione delle *policies*, servendosi dei dispositivi normativi attualmente messi a disposizione dal legislatore sovranazionale. In aggiunta a quanto già rapidamente rassegnato, infatti, tali enti, a differenza di altre componenti della compagine sociale, recano con sé una stratificazione secolare, se non millenaria, di "memoria normativa" e una prassi consolidata di gestione della pluralità valoriale. Tale "competenza" storicamente sedimentata si rivela particolarmente preziosa in un ecosistema digitale segnato da contrasti simbolici ad alta intensità, da divergenze (di varia matrice) radicalizzate e da dinamiche di polarizzazione delle idee a tutti evidente (*echo chambers*, *filter bubbles*)[54].

Ne consegue che qualunque appartenenza confessionale "istituzionalizzata", oltre che essere portatrice di interessi settoriali e, dunque particolari, può e deve essere considerata come depositaria di un *quid pluris* integrativo rispetto alle cornici giuridiche positive, capace di offrire alle piattaforme digitali strumenti di mediazione interculturale e regolamentazione inclusiva, peraltro in perfetta consonanza con i principi sanciti dal diritto internazionale attualmente vigente[55]. Ci si potrebbe chiedere, a ragione, di quali

---

cui «Le grandi piattaforme e i grandi siti emergono come nuovi intermediari di un enorme flusso di informazioni: selezionano gli argomenti più importanti (*agenda setting*) e decidono in maniera autonoma cosa è più opportuno venga diffuso e pubblicizzato. I media digitali superano l'idea di intermediario come è stata intesa finora (disintermediazione), ma non la superano in assoluto, anzi propongono nuove forme di mediazione (neointermediazione)». Peraltro, «le piattaforme svolgono a tutti gli effetti un ruolo di *agenda setting e* quindi di quarto potere, è conseguente che abbiano delle responsabilità importanti nei confronti dell'opinione pubblica democratica», G. Giacomini, *Verso la neointermediazione. Il potere delle grandi piattaforme digitali e la sfera pubblica*, in *Iride*, 2018, 476.

[52] Una dichiarazione congiunta di più confessioni o enti, ad esempio, volta a sottolineare la centralità del pluralismo religioso nello spazio virtuale, avrebbe un peso politico e simbolico non di poco momento, aprendo la strada a forme di "pressione" coordinate, in grado di riequilibrare rapporti di forza altrimenti sbilanciati.

[53] Sulla persistenza della religione come "risorsa morale" utile alla convivenza democratica, si veda diffusamente J. Habermas, *Between naturalism and religion: philosophical essays*, Cambridge, 2008.

[54] Cfr. sul punto gli studi di E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Londra, 2011.

[55] Come auspicato da H. Bedford-Strohm, *The Ethical Challenges of the Digital Age. Between*

strumenti normativi servirsi in un contesto che – almeno in apparenza – pare aver delegato a soggetti privati il ruolo di (auto)regolamentazione dei diritti sui *social*[56]: una possibile risposta, benché parziale, può essere rintracciata nel diritto dell'Unione europea.

4. Le potenzialità (ancora inespresse) offerte dal diritto dell'Unione europea

Nella traiettoria già descritta, irrompe sulla scena il plesso normativo delineato dall'Unione europea che negli ultimi anni ha dato prova, *ratione materiae*, di implementare molteplici tentativi di perequazione del potere egemonico determinatosi dall'oligopolio imposto dai principali (e più frequentati) *social media*[57]. Il tema può essere affrontato sotto una duplice visuale prospettica: in primo luogo, occorre individuare i presupposti normativi nel perimetro dei quali muoversi e, conseguentemente, verificare le ricadute operative già in atto nella loro dimensione (ancora, invero, potenziale) di tutela dei diritti fondamentali degli utenti.
A riguardo del primo profilo, il Regolamento (UE) 2022/2065 – *Digital Services Act* (DSA), ha introdotto un sistema innovativo di obblighi per i fornitori di servizi digitali, prevedendo strumenti di vigilanza e meccanismi di *accountability*[58] che mirano a bilanciare il potere delle piattaforme, "sintonizzandolo" con il *frame* giuridico euro-unionale[59]. In verità, il DSA

Promises of Salvation and Prophecies of Doom, in *The Ecumenical Review*, 2, 2020, 167 ss. Utilizza specificatamente il termine «algoritmo interculturale», I. Valenzi, *Libertà religiosa e intelligenza artificiale: prime* considerazioni, in *Quaderni di diritto e politica ecclesiastica*, 2, 2020, 353 ss.

[56] In dottrina è si è parlato di «una chiara torsione dell'idea di sovranità, che cessa di configurarsi come concetto riconducibile in toto allo spazio pubblico, allo Stato, per diventare invece oggetto di una parziale "condivisione" tra pubblico e privato, se non di una vera e propria "cessione" da parte delle autorità statali a favore del settore ICT», A. Vedaschi, *Intelligenza artificiale e misure antiterrorismo alla prova del diritto costituzionale*, in Liber amicorum *per Pasquale Costanzo*, I, cit., 502.

[57] A questo proposito, si veda E. Bietti, *A genealogy of digital platform regulation*, in *Georgetown Law Technology Review*, 1, 2023, 1 ss.

[58] Cfr. in particolare, G. Giannone Codiglione, *Il contratto dell'utente con il* social network, in *I poteri privati delle piattaforme e le nuove frontiere della privacy*, cit., 334 ss.

[59] Segnatamente, cfr. M.A. Astone, *Digital Services act e nuovo quadro di esenzione dalla responsabilità dei prestatori di servizi intermediari: quali prospettive?*, in *Contratto e Impr*esa, 2022, 1050, la quale osserva che «l'obiettivo è quello di intervenire sulla governance di internet, per tutelare gli utenti e per creare un mercato digitale articolato intorno a due linee di azione: l'inserimento dei servizi resi dalle piattaforme on line all'interno della più generale categoria dei servizi di hosting; la sicurezza della tecnologia e la protezione della persona umana da contenuti illegali e dannosi. L'obiettivo è, in particolare, quello di porre le basi

è a tutti gli effetti «una scelta politica strategica e, in certa misura, persino identitaria, in quanto contribuisce a delineare, in maniera ancora più netta, l'identità – dal punto di vista non solo giuridico ma, in senso più lato, assiologico – dell'Unione europea»: questo dato deve essere rimarcato, ed è evidente la consapevolezza del legislatore sovranazionale di intervenire in «una partita fondamentale per la democrazia e lo stato di diritto, che non può essere lasciata al *laissez faire* dei rapporti (di forza) del mercato, alle magnifiche sorti [...] della tecnica, né alla pretesa autonomia della logica negoziale»[60].

In questa sede non è opportuno addentrarsi nella complessa normativa citata (e, soprattutto, nelle plurime ripercussioni sul nostro ordinamento)[61], ma basti qui ricordare che il quadro regolatorio europeo conferma la rilevanza del contributo di attori collettivi dotati di *expertise* nella *governance*

per mercati equi e contendibili, come si evince dalla considerazione dell'altro Regolamento, quello sui mercati digitali, strettamente correlato al Digital services act, che nei servizi resi dalle piattaforme ricomprende quelli che presuppongono un ruolo attivo del gestore della piattaforma (per esempio motori di ricerca online; servizi di social network online; servizi di piattaforma per la condivisione di video). Ma soprattutto il DSA introduce uno statuto normativo più gravoso per le imprese di grandi dimensioni che gestiscono piattaforme […]», le quali sono sottoposte a «stringenti obblighi riguardanti sia il trattamento dei dati personali, considerato che le loro dimensioni imprenditoriali e territoriali facilitano la trasmissione rapida e la circolazione delle informazioni, sia la prevenzione di squilibri contrattuali nei confronti degli utenti finali dei servizi di piattaforma di base. A tali obblighi si aggiungono pure divieti di pratiche sleali e di condizioni inique a presidio della concorrenza e della protezione del mercato digitale. Da tale statuto normativo emerge l'avvio di una nuova strategia. Infatti la tecnica utilizzata non è più fondata sulla riparazione, come nella direttiva 2000/31/CE, piuttosto sulla prevenzione e sulla responsabilizzazione dei fornitori di piattaforme on line; ciò si realizza con la previsione di obblighi di predisposizione di codici di condotta e della sottoscrizione di accordi di autoregolamentazione e di co-regolamentazione per lo svolgimento di una attività di moderazione dei contenuti, come già previsto dalla direttiva sui servizi media audiovisivi».

[60] F. Resta, *Le piattaforme e la visibilità del potere*, in *I poteri privati delle piattaforme e le nuove frontiere della privacy*, cit., 369. Sul concetto di identità europea, recentemente enucleato dalla Corte, si vedano le sentenze del 16 febbraio 2022 della Corte di giustizia dell'Unione europea, causa C-156/21 e C-157/21 *Ungheria c. Parlamento e Consiglio; Polonia c. Parlamento e Consiglio* (C-157/21, §§ 143-145 e C-156/21, §§ 125-127), in cui si afferma apertamente che «i valori contenuti nell'articolo 2 TUE sono stati identificati e sono condivisi dagli Stati membri. Essi definiscono l'identità stessa dell'Unione quale ordinamento giuridico comune. Pertanto, l'Unione deve essere in grado, nei limiti delle sue attribuzioni previste dai trattati, di difendere detti valori». Sul punto, ancor prima, si rinvia diffusamente a L. S. Rossi*, Il valore giuridico dei valori. L'Articolo 2 TUE: relazioni con altre disposizioni del diritto primario dell'UE e rimedi giurisdizionali*, in *Federalismi*, 19, 2020, I ss.

[61] Cfr., di recente, C. Caruso, *Il tempo delle istituzioni di libertà. Piattaforme digitali, disinformazione e discorso pubblico europeo*, in *Quaderni costituzionali*, 3, 2023, 543 ss.; F. Casolari, *Il "Digital Services Act" e la costituzionalizzazione dello spazio digitale europeo*, in *Giurisprudenza italiana*, 2, 2024, 462 ss.

digitale, di concerto con le istituzioni europee[62].
In particolare, l'art. 45 del DSA, valorizza e disciplina i meccanismi di *notice and action* e l'adozione di *codes of conduct* fondati sul coinvolgimento delle cosiddette parti interessate (*stakeholder engagement*)[63], includendo dunque potenzialmente anche le comunità religiose come portatrici di istanze peculiari nella tutela dei diritti fondamentali *online*. La modalità operativa attualmente prevista dall'art. 45 del DSA[64] enuclea l'elaborazione di codici di condotta prodotti dalla Commissione ma non direttamente imposti ai soggetti privati: questi ultimi però, qualora vi aderiscano, si impegnano a rispettare gli impegni ivi delineati. Specificatamente, allorché necessario, la Commissione – ai sensi dell'art. 45, par. 2, del DSA – coinvolge le «organizzazioni della società civile e altre parti interessate, a partecipare all'elaborazione dei codici di condotta»[65]. Proprio tali interlocuzioni – intese come forme strutturate di dialogo tra soggetti istituzionali, piattaforme e *stakeholders* – potrebbero costituire, nell'immediato, un primo passo concreto verso l'inclusione della compagine religiosa nei processi di elaborazione e applicazione di strumenti di *soft law* nell'ecosistema digitale[66]. In questa prospettiva, il loro coinvolgimento configurerebbe un contributo sostanziale all'elaborazione di codici di condotta settoriali, alla definizione di *standard* etici condivisi[67] e, da una prospettiva più ampia, all'attuazione

[62] Dalla prospettiva ecclesiasticistica, si vedano gli studi di M. Palazzo, *Prime osservazioni sul rapporto tra libertà religiosa e intelligenza artificiale, a partire dall'*AI Act, in questa *Rivista*, numero speciale 2024, 187 ss.; Ead., *La tutela della libertà di pensiero, coscienza e religione nel nuovo Regolamento europeo sull'Intelligenza Artificiale. Prime considerazioni*, in *Quaderni di diritto e politica ecclesiastica*, 2, 2024, 647 ss.

[63] Cfr. P.D. Algica, *Institutional and stakeholder mapping: Frameworks for policy analysis and institutional change*, in *Public Organization Review*, 6, 2006, 79 ss.

[64] Il quale, «può rappresentare una valvola di sfogo atta a consentire implementazioni e miglioramenti relativi al rafforzamento delle tutele dei diritti fondamentali», F. Donà, *Libertà di manifestazione del pensiero* online *e* content moderation *dei nuovi poteri privati: rischi ed opportunità alla luce della nuova coregolazione euro-unitaria*, in questa *Rivista*, 2, 2025, 254.

[65] In argomento si veda R. Griffin, *Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns*, in *Technology and Regulation*, 2024, 167 ss.; M. Husovec, *The DSA as a Co-regulatory System,* in Id., *Principles of the Digital Services Act*, Oxford, 443 ss.

[66] In particolare, nell'adozione dei codici di condotta, R. Griffin, *Codes of Conduct in the Digital Services Act: Functions, Benefits & Concerns*, cit., 177, delinea tre potenziali vantaggi: *«First, their concretising and remedial functions can introduce more specific norms and commitments to which platforms can be held accountable, while retaining flexibility. Second, their oversight and multistakeholder participation functions can develop institutional frameworks to realise accountability in practice. Finally, they can establish risk mitigation measures and commitments in areas which are underemphasised in the DSA, notably in platform design».* Focalizzandosi sul secondo dei tre vantaggi individuati sembra emergere un significativo spazio per i soggetti confessionali istituzionalizzati.

[67] Cfr. pure la *Recommendation on the Ethics of AI* (2021) dell'Organizzazione delle Nazioni

di pratiche di *stakeholder engagement* promosse sia dal Consiglio d'Europa[68] sia dall'Organizzazione per la Cooperazione e lo Sviluppo Economico[69]. Inoltre, la futura partecipazione confessionale a tali sedi di cooperazione multilaterale consentirebbe di profittare della loro peculiare esperienza nella mediazione interculturale e nella gestione dei conflitti valoriali, trasformando così la dimensione religiosa in una risorsa messa a disposizione della collettività virtuale[70]: ciò, peraltro, in perfetta corrispondenza di quanto suggellato dall'art. 17 del Trattato sul funzionamento dell'Unione europea[71]. Il meccanismo delineato dal *Digital Services Act* si concretizza, in coerenza con le consolidate prassi partecipative proprie dell'ordinamento dell'Unione europea, nello strumento della consultazione pubblica: in effetti, tale istituto rappresenta una delle principali modalità attraverso cui le istituzioni europee garantiscono l'inclusione e il coinvolgimento effettivo degli *stakeholders* nei processi di formazione e implementazione delle politiche comunitarie. Più precisamente, l'apertura di una *call* consente ai soggetti portatori di interessi qualificati – siano essi rappresentanti del settore privato, organizzazioni della società civile, enti pubblici, ecc. – di inoltrare una richiesta per essere formalmente interpellati al fine di esporre la propria prospettiva analitica e propositiva in relazione alla tematica oggetto della consultazione. Tale procedura, improntata ai principi di trasparenza, partecipazione e "responsabilità democratica", contribuisce a garantire che il processo decisionale europeo si fondi su un confronto aperto e pluralistico, nel quale le diverse posizioni vengano valutate alla luce di criteri di competenza, rilevanza e impatto sistemico[72]. A questo proposito, si

Unite per l'Educazione, la Scienza e la Cultura (UNESCO).

[68] Cfr. *Raccomandazione* CM/Rec (2022)13.

[69] Cfr. *Principles on Artificial Intelligence*, 2019.

[70] Si vedano, da un punto di vista più ampio di compartecipazione dei vari attori della società civile nei processi di "democratizzazione" delle piattaforme, R. Caplan, *Networked Platform Governance: The Construction of the Democratic Platform*, cit., 3451 ss.

[71] Il quale, come noto, recita: «L'Unione rispetta e non pregiudica lo status di cui le chiese e le associazioni o comunità religiose godono negli Stati membri in virtù del diritto nazionale. L'Unione rispetta ugualmente lo status di cui godono, in virtù del diritto nazionale, le organizzazioni filosofiche e non confessionali. Riconoscendone l'identità e il contributo specifico, l'Unione mantiene un dialogo aperto, trasparente e regolare con tali chiese e organizzazioni». Cfr., per tutti, M. Ventura, *L'articolo 17 TFUE come fondamento del diritto e della politica ecclesiastica dell'Unione europea*, in *Quaderni di diritto e politica ecclesiastica*, 2, 293 ss. Peraltro, nulla esclude che in prospettiva possano giocare un ruolo cruciale in questo frangente anche le organizzazioni filosofiche e non confessionali: cfr. sul punto S. Baldassare, *Contributo allo studio delle organizzazioni filosofiche e non confessionali nel diritto italiano e internazionale*, Pisa, 2023.

[72] Cfr. in particolare H.S. Wallace – A. R. Young, *Participation and policy-making in the European Union*, Oxford, 2023.

potrebbe verificare, in via eventuale ma verosimile, una moltiplicazione di domande anche da parte di istanti la cui confessionalità non sia pacifica e acclarata, il che porrebbe (anche) dinanzi al decisore politico sovranazionale l'annosa diatriba della qualificazione giuridica dei collettivi religiosi: rendendo palese la necessità urgente di approdare, sul punto controverso, a soluzione ragionevoli e condivise[73].

In aggiunta, un'analoga direzione è rinvenibile nella Raccomandazione CM/Rec(2022)13 del Consiglio d'Europa sulla responsabilità delle piattaforme digitali, la quale sottolinea l'esigenza, pur non prevedendo specifici interventi vincolanti, di una *multistakeholder governance* capace di integrare soggetti istituzionali e rappresentanti della società civile nella prevenzione dei discorsi d'odio e nella promozione di un dibattito pubblico pluralista[74].

Nella fase derivata, invero ancora embrionale, l'istituzione dell'*Appeals Centre Europe* rappresenta un esperimento che si prefigge l'ambizioso scopo di creare un contrappeso rispetto alla discrezionalità delle imprese tecnologiche nella fase di *content moderation* e, dunque, delle relative decisioni unilaterali (anche attraverso modalità di "giustizia *in house*" come l'*Oversight Board* di Meta)[75], offrendo agli utenti un canale terzo e imparziale che si occupi di analizzare la legittimità di provvedimenti dei *provider* ritenuti lesivi dei diritti del fruitore[76]. Le decisioni emesse, benché non vincolanti per le piattaforme, devono essere trattate in buona fede da queste ultime, ai sensi delle obbligazioni introdotte dal DSA, e possono essere da loro recepite con conseguente modifica dei provvedimenti originari: in questo frangente gli attori confessionali potrebbero favorire il buon funzionamento dell'*Appeals Centre Europe* con riguardo ai profili dell'orientamento etico-culturale e della sensibilizzazione alla legalità digitale. Specificatamente, l'attività delle comunità religiose può incidere positivamente sulla diffusione di una

[73] Il tema è ampio e non può essere ovviamente affrontato in questa sede. Ad ogni modo, relativamente all'ordinamento italiano, ci si permettere di rinviare a N. Tonti, *Il nuovo pluralismo religioso*, Bologna, 2025.

[74] Cfr. di recente, L. Corchia, *L'*hate speech. *Definizione e meccanismi di propagazione nei* social network, in *Sicurezza e scienze sociali*, 3, 2023, 38 ss.

[75] Alcune note critiche rispetto il funzionamento dell'*Oversight Board* sono state sviluppate da E. Douek, *The meta oversight board and the empty promise of legitimacy*, in *Harvard Journal of Law & Technology*, 1, 2019, 10 ss. Sia consentito il rinvio anche a N. Tonti, *La tutela della libertà religiosa sui social media. Il* pressure test *dell'*Oversight board: *la montagna ha partorito un topolino?*, in *JUS*, 5, 2022, 94 ss.

[76] Cfr. sull'organismo in questione L. Gradoni - P. Ortolani, *Moderation Made in Europe: A Look into the Future of Social Media Content Moderation Litigation*, in *VerfBlog*, 2024; B. Kira, *Regulatory intermediaries in content moderation*, in *Internet Policy Review*, 1, 2025, 1 ss. Si veda pure F. Casarosa, O*ut-of-court dispute settlement mechanisms for failures in content* moderation, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 3, 2023, 391 ss.

cultura giuridica dei diritti digitali, favorendo comportamenti conformi ai principi di correttezza, lealtà comunicativa e rispetto della libertà di espressione sanciti dalla Carta dei diritti fondamentali dell'Unione europea e, parallelamente, esse possono svolgere una funzione sussidiaria in chiave di mediazione culturale, operando come soggetti interposti tra i cittadini, le istituzioni politiche e i grandi agglomerati economico-finanziari operanti nel settore dei *social media*.

A ben vedere, se questi *tools* non verranno integrati da una partecipazione attiva dei soggetti della società civile, tra i quali appunto le organizzazioni religiose, il rischio è che la tutela approntata rimanga una formale proclamazione d'intenti, priva della profondità simbolica necessaria a garantire una protezione effettiva della libertà religiosa e di coscienza. In altre parole, occorre rafforzare la co-partecipazione integrativa delle istituzioni confessionali nei processi decisionali delle infrastutture digitali. Precisamente, a monte, è opportuno prevedere una gestione dei processi di formazione delle *policies* che non può non tenere in considerazione le voci degli attori confessionali, in quanto portatrici di interessi metaindividuali e trasversali che trascendono l'appartenenza dei singoli utenti. Il loro coinvolgimento, infatti, può essere una preziosa risorsa per individuare i limiti degli *standards* aziendali, per segnalare le distorsioni culturali insite nei sistemi di moderazione e, da ultimo, per proporre criteri di valutazione rispettosi della pluralità delle tradizioni cultuali. A valle, l'incidenza delle comunità religiose – come, pure, quello di altri soggetti portatori di interessi – è invece di cruciale rilevanza per l'emersione di eventuali discriminazioni attraverso mirati ricorsi all'*Appeals Centre Europe*, nonché ovviamente dinanzi alle giurisdizioni civili[77].

5. *Quo itur*?

Alla luce di quanto fin qui rammentato, il dialogo tra il diritto statuale, la regolazione sovranazionale, il ruolo delle piattaforme e il contributo delle istituzioni religiose non deve essere concepito come una sovrapposizione caotica di competenze quanto piuttosto come un intreccio armonico in cui ciascun attore condivide la propria quiddità. In breve: lo Stato nazionale deve primariamente offrire rimedi nel caso in cui si compiano gravi violazioni *online*; l'Unione europea, attraverso la sua regolamenta-

[77] Relativamente alla tutela dei diritti nello spazio digitale e sul ruolo sempre più centrale della giurisprudenza, si vedano le preziose pagine di O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Oxford, 2021. Sempre lo stesso Autore, più di recente, ritorna sull'argomento in Id., *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, 569 ss., spec. 580-581.

zione, interviene nell'ambito delle competenze attribuitele offrendo dispositivi normativi capaci di innalzare il livello di tutela degli utenti; le piattaforme consentono l'innovazione tecnologica e mettono a disposizione l'indispensabile *know-how* e, da ultimo, le istituzioni spiritual-religiose devono dimostrare la capacità di mediazione valoriale (la quale trova già concretizzazione nella vita delle comunità "*off line*"), intesa come fattore propulsivo e volano per la creazione di una società virtuale inclusiva. Solo attraverso questa collaborazione sarà possibile per un verso evitare che la cittadinanza digitale si trasformi in un'esperienza frammentata, dominata da decisioni automatizzate insensibili al peso simbolico e socioculturale delle pratiche religiose; per l'altro, garantire che il *cyberspazio* divenga un ambito in cui i diritti fondamentali non siano sacrificati sull'altare della tecnica, ma trovino per converso un nuovo slancio attraverso il contributo di tutti i soggetti che vivono quotidianamente l'agorà digitale[78]. In effetti, la prospettiva che si apre nel futuro immediato impone di concepire i *social media* come un laboratorio di giuridicità in continua evoluzione. Giova evidenziare che in questo "cantiere aperto" la partecipazione dei collettivi religiosi non può essere ridotta a rivendicazione difensiva di prerogative confessionali ma piuttosto deve configurarsi come contributo attivo e qualificato alla costruzione di un ordine digitale rispettoso della dignità umana e della pluralità valoriale, anche di quella propriamente religiosa: in cui, cioè, i diritti della persona, che pure nella *virtual life* pretendono di essere salvaguardati, «sono letti alla luce di una parola che eleva l'uomo sopra la soglia della materialità, lo innalza al rango di persona che chiede, merita di più»[79].

Solo così, infatti, si può giustificare la compartecipazione – in sinergia con altri *stakeholders* – di soggetti confessionali nei processi decisionali che presiedono la definizione delle *policies* delle piattaforme: tale sforzo potrà avvenire attraverso l'elaborazione di proposte, la presentazione di osservazioni e la partecipazione a tavoli di confronto congiunti che vedano partecipi i legislatori, le aziende tecnologiche e i rappresentanti della società civile. In concreto, sfruttando i meccanismi previsti del DSA che stabiliscono i termini dell'intervento (quantomai auspicabile) di attori della società civile nella formazione dei codici di condotta, si potrebbe in prospettiva costruire un solido argine alle forme di auto-normazione di soggetti privati, proprietari dei *social media*. Occorre, cioè, profilare un modello di *governance*

[78] Affinché vengano preservati i principi costituzionali, quali dispositivi «di civilizzazione dei rapporti umani», G. Ferrara, *Conclusioni*, in M. Ruotolo (a cura di), *La Costituzione ha 60 anni*, Napoli, 2008, 377.

[79] C. Cardia, *Il fondamento etico del diritto*, in *Stato, Chiese e pluralismo confessionale*, Rivista telematica (*statoechiese.it),* 7, 2021, 31.

multilivello[80], nel quale le confessioni religiose siano chiamate a intervenire attraverso strumenti consultivi e, in determinate circostanze[81], mediante procedure partecipative formalizzate, così da incidere realmente sulle decisioni riguardanti la moderazione dei contenuti, la definizione dei criteri di accesso e le modalità di utilizzo dei *social networks*. Fuori di dubbio, il DSA non costituirà una panacea capace di livellare disequilibri nei rapporti di potere sulle piattaforme *social* a tutti ormai evidenti: esemplificativamente, il *Recital 90* del DSA prevede che le *Very Large Online Platforms and Search Engine*s dovrebbero coinvolgere esperti indipendenti e la società civile nel processo di valutazione e mitigazione dei rischi sistemici[82]. Tuttavia, tale formulazione non dettaglia le modalità designate per identificare tali soggetti, peraltro non precisando le forme che devono essere utilizzate per la loro consultazione né individuando quali siano esattamente i rischi sistemici da prevenire. È comunque chiara la potenzialità insista in questi strumenti: una simile architettura istituzionale, qualora venga davvero attuata, avrebbe il pregio di fornire contrappesi a un sistema oggi fortemente asimmetrico, in cui i colossi tecnologici detengono una potestà normativa priva di controlli adeguati.

In conclusione, qualora si portassero a realizzazione (e potenziassero) gli strumenti giuridici già a disposizione, il governo delle interazioni sulle piattaforme *social* smetterà di essere un luogo di confinamento dell'appartenenza religiosa per diventare il palcoscenico di una nuova stagione del pluralismo confessionale. Effettivamente, nel solco delle considerazioni già rassegnate, le comunità di fede non solo garantiranno la propria sopravvivenza, ma saranno in grado di contribuire attivamente alla costruzione di un rinnovato umanesimo digitale, restituendo alla dimensione virtuale quella densità simbolica e culturale senza la quale ogni società, neppure quella digitale, non può dirsi pienamente libera.

---

[80] Il concetto, sviluppato sulla dicotomia pubblico-privato ma qui potenzialmente trasponibile, è stato mutuato da G. D. Finocchiaro, *Sovranità digitale*, cit., 825 ss. In particolare, l'Autrice sottolinea incisivamente che «Siamo in una fase di cambiamento, e si va verso un sistema sempre più multilivello. Se dunque la materia da regolare è divenuta di interesse per l'intera società e riveste una rilevanza politica, è necessario che la politica si riappropri del proprio ruolo [...]: siamo davanti ad una matassa da dipanare per capire quali regole si devono applicare e in che modo possono essere coordinate fra di loro. A ben vedere, si possono individuare tanti livelli di regole che, naturalmente, costituiscono altrettante diverse espressioni di potere. Non c'è e non ci sarà mai "il" legislatore del digitale», 825-826.

[81] In particolare, ci si riferisce agli art. 45 ss. del *Digital Service Act* già precedentemente richiamato.

[82] Alcune condivisibili perplessità sono state avanzate da T.E. Frosini, *L'ordine giuridico del digitale*, cit., 36-65.

Nico Tonti

Abstract

L'elaborato esamina la riconfigurazione dei rapporti di potere nell'ecosistema digitale nel quale le piattaforme social assumono sempre di più la fisionomia di veri e propri sistemi normativi, incidendo in modo pervasivo sull'effettività dei diritti fondamentali, segnatamente sulla libertà religiosa. Il saggio propone di riconoscere alle istituzioni confessionali una funzione co-legittimante e co-regolativa nella formazione della *lex digitalis*, quale possibile contrappeso all'oligopolio regolativo delle *big tech*. In tale prospettiva, le confessioni religiose, portatrici di una sedimentata tradizione storica di normazione simbolico-valoriale, sono delineate come interpreti qualificati di un'auspicabile *governance* multilivello, capaci cioè di reimmettere nel cyberspazio i presupposti socio-antropologici del diritto. Il *Digital Services Act*, con i suoi meccanismi di *stakeholder engagement*, viene così interpretato quale strumento giuridico idoneo a istituzionalizzare la loro partecipazione, restituendo alla sfera virtuale uno spessore semantico coerente con nuovo l'umanesimo digitale.

The paper examines the reshaping of power relations in the digital ecosystem, where social media platforms are increasingly taking on the characteristics of actual regulatory systems, having a widespread impact on the enforceability of fundamental rights, particularly religious freedom. The essay proposes that confessional institutions be recognised as having a co-legitimising and co-regulatory function in the formation of lex digitalis, as a counterweight to the regulatory oligopoly of big tech. In this perspective, religious institutions, as bearers of a long-standing historical tradition of symbolic and value-based regulation, are outlined as qualified actors in a possible multi-level governance, capable of reintroducing the socio-anthropological premises of law into cyberspace. The Digital Services Act, with its stakeholder engagement mechanisms, is thus interpreted as a legal instrument suitable for formalising their participation, restoring to the digital sphere an density of values consistent with the new "digital" humanism.

Keywords

lex digitalis – feedom of religion – private self-regulation – Digital Services Act – religious legitimacy

Chiesa cattolica e cyberspazio: verso una nuova dimensione per l'esercizio della *governance* ecclesiale*

Federico Gravino

Sommario

1. Dal digitale all'Intelligenza Artificiale: la missione della Chiesa nei nuovi contesti di fede. – 2. La funzione di insegnare nella dimensione *online* – 3. Sacramenti e sacramentali in rete tra divieti, rischi e opportunità. – 4. Governare con il digitale: il *munus regendi* nell'infosfera. – 5. La salvezza delle anime nella realtà digitale.

1. Dal digitale all'Intelligenza Artificiale: la missione della Chiesa nei nuovi contesti di fede

Esiste una Chiesa cattolica anche nella realtà digitale[1]. Questo dato supera ormai gli interrogativi sollevati dal magistero[2] e dalla dottrina[3] circa i limi-

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

[1] Per un approfondimento si rinvia diffusamente a F. Bolzetta, *La Chiesa nel digitale. Strumenti e proposte*, Todi, 2022.

[2] Pio XII, Lettera enciclica *Miranda Prorsus. Cinema, radio e televisione*, 08 settembre 1957, in *AAS*, 49, 1957, 765 ss.; Pontificio Consiglio delle Comunicazioni Sociali, *Etica in Internet*, 22 febbraio 2002, il cui testo integrale è consultabile sul sito *vatican.va*; Pontificio Consiglio delle Comunicazioni Sociali, Istruzione pastorale *Aetatis novae* sulle Comunicazioni Sociali nel 20° Anniversario della *Communio et Progressio*, 22 febbraio 1992, in *Enchiridium Varicanum*, 13, nn. 1002-1105; Giovanni Paolo II, Messaggio per la XXXIX Giornata Mondiale delle Comunicazioni Sociali "*I mezzi della comunicazione sociale: al servizio della comprensione tra i popoli*", 24 gennaio 2005, il cui testo integrale è consultabile sul sito *vatican.va*; Benedetto XVI, Messaggio per la XLIII Giornata Mondiale delle Comunicazioni Sociali "*Nuove tecnologie, nuove relazioni. Promuovere una cultura di rispetto, di dialogo, di amicizia*", 24 gennaio 2009, il cui testo integrale è consultabile sul sito *vatican.va*; Francesco, Messaggio per la XLVIII Giornata Mondiale delle Comunicazioni Sociali "*Comunicazione al servizio di un'autentica cultura dell'incontro*", 24 gennaio 2014, il cui testo integrale è consultabile sul sito *vatican.va*; Francesco, Messaggio per la 53ma Giornata Mondiale delle Comunicazioni Sociali "*Siamo membra gli uni degli altri*" (Ef. 4,25). *Dalle social network comunities alla comunità umana*, 24 gennaio 2019, il cui testo integrale è consultabile sul sito *vatican.va*.

[3] *Ex plurimis*, J.P. Foley, *Chiesa e Internet*, Città del Vaticano, 2002, 43 ss.; V. Grienti, *Chiesa e*

ti[4], i rischi[5] e le opportunità[6] di una connessione tra comunità ecclesiale e sviluppo tecnologico[7].

Tale intersezione è monitorata dalla Chiesa istituzione per la quale, se è vero che «la scienza e la tecnologia manifestano la qualità fondamentalmente relazionale dell'intelligenza umana: sono prodotti straordinari del suo potenziale creativo»[8], è altrettanto vero che «l'immensa espansione della tecnologia deve essere accompagnata da un'adeguata formazione alla responsabilità per il suo sviluppo»[9]. Perché i progressi tecnologici (in questa sede intesi anche come innovazioni digitali), siano quindi considerati tali, è necessario che migliorino la qualità di vita di tutta l'umanità[10].

È ben chiaro l'orientamento secondo cui «le meravigliose invenzioni tecniche che più direttamente riguardano le facoltà spirituali dell'uomo e che hanno offerto nuove possibilità di comunicare, con massima facilità, ogni

Internet. Messaggio evangelico e cultura digitale, Firenze, 2010, 23 ss.; A. Silvestri, *La luce e la rete. Comunicare la fede nel Web*, Torino, 2010, 20 ss.; R. Marchetti, *La Chiesa in Internet. La sfida dei media digitali*, Roma, 2015, 28 ss.; S. Valentan, *I tre Papi e la necessità degli strumenti di comunicazione sociale nella Chiesa*, in *Theological Quarterly*, 4, 2019, 1075 ss.; A. Vitullo, *Religioni e internet: evangelizzazione o reincantamento del mondo?*, in A. Melloni (a cura di), *Rapporto sull'analfabetismo religioso in Italia*, Bologna, 2014, 362 ss.

[4] W. Kasper, *Fede e storia*, Brescia, 1993, 34 ss., ha sottolineato che l'ostacolo alla possibilità di ammettere declinazioni virtuali del culto cattolico è dato dall'origine di questa fede che è l'incarnazione di Dio in suo Figlio.

[5] R. Marchetti, *Sagrati virtuali: nuove relazioni online*, in *Vita e Pensiero*, 4, 2009, 60 ss., ha analizzato il rischio che l'utilizzo delle tecnologie *online* possa impedire il raggiungimento della salvezza delle anime come fine ultimo dell'ordinamento della Chiesa cattolica.

[6] Sul punto si rinvia diffusamente a R. Petricca, *Pastorale digitale 3.0*, Roma, 2022; G. Ruggeri, *Teologia digitale. Internet come cultura e pensiero per-formante nell'insegnamento teologico. Prassi esperienziale*, Trapani, 2021; V. Annicchiarico, *L'omelia nell'era digitale: la Chiesa non ha paura del nuovo*, Viverein, 2018; A. Palermo, *La Chiesa mediale: sfide, strutture, prassi per la comunicazione digitale*, Milano, 2017; G. Tridente-B. Mastroianni (a cura di), *La missione digitale: comunicazione della Chiesa e social media*, Roma, 2016; M. Scaringella, *Internet e nuova evangelizzazione*, Pessano con Bornago (MI), 2015; F. Pasqualetti-C. Alvati (a cura di), *Reti sociali: porte di verità e di fede, nuovi spazi di evangelizzazione: percorsi di comunicazione*, Roma, 2014.

[7] La dimensione digitale è ormai una nuova piattaforma per l'esercizio della libertà religiosa e, in generale, offre nuove declinazioni dei diritti all'interno dell'assetto costituzionale dello Stato. Per un approfondimento, G. De Gregorio-R. Radu, *Digital constitutionalism in the new era of Internet governance*, in *International Journal of Law & Information Technology*, 30, 2022, 6 ss.

[8] Francesco, Messaggio per la LVII Giornata mondiale della pace "*Intelligenza artificiale e pace*", 01 gennaio 2024, n. 1, il cui testo integrale è consultabile sul sito *vatican.va*.

[9] Francesco, *Messaggio al Presidente Esecutivo del "World Economic Forum" a Dovos-Klosters*, 12 gennaio 2018, il cui testo integrale è consultabile sul sito *vatican.va*.

[10] Francesco, *Discorso ai partecipanti al Seminario "Il bene comune nell'era digitale"*, 27 settembre 2019, il cui testo integrale è consultabile sul sito *vatican.va*.

sorta di notizie, idee, insegnamenti»[11] devono essere conformi ai pilastri su cui il magistero ha strutturato il proprio insegnamento: centralità dell'uomo, servizio delle persone, dialogo con il mondo, comunione ecclesiale e nuova evangelizzazione[12]. Infatti, «l'innovazione tecnologica ha un peso etico e spirituale, poiché ogni scelta progettuale esprime una visione dell'umanità»[13]. In tal senso occorre che «la cultura nuova profondamente segnata e costruita con e dalla tecnologia… rimanga umana»[14].

Queste posizioni coinvolgono pienamente anche gli strumenti di Intelligenza Artificiale[15]. La materia è stata approfondita a partire dal magistero del pontefice emerito, per il quale i sistemi di AI «possono contribuire al processo di liberazione dall'ignoranza e facilitare lo scambio di informazioni tra popoli e generazioni diverse», purché l'uomo decida «se diventare cibo per gli algoritmi oppure nutrire di libertà il proprio cuore, senza il quale non si cresce nella sapienza»[16]. La preoccupazione che l'utilizzo dei modelli di AI possa causare gravi danni all'ambiente ha inoltre incentivato la raccomandazione di sviluppare soluzioni sostenibili «per ridurre il loro impatto sulla "casa comune"»[17].

---

[11] Concilio Vaticano II, Decreto *Inter Mirifica* sugli strumenti di comunicazione sociale, 04 dicembre 1963, in *AAS*, 56, 1964, 145.

[12] Sul punto, Congregazione per l'Educazione Cattolica, *Orientamenti per la formazione dei futuri sacerdoti circa gli strumenti di comunicazione sociale*, 19 marzo 1986, il cui testo integrale è consultabile sul sito *vatican.va*; Pontificio Consiglio delle Comunicazioni Sociali, *Criteri di collaborazione ecumenica e interreligiosa nel campo delle comunicazioni sociali*, 04 ottobre 1989, il cui testo integrale è consultabile sul sito *vatican.va*; Congregazione per la Dottrina della Fede, Istruzione *circa alcuni aspetti dell'uso degli strumenti di comunicazione sociale nella promozione della dottrina della fede*, 30 marzo 1992, il cui testo integrale è consultabile sul sito *vatican.va*; Pontificio Consiglio delle Comunicazioni Sociali, *Etica nella pubblicità*, 22 febbraio 1997, il cui testo integrale è consultabile sul sito *vatican.va*; Pontificio Consiglio delle Comunicazioni Sociali, *Etica nelle comunicazioni sociali*, 04 giugno 2000, il cui testo integrale è consultabile sul sito *vatican.va*; Benedetto XVI, Esortazione apostolica post-sinodale *Verbum Domini*, 30 settembre 2010, in *AAS*, 102, 2010, 681 ss.; Benedetto XVI, *Discorso ai partecipanti all'assemblea plenaria del Pontificio Consiglio delle Comunicazioni Sociali*, 28 febbraio 2011, in *AAS*, 103, 2011, 325 ss.

[13] Leone XIV, *Messaggio ai partecipanti del Builders AI Forum*, 3 novembre 2025, il cui testo integrale è consultabile sul sito *vatican.va*.

[14] Leone XIV, *Saluto agli influencer e missionari digitali*, 29 luglio 2025, il cui testo integrale è consultabile sul sito *vatican.va*.

[15] R. Santoro, *Chiesa cattolica e intelligenza artificiale: dalla Rome Call for AI Ethics alle Linee guida vaticane*, in *Stato, Chiese e pluralismo confessionale*, 4, 2025, 37 ss.

[16] Francesco, Messaggio per la LVIII Giornata mondiale delle comunicazioni sociali "*Intelligenza artificiale e sapienza del cuore: per una comunicazione pienamente umana*", 24 gennaio 2024, il cui testo integrale è consultabile sul sito *vatican.va*.

[17] Dicastero per la Dottrina della Fede-Dicastero per la Cultura e l'Educazione, Nota *Antiqua et nova* sul rapporto tra intelligenza artificiale e intelligenza umana, 14 gennaio 2025, il cui testo integrale è consultabile sul sito *vatican.va*. Per un commento si rinvia a F. Balsamo, *La tutela del diritto di libertà religiosa nell'era dell'intelligenza artificiale*, Cosenza, 2025, 24 ss.; F. Patsch, *«Antiqua*

Su questa scia si pone anche Leone XIV, che riconosce i vantaggi di cui l'umanità può beneficiare grazie allo sviluppo tecnologico ma «è essenziale che la dignità umana e il bene comune continuino a essere solide priorità per tutti, individui ed entità pubbliche»[18]. Questi nuovi strumenti infatti «rimandano all'intelligenza umana che li ha prodotti e traggono molta della loro forza etica dalle intenzioni delle persone che li impugnano. Riconoscere e rispettare ciò che caratterizza in modo unico la persona umana è essenziale per il dibattito su qualunque quadro etico adeguato alla gestione dell'intelligenza artificiale»[19]. Il rischio, secondo il pontefice, è quello di

«modificare radicalmente alcuni dei pilastri fondamentali della civiltà umana… La sfida non è tecnologica, ma antropologica… La questione che ci sta a cuore non è cosa riesce o riuscirà a fare la macchina, ma cosa possiamo e potremo fare noi, crescendo in umanità e conoscenza, con un uso sapiente di strumenti così potenti a nostro servizio… La sfida che ci aspetta non sta nel fermare l'innovazione digitale, ma nel guidarla, nell'essere consapevoli del suo carattere ambivalente. Sta a ognuno di noi alzare la voce in difesa delle persone umane, affinché questi strumenti possano veramente essere da noi integrati come alleati»[20].

È parte di tali dinamiche anche l'ordinamento giuridico cattolico. Il Codice di Diritto Canonico incoraggia l'utilizzo degli "strumenti di comunicazione sociale" (can. 822 § 1), perché finalizzati alla missione di annunciare il Vangelo a tutte le genti[21]. Tra questi trovano una collocazione anche le nuove tecnologie digitali la cui diffusione, oltre a sollevare subbi di natura etica[22], interroga sulla possibile configurazione di un contrasto[23] con i

et Nova». L'intelligenza artificiale al servizio della dignità e del bene comune, in *La Civiltà Cattolica*, 4194, 2025, 207-218.

[18] Leone XIV, Messaggio ai partecipanti al Congresso Internazionale della Pontificia Accademia per la Vita "*AI and Medicine: the Challenge of Human Dignity*", 7 novembre 2025, il cui testo integrale è consultabile sul sito *vatican.va*.

[19] Leone XIV, Messaggio ai partecipanti alla Seconda Conferenza annuale su *Intelligenza Artificiale, Etica e Governance d'Impresa*, 17 giugno 2025, il cui testo integrale è consultabile sul sito *vatican.va*.

[20] Leone XIV, Messaggio per la LX Giornata Mondiale delle Comunicazioni Sociali *Custodire voci e volti umani*, 24 gennaio 2026, il cui testo integrale è consultabile sul sito *vatican.va*.

[21] Pontificia Commissione per le Comunicazioni Sociali, Istruzione pastorale *Communio et Progressio* sugli strumenti della Comunicazione Sociale pubblicata per disposizione del Concilio Ecumenico Vaticano II, 23 maggio 1971, in *AAS*, 63, 1971, n. 73.

[22] A. Fabris, *Etica delle nuove tecnologie*, Brescia, 2012, 23 ss.; I. Sanna, *L'etica della comunicazione nell'era digitale*, Roma, 2012, 75 ss.

[23] Sul punto si rinvia ampiamente a P. Benanti, *Le macchine sapienti: intelligenze artificiali e decisioni umane*, Genova, 2018; G. Manzone, *Morale artificiale: nanotecnologie, intelligenza artificiale, robot.*

principi giuridici che fondano la *governance* ecclesiale esercitata attraverso il *munus docendi*, il *munus sanctificandi* e il *munus regendi*.

2. La funzione di insegnare nella dimensione *online*

La funzione di insegnare della Chiesa[24] presenta profili inediti attraverso l'utilizzo degli strumenti di comunicazione sociale.
Tra questi la dimensione digitale rappresenta un nuovo spazio di esercizio delle attività di evangelizzazione e di predicazione della parola di Dio (cann. 747-833)[25]. Il principale riferimento è ai siti web diocesani e parrocchiali che diffondono il magistero ecclesiale, condividono con i propri fedeli appuntamenti e informazioni e costituiscono "luogo" di evangeliz-

Sfide e promesse, Bologna, 2020; G. Amendola-G. Lorizio, *Antropos-logos: la ragione al crocevia di intelligenza artificiale, razionalità scientifica, pensiero filosofico e teologia cristiana*, Roma, 2021.

[24] Ai sensi del can. 747, la Chiesa possiede il diritto ed il dovere nativo di annunciare il Vangelo a tutte le genti, indipendentemente da qualsiasi umana potestà. I contenuti di questo annuncio sono: 1) il deposito della fede, cioè la Sacra Scrittura e la Sacra Tradizione; 2) i principi morali anche circa l'ordine sociale, in quanto la Chiesa coopera alla salvezza degli uomini; 3) vari aspetti della realtà umana come famiglia, procreazione ed educazione della prole, società civile, lavoro, arti, tecnica, pace, guerra, convivenza umana e laddove lo esigano i diritti fondamentali della persona o la salvezza delle anime.
La letteratura canonistica in materia di *munus docendi* è assai vasta. Per un approfondimento si rinvia, *ex plurimis*, a F.J. Urrutia, *De Ecclesiae munere docendi. Liber III CIC*, Roma, 1987; V. Fagiolo, *Il* Munus docendi*: i canoni introduttivi del* Codex *e la dottrina conciliare del Magistero autoritativo della Chiesa*, in Associazione Canonistica Italiana (a cura di), *L'annuncio cristiano nella società europea contemporanea*, Città del Vaticano, 1987, 19 ss.; C.J. Errázuriz, *Il '*Munus docendi Ecclesiae*': diritti e doveri dei fedeli*, Milano, 1991; Aa.Vv., *La funzione di insegnare della Chiesa*, Milano, 1994; B. Lima, *Il* munus docendi *della Chiesa nei suoi fondamenti giuridico-teologici. Commentario al Libro III del Codice di diritto canonico*, Todi, 2009; G. Boni, *Il ruolo attivo del laicato nel* munus docendi. *I laici educatori nella Chiesa di oggi*, in G. Dalla Torre-P. Lillo-G.M. Salvati (a cura di), *Educazione e religione*, Città del Vaticano, 2011, 87 ss.; C.J. Errázuriz, *La Parola di Dio quale bene giuridico ecclesiale. Il '*munus docendi*' della Chiesa*, Roma, 2012; D.G. Astigueta, *Il libro III del CIC e il Concilio Vaticano II a trenta anni della sua promulgazione*, in *Periodica de re canonica*, 102, 2013, 567 ss.; G. Feliciani, *I diritti e i doveri dei fedeli laici nell'ambito della evangelizzazione. La loro partecipazione al "*munus docendi*"*, in I. Martínez-Echevarría Castillo (a cura di), *Fede, evangelizzazione e diritto canonico*, Roma, 2014, 45 ss.; G. Urru, *La funzione di insegnare della Chiesa nella legislazione attuale*, Roma, 2018; Y.J. Attila, *La missione: insegnare il deposito della fede dovunque e sempre*, Venezia, 2020; M. Del Pozzo, *La differenziazione tra potestà di governo e di magistero nell'assetto costituzionale ecclesiale*, in *Diritto e religioni*, 1, 2021, 24 ss.; P. Palumbo, *Diritto e persona. Il diritto canonico nell'ecclesiologia conciliare*, Napoli, 2022, 189 ss.; Gruppo Italiano Docenti di Diritto Canonico, *Evangelizzazione e missione nella riforma della Chiesa*, Milano, 2023; G. D'Angelo, *La funzione di insegnare a quarant'anni dalla promulgazione del* Codex. *Brevi spunti di riflessione, in prospettiva*, in P. Palumbo-A. Foderaro (a cura di), *Diritto Canonico: Persone, Comunità, Missione. A 40 Anni dalla promulgazione del Codice per la Chiesa latina*, Napoli, 2024, 175 ss.

[25] D. Tarantino, *Comunicare la testimonianza. Il Dicastero per la Comunicazione nella riforma curiale*, Varazze (SV), 2023, 132 ss.

zazione. In questa prospettiva, tutti i fedeli sono chiamati ad un grande senso di responsabilità nell'utilizzo dei nuovi spazi del culto, affinché le attività realizzate siano segno di misericordia nelle parole e nei gesti[26]. Come evidenziato dal documento di sintesi del cammino sinodale delle Chiese che sono in Italia del 2025, «l'annuncio avviene sempre in una relazione comunicativa, ridefinendo lo spazio e il tempo dell'atto comunicativo. Con sobrietà e competenza, dunque, i cristiani sono chiamati ad abitare tutti gli ambienti di vita in cui si svolge l'esistenza delle persone, compreso quello digitale che richiede una formazione adeguata»[27].

Nello specifico dei profili giuridici, il can. 747 § 1 prevede la possibilità di ricorrere all'uso di «propri strumenti di comunicazione sociale… per predicare il Vangelo a tutte le genti». L'uso della tecnologia, com'è già stato evidenziato, «non consiste tanto nell'aggiungere certi contenuti, quanto nel dare una nuova dimensione, quella cristiana, ad ogni attività umana che abbia a che fare con le comunicazioni sociali»[28]. Benché l'esperienza dimostri il ricorso sempre più frequente alle risorse digitali per predicare la parola di Dio, il vigente impianto legislativo nulla prevede in merito[29]. L'unico riferimento è rappresentato dal can. 772 § 2, ai sensi del quale «Per parlare sulla dottrina cristiana mediante la radio o la televisione, siano osservate le disposizioni date dalla Conferenza Episcopale»[30]. La norma disciplina l'esercizio del ministero della parola divina attraverso l'attività di predicazione fatta non all'interno di una chiesa, un oratorio o una celebrazione ma attraverso i mezzi di comunicazione sociale. Il riferimento del legislatore universale è agli strumenti che erano diffusi all'epoca dell'entrata in vigore del Codice: la radio e la televisione. La dottrina, contemporanea al periodo di promulgazione del *Codex*, ha già evidenziato che, seppur con

---

[26] Francesco, Messaggio per la L Giornata mondiale delle comunicazioni sociali "*Comunicazione e misericordia: un incontro fecondo*", 24 gennaio 2016, il cui testo integrale è consultabile sul sito *vatican.va*.

[27] Terza Assemblea Sinodale delle Chiese in Italia, *Lievito di pace e di speranza. Documento di sintesi del cammino sinodale delle Chiese che sono in Italia*, 25 ottobre 2025, n. 33, 23, il cui testo interale è consultabile sul sito *camminosinodale.chiesacattolica.it*, ha avanzato la proposta di costituire, almeno a livello interdiocesano o di regione ecclesiastica, *équipe* per la pastorale digitale, che si avvalgono di esperti e professionisti per elaborare un piano integrato di comunicazione, e di promuovere percorsi educativi per una presenza consapevole della Chiesa nei *social media* in modo da aiutare a raccontare la bellezza del Vangelo, anche contrastando *fake news* e post-verità.

[28] C.Z. Erràzzuriz, *Gli strumenti di comunicazione sociale e in specie i libri (cann. 822-832)*, in Aa.Vv., *La funzione di insegnare della Chiesa*, Milano, 1994, 98 ss.

[29] Per un'analisi, A. Chirico, *Profili giuridici della comunicazione nella Chiesa*, Bari, 20124, 99 ss.

[30] R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, Napoli, 2024, 173 ss., evidenziano che il can. 831 § 2 attribuisce alle Conferenze episcopali il compito di stabilire i requisiti per la lecita partecipazione dei chierici e dei membri di Istituti religiosi a trasmissioni radiofoniche e televisive che trattano questioni attinenti alla dottrina cattolica o la morale.

modalità differenti, «la predicazione della parola di Dio deve essere compiuta in ottemperanza a quei criteri di autenticità previsti per ogni forma di predicazione»[31]. Spetta alle Conferenze Episcopali inoltre disciplinare la possibilità di predicazione attraverso questi mezzi. Esse hanno indicato la necessità di un'autorizzazione da parte dell'autorità competente e le qualità che il richiedente deve avere per poter parlare di fede e morale in una trasmissione televisiva o radiofonica[32].

L'attualità della norma esaminata consente di estendere le riflessioni in materia di radio e televisione anche ai mezzi di comunicazione oggi protagonisti nella società digitale[33]. Pertanto, il canone potrebbe essere modificato includendo anche gli strumenti e i "luoghi" digitali come modalità e spazi di esercizio della funzione di insegnare della Chiesa[34].

Ulteriore declinazione digitale della funzione di insegnare potrebbe essere offerta dai cann. 769 e 771 §1. Il primo raccomanda che «La dottrina cristiana sia proposta in modo conforme alla condizione degli uditori e adattato alle necessità dei tempi». Un'interpretazione evolutiva della disposizione consentirebbe di tener conto della dimensione digitale come luogo attraverso cui esercitare l'attività di predicazione. Il can. 771 § 1 prescrive inoltre «un particolare interessamento per quei fedeli che, a motivo delle loro condizioni di vita, non possono godere dell'ordinario ministero dei parroci o sono privi di qualsiasi assistenza». Il magistero ecclesiastico specifica l'ambito di applicazione soggettiva della norma, includendo tra quei soggetti gli emigrati, gli esuli, i profughi, i marittimi, i turisti, i nomadi, gli addetti ai trasporti aerei. Costoro ben potrebbero ricorrere all'uso delle tecnologie digitali per beneficiare del valore salvifico della predicazione.

Anche l'attività catechetica incontra nuove prospettive nella realtà digitale. *Influencer* sono anche sacerdoti e suore che, attraverso i *social networks*, offrono attività di catechesi e di annuncio per i loro *followers*[35]. Il magistero

---

[31] T. Vanzetto, *Quando il pulpito da cui viene la predica è la radio o la televisione (can. 772 § 2)*, in *Quaderni di diritto ecclesiale*, 2, 1999, 208 ss.

[32] Nel 2004 i vescovi italiani hanno emanato il documento *Comunicazione e missione. Direttorio sulle comunicazioni sociali nella missione della Chiesa*, perché «la comunione ecclesiale e la missione evangelizzatrice della Chiesa trovano nei media un campo privilegiato di espressione e per attuare una pastorale organica e integrata dinanzi alle opportunità e alle sfide della comunicazione sociale». Per un approfondimento si rinvia a Conferenza Episcopale Italiana, Decreto *Comunicazione e missione. Direttorio sulle comunicazioni sociali nella missione della Chiesa*, 18 giugno 2004, il cui testo integrale è consultabile sul sito *chiesacattolica.it*.

[33] D.E. Viganò, Miranda prorsus. *La Chiesa cattolica nell'età della comunicazione di massa (1957)*, in D.E. Viganò, *Papi e media. Redazione e ricezione dei documenti di Pio XI e Pio XII su cinema, radio e tv*, Bologna, 2023, p. 213 ss.

[34] R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 177 ss.

[35] G. Ruggeri, *Lo smartphone nella tonaca: mutazioni. Internet e i social network mutano l'identità della persona consacrata e la comunità*, in *Vita Consacrata*, 1, 2019, 58 ss.; P.A. Soukup, *TikTok: un nuovo*

pontificio ha tuttavia evidenziato che la realtà digitale non deve essere il fine ma lo strumento. In occasione della 44° Giornata Mondiale delle Comunicazioni Sociali del 2010 Benedetto XVI ha affermato che

«con la comunicazione del mondo digitale vengono offerte al sacerdote nuove possibilità di esercitare il proprio servizio *alla* Parola e *della* Parola. Con la loro diffusione, pertanto, la responsabilità dell'annuncio non solo aumenta, ma si fa più impellente e reclama un impegno più motivato ed efficace. La dimensione digitale può comportare il rischio di un'utilizzazione dettata principalmente dalla mera esigenza di rendersi presente, e di considerare erroneamente il web solo come uno spazio da occupare. Ai Presbiteri, invece, è richiesta la capacità di essere presenti nel mondo digitale nella costante fedeltà al messaggio evangelico, per esercitare il proprio ruolo di animatori di comunità»[36].

Il can. 779 presenta un riferimento diretto alla relazione tra catechesi e dimensione digitale: «L'istruzione catechetica sia trasmessa con l'uso di tutti gli aiuti, sussidi didattici e strumenti di comunicazione sociale, che sembrano più efficaci perché i fedeli, in modo adatto alla loro indole, alle loro capacità ed età come pure alle condizioni di vita, siano capaci di apprendere più pienamente la dottrina cattolica e di tradurla in pratica in modo più conveniente». Indole, capacità, età e condizioni di vita potrebbero essere l'incentivo per prevedere in modo espresso l'esercizio della catechesi nel cyberspazio a vantaggio dei cd. nativi digitali. Questa previsione non sarebbe *contra Codicem*, perché il legislatore ha previsto l'utilizzo dei mezzi più idonei alla condizione dei fedeli.
Il pontefice emerito ha mostrato un'importante apertura rispetto alle tecnologie digitali. Con la Costituzione apostolica *Praedicate evangelium* del 19 marzo 2022 Francesco ha affermato che «Il Dicastero per le Comunicazioni Sociali provvede alle necessità della missione evangelizzatrice della Chiesa utilizzando i modelli di produzione, le innovazioni tecnologiche e le forme di comunicazione attualmente disponibili e quelle che potranno svilupparsi nel tempo a venire» (art. 184)[37].
Nell'ambito del *munus docendi* un rilevante strumento di trasmissione della

approccio ai social media, in *La Civiltà Cattolica*, 4195/4196, 2025, 255, evidenzia che l'apertura della piattaforma alla libertà dell'espressione creativa incoraggia i creatori di contenuti religiosi ad utilizzare questo "spazio" per educare e spiegare le proprie tradizioni religiose.

[36] Benedetto XVI, Messaggio per la XLIV Giornata mondiale delle Comunicazioni Sociali "*Il sacerdote e la pastorale nel mondo digitale: i nuovi media al servizio della Parola*", 16 maggio 2010, il cui testo integrale è consultabile sul sito *vatican.va*.

[37] Francesco, Costituzione apostolica *Praedicate evangelium* sulla Curia romana e il suo servizio alla chiesa nel mondo, 19 marzo 2022, il cui testo integrale è consultabile sul sito *vatican.va*.

Parola è anche l'azione missionaria della Chiesa. Questa modalità si serve del supporto di strumenti digitali per annunciare il Vangelo ed approfondire la vita di fede. Difatti, si sta definendo con intensità sempre maggiore la presenza di missionari ed evangelizzatori digitali, la cui attività è ritenuta importante dal magistero pontificio per «'missionare' e 'samaritanare' gli ambienti digitali, affinché la cultura contemporanea possa conoscere Dio»[38]. Questo tema è stato uno dei 'cenacoli' del *World Meeting on Human Fraternity*, tenutosi nel maggio 2024, dal tema #*BeHuman*. La riflessione definisce uno stile di fraternità nella realtà digitale per creare un nuovo *social media*, basato non sullo sfruttamento degli altri a beneficio del gestore, ma a favore degli altri[39]. Il primo incontro mondiale di queste figure si è tenuto nel luglio 2023 a Lisbona durante il Festival degli *influencer* cattolici. Inoltre, in occasione della preparazione del Sinodo dei Vescovi sulla sinodalità è stata creata una piattaforma virtuale (sinododigital.com) con l'obiettivo di portare il Sinodo anche negli ambienti digitali, garantire a tutti l'inclusione e la possibilità di essere ascoltato, nonché la possibilità di dare il proprio contributo alla Chiesa[40]. In tal senso il Dicastero per la Comunicazione ha evidenziato il sostegno che i missionari digitali possono portare per

«evitare che la Chiesa seppellisca i doni dell'era digitale stimolando a metterli in pratica, a usare il web per chiamare a raccolta uomini e donne di buona volontà, a mostrare che un'altra strada è sempre possibile per usare i social media per testimoniare l'essere Chiesa, facendo della missione digitale un nuovo ministero ecclesiale»[41].

L'evangelizzazione in Internet ha favorito la nascita di diversi movimenti ecclesiali[42]. Questi vedono protagoniste principalmente le donne. In particolare, si segnala il caso dell'associazione '*iMisión*', un'attività di evangelizzazione *online* proposta da Xiskya Valladares, una religiosa della Purezza di Maria Santissima, filologa e giornalista, originaria del Nicaragua ma residente in Spagna, nota come la "*monja tuitera*". L'associazione è nata sulla

[38] Francesco, *Videomessaggio per "Hechos 29", Incontro internazionale di giovani evangelizzatori digitali in Messico*, 5-6 agosto 2022, in *L'Osservatore Romano*, 9 agosto 2022, 8.

[39] D. Imeneo, *Chiesa digitale. La sfida per influencer e comunicatori? Portare la fraternità sul web*, in *Avvenire*, 16 maggio 2024, il cui testo integrale è consultabile sul sito *avvenire.it*.

[40] Sinodo dei Vescovi, *Sintesi della tappa continentale. Sinodo digitale*, 30 marzo 2023, il cui testo integrale è consultabile sul sito *synod.va*.

[41] P. Ruffini, *Messaggio in occasione della Jornada de Oración – Evangelizadores Digitales*, 22 ottobre 2022, il cui testo integrale sul sito *vatican.va*.

[42] Il principale riferimento in materia è al Servizio per l'Apostolato Digitale, inserito nell'Ufficio per la Pastorale Universitaria dell'Arcidiocesi di Torino, che promuove progetti per diffondere la cultura digitale con un'ottica di fede. Per un approfondimento è possibile consultare il sito *apostolatodigitale.it*.

scorta del magistero pontificio per cui

«la Chiesa non è chiamata solo a usare i mezzi di comunicazione per diffondere il Vangelo ma, soprattutto oggi più che mai, a integrare il messaggio di salvezza nella "nuova cultura" che questi mezzi potenti creano e amplificano. La Chiesa avverte che l'uso delle tecniche e delle tecnologie contemporanee da parte della propria missione del terzo millennio»[43].

Su questi presupposti è stato pubblicato il Decalogo per l'evangelizzazione su Internet con l'obiettivo di diffondere le regole per il corretto uso delle tecnologie digitali nel campo dell'annuncio[44]. Questa nuova realtà ha attirato l'attenzione di Francesco che, nel luglio del 2023, ha nominato la fondatrice della comunità virtuale membro del Sinodo con diritto di voto. La riflessione sinodale si è concentrata inoltre sulla necessità di offrire maggiori opportunità di partecipazione ai fedeli laici, uomini e donne, «esplorando ulteriori forme di servizio e ministero in risposta alle esigenze pastorali del nostro tempo»[45]. In tal senso, il documento finale del Sinodo parla di missione digitale come "ministero" e, alla luce delle esperienze *online* già esistenti, potrebbe ammettersi l'introduzione di un ministero femminile di "evangelizzatrice digitale".
La celebrazione del Giubileo del 2025 è stata l'occasione di un incontro specifico per i missionari digitali e gli *influencer* cattolici. Leone XIV ha esortato i partecipanti a «nutrire di speranza cristiana le reti sociali e gli ambienti digitali», ricordando che «non si tratta semplicemente di generare contenuti, ma di incontrare cuori, di cercare chi soffre e ha bisogno di conoscere il Signore per guarire le proprie ferite» ed invitando a «riparare le reti […] reti dove si possa ricucire ciò che è spezzato, dove si possa guarire dalla solitudine, non contando il numero dei *follower*, ma sperimentando in ogni incontro la grandezza infinita dell'Amore»[46].
L'attitudine della Chiesa a stare al passo con i tempi[47] si traduce in un'aper-

[43] Giovanni Paolo II, Lettera apostolica *Il rapido sviluppo*, 24 gennaio 2005, n. 2, il cui testo integrale è consultabile sul sito *vatican.va*.

[44] Attraverso il sito *imision.org* è possibile accedere al programma *Conecta* che eroga corsi *online* per l'evangelizzazione su *Tiktok*, *Youtube*, *Instagram* e, in generale, nel continente digitale. Inoltre, gli utenti possono partecipare a *iJornada*, un evento annuale finalizzato alla formazione dei missionari digitali (*IAlumni*).

[45] XVI Assemblea Generale Ordinaria del Sinodo dei Vescovi, Documento finale della Seconda Sessione "*Per una Chiesa sinodale: comunione, partecipazione, missione*", 26 ottobre 2024, n. 77, il cui testo integrale è consultabile sul sito *press.vatican.va*.

[46] Leone XIV, *Saluto agli influencer e missionari digitali*, cit.

[47] Per un'analisi dell'espressione in prospettiva storica attraverso i documenti del magistero, si rinvia ampiamente ad A. Steccanella, *Segni dei tempi. Dialogo tra Vangelo e storia*, Padova, 2024.

tura che non demonizza la realtà digitale ma la considera un'importante alleata nell'esercizio della funzione di insegnare. In questo ambito, i laici possono dare un rilevante contributo nel trasformare gli strumenti tecnologici in «meravigliosi invenzioni tecniche»[48] idonee alla diffusione del messaggio di salvezza.

3. Sacramenti e sacramentali in rete tra divieti, rischi e opportunità

La rivoluzione digitale coinvolge notevolmente anche l'esercizio della funzione di santificare della Chiesa cattolica[49].
A tal riguardo si è osservato che «se il sacramento è lo strumento di relazione tra il fedele e Dio, questa maggiore conoscenza può realizzarsi in qualunque luogo. L'ambiente digitale non rappresenta dunque un ostacolo per il fedele che vuole conoscere Dio, il quale si manifesta nello spazio fisico come in quello digitale»[50]. Pertanto, certamente la realtà digitale non è sacramentale, ma «non è neanche scontatamente profana»[51].
Il Concilio Vaticano II ha affermato che:

«la santificazione dell'uomo è significata per mezzo di segni sensibili e realizzata in modo proprio a ciascuno di essi […]. Ogni celebrazione liturgica, in quanto opera di Cristo e del suo corpo, che è la Chiesa, è azione sacra per eccellenza e nessun'altra azione della Chiesa ne eguaglia l'efficacia allo stesso titolo e allo stesso grado»[52].

In questo senso si è espresso anche il Dicastero per le Comunicazioni Sociali (già Pontificio Consiglio) secondo il quale

«La realtà virtuale non può sostituire la reale presenza di Cristo nell'Eucaristia, la realtà sacramentale degli altri Sacramenti e il culto partecipato in

[48] Concilio Vaticano II, Decreto *Inter Mirifica* sugli strumenti di comunicazione sociale, cit., 145 ss.

[49] F. Pasqualetti, *Universo digitale. Come sta cambiando il nostro mondo*, Città del Vaticano, 2021, 9 ss.

[50] T. Berger, *@Worship: Liturgical Practices in Digital Worlds (Liturgy, Worship and Society)*, Routledge, 2019, XI.

[51] J. Geldhof, *Homo adorans in tempi di digitalizzazione? Prospettive teologiche su un'antropologia liturgica per il futuro*, in D. Jurczak-O.M. Sarr-M. Tymister (a cura di), *Liturgia "virtuale"? Atti del XII Congresso Internazionale di Liturgia*, Napoli, 2022, 43.

[52] Concilio Vaticano II, Costituzione apostolica *Sacrosanctum Concilium*, 04 dicembre 1963, il cui testo integrale è consultabile sul sito *vatican.va*.

seno a una comunità umana in carne e ossa. Su Internet non ci sono Sacramenti. Anche le esperienze religiose che vi sono possibili per grazia di Dio, sono insufficienti se separate dall'interazione del mondo reale con altri fedeli. Questo è un altro aspetto di Internet che richiede studio e riflessione. Al contempo, la programmazione pastorale dovrebbe riflettere su come condurre le persone dal ciberspazio alla comunità autentica e su come, mediante l'insegnamento e la catechesi, Internet possa essere utilizzato successivamente per sostenerle e arricchirle nel loro impegno cristiano»[53].

La liturgia non può fare a meno di una necessaria materialità. Se è vero che «l'apparente perennità del digitale… è in aperto contrasto con l'unicità dell'evento sacramentale»[54], impedendo agli strumenti digitali di sostituirsi ai segni sensibili e alla materia che caratterizzano i sacramenti[55], è altrettanto vero che la comunità ecclesiale è chiamata a comprendere pienamente il posto che il digitale occupa nella società e nella cultura[56], quindi anche nella Chiesa e nella sacra liturgia.
È opportuno chiedersi pertanto se il mondo reale si contrapponga davvero all'ambiente digitale, dal momento che l'inculturazione della liturgia e dei sacramenti nell'infosfera si avvale di una mediazione virtuale che è parte integrante dell'esistenza delle persone[57]. Continuare ad utilizzare strumenti digitali e trasmettere in *streaming* le celebrazioni e le altre attività liturgiche è ormai parte di un processo identitario che ha riformato la Chiesa stessa.
Nell'Esortazione apostolica *Christus vivit* del 2019 Francesco ha affermato che

«non si tratta più soltanto di 'usare' strumenti di comunicazione, ma di vivere in una cultura ampiamente digitalizzata che ha impatti profondissimi sulla nozione di tempo e di spazio, sulla percezione di sé, degli altri, del

[53] Pontificio Consiglio delle Comunicazioni Sociali, *La Chiesa e Internet*, 22 febbraio 2002, n. 9, il cui testo integrale è consultabile sul sito *vatican.va*.

[54] R. Maier, *Streaming eucaristici in tempo di epidemia. Una riflessione in seconda battuta*, 29 marzo 2020, il cui testo integrale è consultabile nel sito *olir.it*.

[55] L. Peyron-C. Tarditi, *Forme simboliche, liturgia e cultura digitale. Note filosofiche e teologiche*, in M. Olzi-R. Revello (a cura di), *Religioni e Media. Un'introduzione ad alcune problematiche*, Milano, 2021, 203 ss.

[56] N. Sintobin, *Celebrazioni digitali? Una domanda dall'esperienza*, in *La Civiltà Cattolica*, 4078, 2020, il cui testo integrale è consultabile sul sito *laciviltacattolica.it*.

[57] R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 242 ss., evidenziano che le posizioni di chi ritiene completamente estraneo alla vita di fede e liturgico-rituale l'apporto del digitale sono fuori dallo spazio, dal tempo e dalla realtà, tenuto anche conto che i media digitali assumono sempre più la grammatica del corpo, lo estendono e lo amplificano, partecipando di tutti i sensi che normalmente sono coinvolti nelle esperienze ecclesiali.

mondo, sul modo di comunicare, di apprendere, di informarsi, di entrare in relazione con gli altri»[58].

Da tempo la Chiesa cattolica ha intrapreso questa direzione. Dapprima con la Nota pastorale *Il giorno del Signore* del 1984 della Conferenza Episcopale Italiana[59], poi con la Lettera apostolica *Dies Domini* pubblicata da Giovanni Paolo II nel 1998[60] e l'Esortazione apostolica postsinodale *Sacramentum caritatis* di Benedetto XVI del 2007[61], l'orientamento assunto ha riconosciuto e riconosce i vantaggi e le opportunità che gli strumenti di comunicazione sociale (ad oggi quelli della realtà digitale) possono offrire alla celebrazione dei sacramenti. Senza dubbio questa modalità di partecipazione non è equiparabile a quella in presenza, ma essa non è da escludersi per quanti non possano vivere di persona il sacrificio eucaristico.
La lettura delle norme poste a garanzia della validità giuridica dei sacra-

[58] Francesco, Esortazione apostolica post-sinodale *Christus vivit*, 25 marzo 2019, n. 86, il cui testo integrale è consultabile sul sito *vatican.va*.

[59] Conferenza Episcopale Italiana, Nota pastorale *Il giorno del Signore*, 07-11 maggio 1984, il cui testo integrale è consultabile sul sito *chiesacattolica.it*, in merito alla messa teletrasmessa seguita da persone malate, anziane o impossibilitate a recarsi in Chiesa, ha affermato che tale modalità di partecipazione alla celebrazione della domenica «può offrire un servizio spiritualmente assai utile (…). Chi per seri motivi è impedito, non è tenuto al precetto. D'altra parte, la partecipazione alla Messa alla radio o alla televisione non soddisfa mai il precetto. Tuttavia, è evidente che una Messa alla televisione o alla radio, che in nessun modo sostituisce la partecipazione diretta e personale all'assemblea eucaristica, ha i suoi aspetti positivi: la Parola di Dio viene proclamata e commentata "in diretta" e può suscitare la preghiera; il malato e l'anziano possono unirsi spiritualmente alla comunità che in quello stesso momento celebra il rito eucaristico; la preghiera universale può essere condivisa e partecipata. Manca certamente la presenza fisica, ma l'impossibilità di portare un'offerta all'altare non esclude quella di fare della propria vita (malattia, debolezza, memorie, speranze, timori) un'offerta da unire a quella di Cristo» (n. 35).

[60] Giovanni Paolo II, Lettera apostolica *Dies Domini*, 31 maggio 1998, il cui testo integrale è consultabile sul sito *vatican.va*, ha invitato i fedeli che «a causa di malattia, infermità o per qualche altra grave ragione, ne sono impediti (…) ad unirsi da lontano nel modo migliore alla celebrazione della Messa domenicale (…). In molti Paesi, la televisione e la radio offrono la possibilità di unirsi ad una Celebrazione eucaristica nel momento in cui essa si svolge in un luogo sacro. Ovviamente questo genere di trasmissioni non permette in sé di soddisfare al precetto domenicale, che esige la partecipazione all'assemblea dei fratelli mediante la riunione in un medesimo luogo e la conseguente possibilità della comunione eucaristica. Ma per coloro che sono impediti dal partecipare all'Eucaristia e sono perciò scusati dall'adempiere il precetto, la trasmissione televisiva o radiofonica costituisce un aiuto prezioso» (n. 54).

[61] Benedetto XVI, Esortazione apostolica post-sinodale *Sacramentum caritatis*, 22 febbraio 2007, il cui testo integrale è consultabile sul sito *vatican.va*, ha ricordato che «il linguaggio dell'immagine rappresenta la realtà, ma non la riproduce in sé stessa. Se è assai lodevole che anziani e malati partecipino alla santa Messa festiva attraverso le trasmissioni radiotelevisive, non altrettanto potrebbe dirsi di chi, mediante tali trasmissioni, volesse dispensarci dall'andare in chiesa per partecipare alla Celebrazione eucaristica nell'assemblea della Chiesa viva» (n. 57).

menti[62] interroga quindi sull'effettiva possibilità per la Chiesa di esercitare *online* la propria funzione di santificare. I sacramenti infatti «sono diritto e fonte di diritto»[63]. Questa prospettiva è definita dai cann. 213 e 843 del Codice di Diritto Canonico: il primo sancisce il diritto dei fedeli a ricevere i sacramenti, il secondo il dovere dei ministri di amministrarli[64]. Tali riferimenti sono confermati dalla previsione di segni specifici, materia, forma e luoghi determinati per la valida celebrazione sacramentale al fine di evitare che si favorisca uno «spazio per la creatività che, nell'ambito della celebrazione dei Sacramenti, si trasforma piuttosto in una 'volontà manipolatrice'»[65].

L'acqua benedetta è il segno per amministrare il battesimo (can. 853), che deve essere conferito o per immersione o per infusione (can. 854) all'interno di una chiesa o di un oratorio (can. 857 § 1). Se invece a causa della distanza o per altre circostanze non sia possibile accedere ai luoghi prescritti senza grave disagio, il sacramento deve essere conferito in un'altra chiesa o oratorio più vicini o anche in altro luogo decoroso (can. 859). Il legislatore ne vieta l'amministrazione nelle case private o negli ospedali, salvo diverse previsioni dell'autorità ecclesiastica competente (can. 860), in quanto il battesimo è un sacramento e, come azione di tutta la Chiesa, chiede la presenza della comunità[66]. La rigidità delle disposizioni normative esclude la possibilità di amministrazione attraverso l'esclusivo ausilio degli strumenti digitali. Una simile celebrazione non avrebbe alcuna validità giuridica per l'ordinamento canonico[67].

Il sacramento della confermazione deve essere conferito invece attraverso «l'unzione del crisma sulla fronte, unzione che si fa con l'imposizione della mano e con le parole prescritte nei libri liturgici approvati» (can. 880 § 1). L'unzione[68] va fatta con il pollice della mano destra senza l'ausilio di ovatta o di altro mezzo[69]. È opportuno, secondo il disposto del can. 881,

---

[62] Un'ampia trattazione in materia è offerta da A. Sánchez-Gil, *Sacramenti e diritto: i sacramenti come diritti e come sorgenti di diritto*, Roma, 2022.

[63] C.J. Errázuriz, *Chiesa e diritto: saggi sui fondamenti del diritto nella Chiesa*, Roma, 2022, 42.

[64] G. Incitti, *La nota «Gestis verbisque» del Dicastero per la Dottrina della Fede. Prospettive canonistiche*, 17 giugno 2024, il cui testo integrale è consultabile sul sito *osservatoreromano.va*.

[65] Dicastero per la Dottrina della Fede, Nota *Gestis verbisque* sulla validità dei sacramenti, 02 febbraio 2024, il cui testo integrale è consultabile sul sito *vatican.va*.

[66] E. Frank, *I Sacramenti dell'Iniziazione, della Penitenza e dell'Unzione degli infermi*, Città del Vaticano, 2012, 58.

[67] R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 247.

[68] Il can. 880 § 2 prescrive che il sacro crisma sia realizzato con olio d'oliva misto con balsamo e consacrato a questo scopo dal Vescovo.

[69] L. Chiappetta, *Il Codice di Diritto Canonico. Commento giuridico-pastorale*, vol. 2, a cura di F. Catozzella-A. Catta-C. Izzi-L. Sabbarese, Bologna, 2011[3], 123.

che questo sacramento sia celebrato «in chiesa e durante la messa; tuttavia per una giusta e ragionevole causa può essere celebrato (…) in qualsiasi luogo degno». Benché l'ultima parte della norma ammetta la possibilità di celebrazione in un luogo diverso da quelli previsti a condizione che sia decoroso e in presenza di una giusta e ragionevole causa (come una malattia o l'impossibilità di spostarsi), la dottrina afferma che questa previsione non legittima il fedele a scegliere il posto in cui ricevere il sacramento[70]. Né tanto meno è possibile interpretare il canone nel senso che un "qualsiasi luogo degno" sia anche lo spazio digitale.

La materia dell'eucaristia è costituita da pane e vino ai quali va aggiunta un po' d'acqua (can. 924 § 1)[71]. La chiarezza delle prescrizioni giuridiche non ha impedito l'introduzione di modalità di celebrazione eucaristica nella dimensione *online*. Il riferimento è alla *cyber-eucarestia*, che viene amministrata attraverso la lettura di un testo davanti al computer e il cibarsi di pane e vino, o al *communion service* su *Twitter*, introdotto da un ministro della Chiesa metodista inglese, che consente di ricevere la comunione a distanza come quella che ricevono i fedeli nello stesso momento ma non nello stesso luogo del celebrante[72].

Dalla storia della Chiesa emerge la possibilità di partecipare all'eucaristia 'a distanza'[73]. Francesco ha sollecitato il ricorso a questa pratica durante le liturgie celebrate nel periodo pandemico, invitando i fedeli a recitare la co-

---

[70] T. Rincón-Pérez, *La liturgia e i sacramenti nel diritto della Chiesa*, Roma, 2018, 143 ss.

[71] Il can. 924 § 2 precisa che «il pane deve essere solo di frumento e confezionato di recente», mentre il § 3 sottolinea che «il vino deve essere naturale, del frutto della vite e non alterato». Questi requisiti sono previsti a pena di invalidità e non consentono di considerare altri elementi come materia valida. A tal riguardo, la Congregazione per la Dottrina della Fede, Lettera ai Presidenti delle Conferenze Episcopali *circa l'uso del pane con poca quantità di glutine e del mosto come materia eucaristica*, 24 luglio 2003, il cui testo integrale è consultabile sul sito *vatican.va*, ha previsto che l'uso di pane con poco glutine è consentito solo per le persone affette da celiachia. Allo stesso modo il mosto è stato permesso solo per i sacerdoti che in nessun modo possono bere bevande alcoliche, con la licenza dell'Ordinario.

[72] A. Spadaro, *Liturgia e tecnologia*, in *La Civiltà Cattolica*, 3860, 2011, 109 ss.

[73] M. Ganarin, *Specificità e potenzialità del diritto canonico al tempo della crisi epidemica in Italia*, in *Ius Canonicum*, 61, 2021, 223, ricorda che già il Concilio di Trento parlava di "comunione spirituale o di desiderio". La preghiera per partecipare spiritualmente al sacrificio eucaristico è presente in Sant'Alfonso Maria de' Liguori, *Visite al SS. Sagramento ed a Maria Santissima: colla pratica ed atti per la comunione spirituale*, Roma, 1839, 32: «Gesù mio, io credo che sei realmente presente nel Santissimo Sacramento. Ti amo sopra ogni cosa e ti desidero nell'anima mia. Poiché ora non posso riceverti sacramentalmente, vieni almeno spiritualmente nel mio cuore. Come già venuto, io ti abbraccio e tutto mi unisco a te; non permettere che mi abbia mai a separare da te»; C. Giraudo, *La vita sacramentale in tempo di pandemia*, in L. Alici-G. De Simone-P. Grassi (a cura di), *Quaderni di dialoghi. Speciale 2020. La fede e il contagio nel tempo della pandemia*, Roma, 2020, 53 ss., ha precisato che la comunione spirituale non è una pratica devozionale ma il desiderio dell'assunzione reale dell'eucaristia e di una unione spirituale con il Signore.

munione spirituale, se spinti dal desiderio di ricevere quella sacramentale[74]. In modo unanime si è ritenuto tuttavia che essa «non sostituisce il vero cibo che è l'Eucaristia, non sostituisce la comunione reale che è vitale per la vita del cristiano»[75]. Non è dunque ipotizzabile una celebrazione eucaristica esclusivamente nello spazio digitale, perché essa è un evento comunitario che chiede l'interazione fisica, personale e reale tra i suoi membri (can. 899 § 2)[76].

Requisiti stringenti sono previsti anche in relazione al luogo di celebrazione. Il can. 932 § 1 sancisce che «la celebrazione eucaristica venga compiuta nel luogo sacro» o in casi di particolari necessità «in un luogo decoroso», mentre il can. 932 § 2 prescrive che «il sacrificio eucaristico si deve compiere sopra un altare dedicato o benedetto». La lettura combinata delle norme citate esclude la possibilità di celebrazione in un 'luogo' digitale che è privo sia della materia richiesta (pane e vino), sia di un altare dedicato o benedetto la cui esistenza è subordinata all'intervento dell'autorità ecclesiastica competente (cann. 1206-1207)[77]. L'ipotesi di una "transustanziazione a distanza" sarebbe dunque giuridicamente invalida.

Sul presupposto che la consacrazione del pane e del vino è un memoriale[78], è altresì fondamentale la relazione tra celebrante ed altare, perché quella "vicinanza" è strumento di partecipazione diretta al sacrificio eucaristico. A tale riguardo, nel 2014 l'allora Congregazione per il Culto Divino e la Disciplina dei Sacramenti ha ritenuto che, se la presenza di molti sacerdoti concelebranti «non permette di assegnare ad essi un posto nelle vicinanze dell'altare, rendendoli tanto distanti da destare perplessità la relazione con esso (…) conviene che il numero dei concelebranti sia adeguato alla

---

[74] "Ai tuoi piedi, o mio Gesù, mi prostro e ti offro il pentimento del mio cuore contrito che si abissa nel suo nulla e nella Tua santa presenza. Ti adoro nel Sacramento del Tuo amore, desidero riceverti nella povera dimora che ti offre il mio cuore. In attesa della felicità della comunione sacramentale, voglio possederti in spirito. Vieni a me, o mio Gesù, che io venga da Te. Possa il Tuo amore infiammare tutto il mio essere, per la vita e per la morte. Credo in Te, spero in Te, Ti amo. Così sia». Per un commento si rinvia a G. Gambassi, *Coronavirus. Con la Comunione spirituale l'Eucaristia "entra" nel cuore*, 15 aprile 2020, il cui testo integrale è consultabile sul sito *avvenire.it*.

[75] J. San Jose Prisco, *La celebración de los sacramentos en un mundo digital*, in *Estudios eclesiásticos: Revista de investigación e información teológica y canónica*, 383, 2022, 1051.

[76] *Ex plurimis*, M. Torcivia, *Spiritualità e liturgia. La riflessione post-conciliare*, in *Teresianum*, 61, 2010, 59 ss.

[77] F. Passaseo, *La dimensione giuridico-ecclesiologica degli altari delle Chiese dismesse: questioni divise tra diritto canonico, diritto liturgico e diritto dello Stato*, in *Stato, Chiese e pluralismo confessionale*, 14, 2021, 211 ss.

[78] G. De Rosa, *«Questo è il mio corpo. Questo è il mio sangue». L'istituzione dell'Eucaristia*, in *La Civiltà Cattolica*, 3637, 2002, 25, ricorda che il sacerdote rende attuale e rinnova il sacrificio di Gesù Cristo attraverso le stesse parole pronunciate e gli stessi gesti da Lui compiuti nell'Ultima Cena.

capienza del presbiterio o dell'area equivalente» (lett. b, n. 9)[79]. Questa prospettiva rende evidente l'impossibilità di una consacrazione *online* del pane e del vino.

Diversa potrebbe essere l'ipotesi della "comunione da asporto"[80], per cui il fedele porterebbe a casa le specie già consacrate per riceverle dopo aver partecipato virtualmente alla celebrazione eucaristica. Questa possibilità potrebbe trovare fondamento sia nel can. 918, che prevede di dare e ricevere la sacra comunione fuori della Messa a coloro che la chiedono per una giusta causa[81], sia nell'istituto del Viatico per i fedeli che si trovino in pericolo di morte (can. 921) e per gli infermi (can. 922) che sono oggettivamente impossibilitati a partecipare fisicamente alla celebrazione eucaristica. È auspicabile quindi un intervento dei vescovi e delle Conferenze episcopali a vantaggio di quei fedeli che, al di fuori delle situazioni previste dal diritto, si trovino in uno stato di vita che non permetta di partecipare in presenza alla celebrazione liturgica[82].

Il sacramento della penitenza deve essere amministrato in una chiesa o oratorio, *ex* can. 964 § 1. Il legislatore rimette alle Conferenze episcopali la scelta di individuare la sede per le confessioni, purché i confessionali «si trovino sempre in un luogo visibile, provvisti di una grata fissa tra il penitente e il confessore, cosicché i fedeli che lo desiderano possano liberamente servirsene» (can. 964 § 2)[83]. In presenza di una giusta causa è possibile celebrare il sacramento in un luogo diverso dal confessionale (can. 964 § 3) che, tuttavia, deve essere sempre sacro, in quanto ogni sacramento è azione della Chiesa[84]. La disciplina in esame non è prescritta a pena di invalidità del sacramento[85] e ciò consentirebbe di affermare che anche uno spazio digitale possa essere 'luogo di pentimento e di conversione'[86]. In tal

---

[79] Congregazione per il Culto Divino e la Disciplina dei Sacramenti, *Guida per le grandi Celebrazioni*, 13 giugno 2014, il cui testo integrale è consultabile sul sito *vatican.va*.

[80] J. San Jose Prisco, *La celebración de los sacramentos en un mundo digital*, cit., 1066 ss.

[81] In tal senso, Congregazione per il Culto Divino e la Disciplina dei Sacramenti, Decreto *Eucharistiae celebratio*, 21 giugno 1973, n. 14, il cui testo integrale è consultabile sul sito *vatican.va*.

[82] B.F. Pighin, *Il nuovo sistema penale della Chiesa*, Venezia, 2021, 399 ss. evidenzia che l'introduzione di un regolamento specifico disciplinerebbe anche i casi di abuso e costituirebbe un ulteriore deterrente contro il delitto di profanazione delle specie sacre (can. 1382).

[83] M. Del Pozzo, *Luoghi della celebrazione "sub specie iusti". Altare, tabernacolo, custodia degli oli sacri, sede, ambone, fonte battesimale, confessionale*, Milano, 2010, 357 ss.

[84] A tal riguardo si rinvia ampiamente ad A.V. Amarante-F. Sacco (a cura di), *Riconciliazione sacramentale. Morale e Prassi pastorale*, Padova, 2019.

[85] La disciplina non irritante del canone ha consentito nel tempo continue modifiche delle modalità di amministrazione del sacramento. Per un approfondimento, F. Rodríguez, *Storia del sacramento della Penitenza*, in *Angelicum*, 4, 2013, 977 ss.

[86] C. Ciotola, *Confessione anche on line? Spunti di riflessione sul sacramento della penitenza*, in *Diritto e*

senso si esprimono quanti ritengono che la materia e la forma del sacramento della penitenza (la confessione orale della colpa e le parole di assoluzione pronunciate dal confessore) sussistono anche quando il sacramento è amministrato attraverso un colloquio telefonico o in videochiamata, perché «il perdono di Dio si riceve in presenza di una conversione sincera del penitente e il ministro dà l'assoluzione»[87]. Al pari degli altri sacramenti, la confessione rappresenta infatti l'occasione in cui la *salus animarum* deve prevalere rispetto alle esigenze liturgiche e giuridiche della Chiesa[88]. Questa posizione confligge con l'orientamento dottrinale per cui la presenza fisica del penitente è assolutamente necessaria per la valida amministrazione del sacramento[89] il quale si basa, come tutti gli altri sacramenti, sul criterio della incarnazione[90]. La prospettiva teologica ha evidenziato inoltre che «il collegamento del confessore con la sede, la paziente attesa dei penitenti non è solo funzionale ma simbolica e rappresentativa dell'ansia e del desiderio di perdono e riconciliazione da parte di Dio»[91].
L'orientamento della Chiesa è chiaro da tempo. Già con il documento *Reconciliatio et Paenitentia* del 1984 Giovanni Paolo II ha ricordato che per la confessione occorre la presenza fisica del penitente. Essa non può avvenire per telefono o email o altri mezzi di comunicazione sociale per motivi legati alla tutela del sigillo sacramentale[92]. Con una Nota del 2002 la Peni-

Religioni, 2, 2010, 27 ss.; J. Hahn, *Communion in an Online Mass? Sacramental Questions in Light of the COVID Crisis*, in *Studia Canonica*, 2, 2020, 457 ss. Tra le numerose applicazioni create per amministrare il sacramento della confessione in via digitale si segnala l'app *Confession: a Roman Catholic App*, che consente di riconciliarsi tramite *smartphone* attraverso la guida ad un esame di coscienza e al riconoscimento dei peccati da confessare al sacerdote virtuale.

87 F.M. Arocena, *Il sacramento della penitenza, realtà antropologica e culturale*, in *Scripta Theologica*, 3, 2009, 756.

88 In questo senso si sottolinea la prospettiva "terapeutica" del sacramento che vede il confessore quale "medico" delle anime, come già affermato dal n. 1421 del Catechismo della Chiesa Cattolica. Per un approfondimento si rinvia a P. Sorci, *Il "Confessore" o Ministro del Sacramento della Penitenza*, in *Rivista di Pastorale Liturgica*, 281, 2010, 46 ss.; D. Tarantino, *Dalla riconciliazione alla guarigione. Alcune riflessioni sulla confessione come* cura animarum *nella teologia morale e nel diritto canonico*, in *Stato, Chiese e pluralismo confessionale*, 9, 2017, 1 ss.

89 In riferimento all'utilizzo dell'app *Confession: A Roman Catholic App*, progettata dalla società americana LittleiApps in sostituzione della confessionale tradizionale, l'allora portavoce vaticano il 9 febbraio 2011 ha affermato l'importanza di comprendere che «il sacramento della penitenza richiede necessariamente il rapporto di dialogo personale tra il penitente ed il confessore e l'assoluzione da parte del confessore presente». Il testo completo della dichiarazione è consultabile sul sito *vatican.va*.

90 *Ex plurimis*, T. Weinandy, *Sacrament of Mercy: A Spiritual & Practical Guide to Confession*, Boston, 1997, 48 ss.

91 M. Del Pozzo, *Il ministero del confessionale tra disponibilità e obbligatorietà*, in *Annales Theologici*, 35, 2021, 116.

92 Giovanni Paolo II, Esortazione apostolica post-sinodale *Reconciliatio et Paenitentia*, 02

tenzieria Apostolica ha affermato, inoltre, l'illegittimità di una confessione via telefono per il pericolo di violazione del sigillo sacramentale che tale pratica può arrecare[93].

Le restrizioni causate dall'emergenza sanitaria e l'esigenza dei fedeli di riconciliarsi con Dio[94] hanno sollecitato la Conferenza Episcopale Italiana ad individuare nuove possibili modalità di amministrazione del sacramento[95] (luoghi ampi e areati, distanza di almeno un metro tra ministro e penitente, utilizzo di D.P.I.)[96]. Nelle ipotesi di assoluta impossibilità di ricevere l'assoluzione sacramentale, i vescovi italiani hanno ricordato che la Chiesa prevede la possibilità di ricevere il perdono del Signore nella forma del cd. *votum confessionis*, cioè esprimere il sincero desiderio di ricevere il sacramento della riconciliazione proponendosi di celebrarlo successivamente, non appena possibile[97].

---

dicembre 1984, il cui testo integrale è consultabile sul sito *vatican.va*.

[93] Penitenzieria Apostolica, *Lettera circolare agli episcopati sull'uso dei mezzi tecnologici e rispetto del segreto della coscienza*, 23 ottobre 2002, il cui testo integrale è consultabile sul sito *penitenzieria.va*.

[94] La diffusione della pandemia da Covid-19 ha sviluppato nuove modalità di amministrazione dei sacramenti, la cui validità è stata ampiamente oggetto di discussione. In materia di penitenza, D. Tarantino, *La resilienza della Riconciliazione fra tradizione e nuove prospettive. Spunti per una riflessione*, in *Diritto e Religioni*, 1, 2020, 48 ss., la quale riporta i casi di *drive confession* nati negli Stati Uniti, dove alcuni parroci hanno iniziato a confessare i fedeli nel parcheggio della Chiesa attraverso i finestrini delle auto dei penitenti.

[95] Durante l'emergenza sanitaria ha trovato applicazione l'assoluzione collettiva disciplinata dal can. 961 § 1 n. 2, secondo cui «L'assoluzione a più penitenti insieme senza la previa confessione individuale non può essere impartita se non vi sia grave necessità, ossia quando, tenuto conto del numero dei penitenti, non si hanno a disposizione confessori sufficienti per ascoltare, come si conviene, le confessioni dei singoli entro un tempo conveniente, sicché i penitenti, senza loro colpa, sarebbero costretti a rimanere a lungo privi della grazia sacramentale o della sacra comunione…». Sul punto, Penitenzieria Apostolica, *Nota circa il Sacramento della Penitenza nell'attuale situazione di pandemia*, 19 marzo 2020, il cui testo integrale è consultabile sul sito *penitenzieria.va,* ha chiarito che la modalità straordinaria dell'assoluzione collettiva poteva essere applicata soprattutto nei luoghi maggiormente interessati dal contagio pandemico, come gli ospedali, e fino a quando il fenomeno non sarebbe rientrato. Tuttavia, spettava al vescovo diocesano determinare i casi di grave necessità e il fedele avrebbe potuto ottenere il perdono dei peccati, compresi quelli mortali, mediante la contrizione perfetta espressa da una sincera richiesta di perdono e accompagnata dalla ferma intenzione di ricorrere, appena possibile, alla confessione sacramentale. Si veda anche l'esperienza della confessione via *whatsapp* amministrata da un sacerdote bergamasco: D. Tarantino, *The on the road reconciliation. A way to deal with the Pandemic*, in F. Balsamo-D. Tarantino (a cura di), *Law, religion and the spread on Covid-19 Pandemic*, Pisa, 2021, il cui testo integrale è consultabile sul sito *diresom.net*.

[96] Per una rassegna delle disposizioni di diritto particolare adottate dai vescovi di alcune diocesi e regioni ecclesiastiche italiane, N. Tonti, *Il sacramento della riconciliazione dinanzi alla pandemia di Covid-19. L'assoluzione generale senza previa confessione individuale e le disposizioni di diritto particolare di alcuni vescovi diocesani italiani*, in *Diritto e Religioni*, 2, 2021, 102 ss.

[97] Conferenza Episcopale Italiana, *Suggerimenti per la celebrazione dei sacramenti in tempo di*

La linea tracciata dalla Chiesa è uniforme nel ritenere invalida l'assoluzione impartita attraverso i mezzi di comunicazione sociale (tra cui quelli digitali)[98], anche per la pericolosità che ne deriva per la violazione del sigillo sacramentale[99] causata, ad esempio, dalla presenza di terze persone che possono assistere alla videochiamata tra penitente e confessore[100], in quanto «manca la presenza reale del penitente e non si verifica la reale trasmissione delle parole dell'assoluzione: si tratta solo di vibrazioni elettriche che riproducono la parola umana»[101]. La Penitenzieria Apostolica ha ulteriormente ribadito che «i sacramenti non sono gesti magici e vanno vissuti nella loro dimensione di celebrazione ecclesiale dove la ritualità di gesti e parole è necessaria per la loro verità. È necessaria, pertanto, la presenza reale e non solo virtuale o digitale»[102].
La dottrina, in modo conforme al magistero, evidenzia che

«l'amministrazione del sacramento della penitenza attraverso strumenti tecnologici è assolutamente vietata non solo perché in questo modo non è affatto tutelato il sigillo sacramentale, ma anche perché il rapporto reale che deve instaurarsi tra ministro confessore e soggetto penitente esige la

emergenza Covid-19, 17 marzo 2020, il cui testo integrale è consultabile sul sito *chiesacattolica.it*; Francesco, *Omelia*, 20 marzo 2020, il cui testo integrale è consultabile sul sito *vatican.va*, ha affermato che nell'impossibilità di trovare un sacerdote per la confessione si può "parlare" sinceramente con Dio, affidandogli pene, afflizioni, peccati, chiedendo con costrizione il Suo perdono, perché con «un Atto di Dolore ben fatto, così la nostra anima diventerà bianca come la neve».

98 Si può ricordare nel periodo pandemico l'esperienza temporanea della *video confession* promossa dal vescovo della prelatura di Caravelì in Perù.

99 E. Baura, *Il diritto all'intimità nella Chiesa: bene giuridico e disponibilità del diritto*, in *Ephemerides iuris canonici*, 2, 2021, 719 ss.

100 *Ex plurimis*, P. Lo Iacono, *Repressione dei* delicta graviora contra mores*, sigillo sacramentale e segreto pontificio (il difficile equilibrio tra riservatezza e trasparenza)*, in M. d'Arienzo-V. Buonomo-O. Échappé (a cura di), Lex rationis ordinatio, Cosenza, 2022, 889 ss.; G. Boni, *Tutela del sigillo sacramentale e del segreto ministeriale in Italia*, in *Ephemerides iuris canonici*, 61, 2021, 527 ss.; D. Tarantino, *Note intorno al sigillo sacramentale. Legislazione e dottrina dal Concilio Lateranense IV alla codificazione del diritto canonico*, in *Stato, Chiese e pluralismo confessionale*, 32, 2016, 1 ss.

101 Penitenzieria Apostolica, *Lettera ai confessori in occasione del Natale 2020*, 20 dicembre 2020, il cui testo integrale è consultabile sul sito *penitenzieria.va*.

102 Penitenzieria Apostolica, XXXIV Corso sul Foro interno *Il confessore e il penitente: diritti e doveri nel sacramento della Penitenza*, 4-8 marzo 2024, il cui testo integrale è consultabile sul sito *penitenzieria.va*. Va evidenziato, tuttavia, che in una risposta del 1989 l'allora Congregazione per la Dottrina della Fede ricordava che la confessione "per telefono" era permessa solo in caso di estrema necessità. Il rischio espresso nella risposta è che si possa addivenire ad una privatizzazione della riconciliazione (la traduzione italiana del testo è riportata da A. Zambon, *QDEonline: le questioni di maggiore interesse*, in *Quaderni di diritto ecclesiale*, 1, 2017, 116 ss.

loro compresenza fisica, non sostituibile con quella virtuale»[103].

Pertanto, nonostante i tentativi di estendere anche all'*online* le modalità di amministrazione del sacramento, la disciplina analizzata rileva che la funzione santificatrice della Chiesa nel celebrare la riconciliazione segue, con fermezza, la disciplina giuridica universale che intende preservare il fedele sia nella cura della sua anima che nella tutela della sua riservatezza.
Gli elementi costitutivi dell'unzione degli infermi sono l'olio benedetto, le sacre unzioni e la preghiera rituale[104]. Questo sacramento deve essere amministrato dal ministro «con le parole, l'ordine e il modo stabiliti nei libri liturgici…» (can. 1000 § 1) e «con la propria mano, salvo che una grave ragione non suggerisca l'uso di uno strumento» (can. 1000 § 2). Le norme del Codice affiancano il Catechismo della Chiesa cattolica secondo il quale

«L'essenziale della celebrazione di questo sacramento consiste nell'unzione sulla fronte e sulle mani del malato (nel rito romano) o su altre parti del corpo (in Oriente), unzione accompagnata dalla preghiera liturgica del sacerdote celebrante che implora la grazia speciale di questo sacramento» (n. 1531)[105].

Il ministro dunque deve compiere le unzioni direttamente con la mano (nello specifico con il pollice destro), salvo che una grave causa consigli l'utilizzo di uno strumento, come nel caso di una malattia contagiosa o di una persona intrappolata che non è raggiungibile con la mano[106]. L'ipotesi di amministrare questo sacramento attraverso la dimensione digitale, oltre a violare il dettato codicistico e le fonti liturgiche *extra Codicem*, priverebbe l'azione e i gesti compiuti dal ministro sacro del loro significato teologico e degli effetti connessi all'amministrazione fisica dell'unzione.
L'ordine sacro viene conferito «mediante l'imposizione delle mani e la preghiera consacratoria, che i libri liturgici prescrivono per i singoli gradi» (can. 1009 § 2). Materia del sacramento, pertanto, è l'imposizione delle mani[107], mentre la forma è la preghiera consacratoria che varia a seconda dei gradi dell'ordine: episcopato, presbiterato e diaconato. L'assenza di questi elementi inficia la validità giuridica del sacramento[108]. Circa il tempo

---

[103] B.F. Pighin, *I sacramenti. Dottrina e disciplina canonica*, Venezia, 2020, 248.

[104] E. Miragoli, *Il sacramento dell'unzione degli infermi*, in Aa.Vv., *Il diritto nel mistero della Chiesa*, vol. III, Roma, 2004, 139 ss.

[105] Il testo integrale del documento è consultabile sul sito *vatican.va*.

[106] L. Chiappetta, *Il Codice di Diritto Canonico. Commento giuridico-pastorale*, vol. 2, cit., 217.

[107] Pio XII, Costituzione apostolica *Sacramentum Ordinis*, 30 novembre 1957, il cui testo integrale è consultabile sul sito *vatican.va*.

[108] W.H. Woestman, *The Sacrament of Orders and the Clerical State. A Commentary on the Code of*

e il luogo di amministrazione, il can. 1010 prevede che «l'ordinazione si celebri durante la Messa solenne, in giorno di domenica o in una festa di precetto, ma per ragioni pastorali si può compiere anche in altri giorni, non esclusi i giorni feriali»[109]. La precisa indicazione di materia, forma e luogo di conferimento del sacramento in esame rende inimmaginabile un'amministrazione digitale dello stesso. Se così fosse, l'ordine sacro conferito sarebbe giuridicamente invalido. Ciò vale a maggior ragione considerando la minuziosità della disciplina prescritta per il sacramento in esame (requisiti soggettivi ed obblighi dell'ordinando[110], possesso di adeguate capacità e virtù ai sensi del can. 1029, età minima prevista dal can. 1031, requisiti previ all'ordinazione disciplinati dai cann. 1033-1039, irregolarità e impedimenti alla ricezione del sacramento *ex* cann. 1041-1042, nonché la documentazione necessaria per la promozione ai sacri ordini, per attestare lo scrutinio circa le qualità richieste nell'ordinando, per annotare l'ordinazione e comunicarne la notizia al parroco del luogo del battesimo dell'ordinato ai fini dell'annotazione secondo quanto previsto ai cann. 1050-1054)[111]. Non emergono concrete possibilità di celebrazione digitale neanche per il sacramento del matrimonio. Il legislatore canonico detta precise regole in materia di forma, materia e requisiti (cann. 1095-1103) del vincolo nuziale (cann. 1055-1165)[112]. Questa articolata disciplina non ammette manifestazioni di consenso espresse attraverso i mezzi di comunicazione sociale ma è necessario che i contraenti siano presenti contemporaneamente, sia di persona sia tramite procuratore, e manifestino il consenso con le parole o, se non possono parlare, con altri segni (can. 1104)[113].

La dimensione digitale potrebbe offrire invece utili strumenti per le attività di registrazione e archiviazione dei sacramenti amministrati (can. 535) in

Canon Law, Ottawa, 2001, 37 ss.

[109] Il can. 1011 § 1 precisa inoltre che «l'ordinazione si celebri generalmente nella chiesa cattedrale; tuttavia per ragioni pastorali può essere celebrata in un'altra chiesa o oratorio».

[110] Il can. 1026 prescrive che «chi viene ordinato deve godere della debita libertà; non è assolutamente lecito costringere alcuno, in qualunque modo, per qualsiasi causa a ricevere gli ordini, oppure distogliere un candidato canonicamente idoneo dal riceverli». Per un commento si rinvia a G. Degiorgi, *Le condizioni soggettive per la valida ordinazione. Seconda parte*, in *Revista Universitas Canonica*, 48, enero-diciembre 2015, 136 ss., il quale precisa che il Codice prescrive la presenza nel candidato di un'intenzione attuale e abituale-esplicita, decisiva per la validità del sacramento.

[111] B.F. Pighin, *I sacramenti. Dottrina e disciplina canonica*, cit., 108 ss., esclude il ricorso agli strumenti digitali anche per realizzare gli adempimenti prescritti per la trasmissione dei documenti e la relativa annotazione nei registri parrocchiali, dato il valore teologico delle previsioni normative.

[112] Per un approfondimento si rinvia a L. Sabbarese, *Manuale di diritto canonico*, Molfetta, 2022, 423 ss.

[113] R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 404.

termini di risparmio di spazio fisico, riduzione dei costi di archiviazione, accessibilità ai documenti, aumento della produttività e riduzione del rischio di smarrimento o danneggiamento dei documenti[114]. In tal senso il Decreto generale della C.E.I. del 2018 recante *Disposizioni per la tutela del diritto alla buona fama e alla riservatezza*[115] ha espressamente previsto la possibilità di utilizzare registri informatici per la gestione dei dati sacramentali (art. 8). Questa previsione necessita tuttavia di essere contemperata con una Risposta del Dicastero per i Testi Legislativi, secondo il quale la registrazione e l'archiviazione digitali non devono sostituire quelle tradizionali, poiché «gli strumenti multimediali non sono in grado di garantire la completa sicurezza della privacy né la tutela dai rischi informatici (*hackeraggio*) con tutte le altre conseguenze»[116].

La riflessione fin qui condotta può essere estesa anche ai sacramentali, ovvero «i segni sacri con cui, per una qualche imitazione dei sacramenti, vengono significati e ottenuti per l'impetrazione della Chiesa effetti soprattutto spirituali» (can. 1166)[117].

La distinzione tra *res* ed *actiones* prevista dall'abrogato Codice del 1917 (can. 1144)[118] è confermata dalle disposizioni vigenti. Mentre la consacrazione e la benedizione possono avere ad oggetto sia una persona che una cosa, la dedicazione riguarda espressamente i luoghi sacri (chiese ed altari)[119]. Pro-

---

[114] A tale riguardo si rinvia al caso di una parrocchia della provincia di Ancona il cui parroco, nell'atto di rilasciare un attestato di confermazione richiesto da un fedele in procinto di sposarsi, ha scoperto che il parroco emerito aveva omesso di registrare. Per un approfondimento, P. Palumbo, *Annotazione e prova della confermazione. Intorno alla vicenda del parroco che per 15 anni non ha registrato i certificati di confermazione*, in *Diritto e Religioni. News*, 17 maggio 2024, consultabile sul sito *rivistadirittoereligioni.com*.

[115] Il testo integrale del Decreto Generale è consultabile sul sito *chiesacattolica.it*.

[116] Dicastero per i Testi Legislativi, Risposta particolare *circa l'uso dei sistemi informatici web-based nella gestione dei dati sacramentali (can. 535 CIC)*, 16 dicembre 2014, il cui testo integrale è consultabile sul sito *delegumtextibus.va*.

[117] Concilio Ecumenico Vaticano II, Costituzione apostolica *Sacrosanctum Concilium*, cit., n. 60, ha ricordato che attraverso i sacramentali «gli uomini vengono disposti a ricevere l'effetto principale dei sacramenti e sono santificate le varie circostanze di vita»; sulla differenza tra sacramenti e sacramentali si rinvia a J.T. Martín De Agar, *Commentario ai cann. 1166-1253*, in J.I. Arrieta (a cura di), *Codice di diritto canonico e leggi complementari commentato*, Roma, 2018, 778 ss., il quale precisa che i sacramentali, al pari dei sacramenti, perseguono la finalità del culto divino, della santificazione dei fedeli e dell'edificazione della comunità ecclesiale, anche se a differenza dei primi non producono la grazia sacramentale, ma semplicemente dispongono gli uomini a riceverla.

[118] L. Chiappetta, *Il Codice di Diritto Canonico. Commento giuridico-pastorale*, vol. 2, cit., 448, ricorda che erano disciplinati come *res* i sacramentali il cui oggetto di intervento era una cosa (acqua, cero pasquale, oggetti riservati al culto, sacre ceneri); *actiones*, quelli relativi a consacrazioni, benedizioni, dedicazioni, preghiere liturgiche, processioni e segno della Croce.

[119] M. del Mar Martín, *Comentario sobre los cánones 1166-1253*, in Á. Marzoa-J. Miras-R.

prio in relazione alle benedizioni possono configurarsi prospettive digitali dei sacramentali. La normativa canonica non richiede che le benedizioni siano impartite in presenza. La loro efficacia (come per tutti i sacramentali) è *ex opere operantis*, cioè «mediante la preghiera di intercessione non infallibile della Chiesa»[120]. Sarebbe possibile ritenere pertanto che una benedizione impartita attraverso gli strumenti digitali sia in grado di produrre gli stessi effetti di quella effusa con modalità ordinarie.

Questa prospettiva può trovare conferma nell'esperienza ecclesiale. La benedizione apostolica *Urbi et Orbi* riservata al Romano Pontefice (can. 1169 § 2) e impartita due volte all'anno in occasione della celebrazione del Natale e della Pasqua è trasmessa e diffusa dalla televisione in tutto il mondo[121]. Il Dicastero per il Servizio della Carità (già noto come Elemosineria Apostolica) è inoltre provvisto della «facoltà di concedere la Benedizione Apostolica a mezzo di diplomi su carta pergamena debitamente autenticati e tutto il ricavato viene destinato per la carità»[122]. La richiesta di ricevere o trasmettere pergamene contenenti la benedizione pontificia può essere presentata in presenza o con una procedura *online* da ogni parte del mondo attraverso il sito internet istituzionale. Dalla prima benedizione di Pio XI nel 1931 in occasione della inaugurazione della *Statio Radiophonica Vaticana*[123] o impartite diverse volte attraverso la televisione a quelle su

Rodríguez-Ocaña (a cura di), *Comentario exegético al Código de Derecho canónico*, vol. III/2, Pamplona, 2002, 1654 ss., evidenzia che le benedizioni sono una effusione di doni celesti e si distinguono in costitutive e invocative: mentre le prime rendono sacro un luogo o una cosa (chiesa, tabernacolo, oratorio, cappella, battistero, altare, cimitero), le seconde invocano la protezione di Dio sulle persone, su un luogo, su un animale o su un oggetto. Inoltre, distingue tra benedizioni invocative, costitutive, consacrazioni con utilizzo di oli sacri ed esorcismi, cioè ammonizioni in nome di Cristo contro il demonio.

120 B.F. Pighin, *I sacramenti. Dottrina e disciplina canonica*, cit., p. 303.

121 Al di fuori dei casi previsti, il 27 marzo 2020 Francesco ha impartito, in via straordinaria, la benedizione *Urbi et Orbi* da Piazza San Pietro, invocando la protezione di Dio durante l'emergenza pandemica. La benedizione è stata trasmessa in diretta mondiale su tutti i profili social e il canale *YouTube*. Per un approfondimento, Francesco, *Benedizione "Urbi et Orbi". Momento straordinario di preghiera in tempo di epidemia*, 27 marzo 2020, il cui testo integrale è consultabile sul sito *vatican.va*. Gli stessi effetti sono stati prodotti dalla benedizione impartita da Leone XIV in occasione della sua elezione al soglio pontificio l'8 maggio 2025.

122 Il Dicastero precisa anche che i costi indicati per la concessione della Benedizione papale si riferiscono unicamente al diploma, alle spese per la preparazione e la spedizione dello stesso e ad un contributo per la carità del papa. Tutte le informazioni sono consultabili sul sito *elemosineria.va*.

123 A. De Carolis, *12 febbraio 1931, il giorno che il Papa andò alla Radio*, 12 febbraio 2019, il cui testo integrale è consultabile sul sito *vaticannews.va*.

Twitter di Francesco[124] o su *Instagram* di Benedetto XIV e di Leone XIV[125], questo tipo di sacramentale trova uno spazio sempre maggiore nella realtà digitale. Essa può facilitare la diffusione dell'annuncio del Vangelo e il perseguimento della missione salvifica della Chiesa.

Tra i sacramentali è disciplinato l'esorcismo[126], una particolare forma di preghiera che la Chiesa da sempre utilizza contro il potere del diavolo (CCC, n. 1667)[127]. L'articolata normativa in materia[128] può incontrare la possibilità che il rito avvenga con i mezzi digitali in assenza di divieti assoluti al riguardo, come già è accaduto nella prassi[129]. Sul punto la Chiesa cattolica si mostra reticente. Il Rituale *De exorcismis et supplicationibus quibusdam* considera tali strumenti quali «moltiplicatori di un diffuso e malsano interesse per la sfera del demoniaco» (Presentazione, n. 4). È necessario pertanto che i sacerdoti prestino attenzioni pastorali nel «mettere in guardia i fedeli nei confronti di libri, programmi televisivi, informazioni dei

[124] In occasione della 50ª Giornata Mondiale delle Comunicazioni Sociali "*Comunicazione e misericordia: un incontro fecondo*" del 24 gennaio 2016, Francesco ha impartito una benedizione attraverso i suoi profili *@franciscus* su *Instagram* e *@Pontifex* su *Twitter*: «A te, che dalla grande comunità digitale mi chiedi benedizione e preghiere voglio dire: tu sarai il dono prezioso nella mia preghiera al Padre. E tu non dimenticarti di pregare per me e per il mio essere servo del Vangelo della Misericordia». Il canale *Twitter @Pontifex* è stato voluto da Benedetto XVI, che il 12 dicembre 2012 lanciava il primo *tweet* e la prima benedizione: «Cari amici, è con gioia che mi unisco a voi via *Twitter*. Grazie per la vostra generosa risposta. Vi benedico tutti di cuore». Oggi l'account ha oltre 5 milioni di *follower*.

[125] L'account di papa Leone XIV *pontifex* oggi è seguito da oltre 14 milioni di utenti.

[126] Per una ricostruzione storica si rinvia a Pio XII, Lettera enciclica *Mediator Dei*, 20 novembre 1947, il cui testo integrale è consultabile sul sito *vatican.va*.

[127] D. Salvatori, *Indemoniati ed esorcismi: alcuni chiarimenti dal punto di vista terminologico*, in *Quaderni di diritto ecclesiale*, 27, 2014, 10 ss.

[128] Congregazione per il Culto Divino e la Disciplina dei Sacramenti, Rituale *De exorcismis et supplicationibus quibusdam*, 22 novembre 1998, il cui testo integrale è consultabile sul sito *vatican.va*; Associazione Internazionale Esorcisti (a cura di), *Linee guida per il ministero dell'esorcismo alla luce del rituale vigente*, Padova, 2020. Per un commento si rinvia a G. Ferraro, *Il nuovo rituale degli esorcismi: strumento della signoria di Cristo*, in *Notitiae*, 3-4, 1999, 177 ss.; M. Barba, *«De exorcismis»: variazioni nell'«editio typica emendata»*, in *Rivista Liturgica*, 91, 2004, 901 ss.

[129] Lo hanno affermato il card. esorcista Ernest Simoni in un'intervista del 16 novembre 2018, pubblicata sul sito *ansa.it*, e padre Gabriele Amorth con una dichiarazione del 24 agosto 2014, reperibile sul sito *aleteia.org,* nella quale in riferimento alla possibilità di utilizzare i *social network* per celebrazione del rito, ha sostenuto che «La risposta da parte mia è positiva, anche se in via non ordinaria. L'ideale, infatti, è sempre di incontrarsi personalmente, come del resto prevede il Rituale. (...) Spesso per aiutare queste persone sono costretto a fare esorcismi per telefono. Ovviamente quando pratico un esorcismo a distanza lo faccio solo se conosco la persona e se ne ho accertato personalmente lo stato di possessione diabolica o altro disturbo spirituale. (...) Nel caso dell'esorcismo, si tratta di un sacramentale e non di un sacramento. (...) Nel caso dell'esorcismo, diciamo che non è vietato: penso che, a mali estremi… estremi rimedi».

mezzi di comunicazione che a scopo di lucro sfruttano il diffuso interesse per fenomeni insoliti o malsani» (Presentazione, n. 8). Inoltre, per evitare che l'esorcismo sia interpretato come un atto di magia o di superstizione, il rito non deve diventare uno "spettacolo". Di conseguenza, secondo il Rituale, «durante lo svolgimento dell'esorcismo non si ammettano mezzi di comunicazione sociale e, sia prima che dopo la celebrazione del rito, tanto l'esorcista che i presenti evitino di divulgarne la notizia, mantenendo un giusto riserbo» (Premesse generali, n. 19).

A differenza dell'esorcismo, le preghiere di liberazione sono una forma di preghiera privata attraverso cui ogni fedele o gruppi di fedeli possono rivolgersi a Dio per ottenere la liberazione dagli influssi e dai disturbi del maligno. Non vi è uno specifico formulario delle preghiere di liberazione, sebbene il Rituale degli esorcismi proponga nell'Appendice I (nn. 1-12) una serie di celebrazioni e preghiere, diverse da quelle dell'esorcismo vero e proprio, che possono essere usate dai fedeli personalmente o in modo comunitario ma solo sotto la guida di un sacerdote. Attraverso le preghiere di guarigione invece il fedele implora guarigione e salute da Dio anche con il ricorso alla intercessione di santi taumaturghi, a messe *pro infirmis* e a luoghi di preghiera e di pellegrinaggio in cui Dio si è manifestato attraverso guarigioni straordinarie[130]. Nel 2000 l'allora Congregazione per la Dottrina della Fede ha pubblicato l'Istruzione *circa le preghiere per ottenere da Dio la guarigione*[131], specificando che tali preghiere possono essere elevate a Dio da ogni fedele, a meno che non si svolgano in chiesa o altro luogo sacro rendendo conveniente, in questo caso, che esse siano guidate da un ministro ordinato. Anche in tali ipotesi non sembrano emergere ostacoli dinanzi alla possibilità che le preghiere siano rivolte "da remoto" attraverso *smartphone* o in videoconferenza.

Tra gli altri atti del culto divino rientra anche la liturgia delle ore (cann. 1173-1175), con cui la Chiesa «ascoltando Dio che parla al suo popolo e facendo memoria del mistero della salvezza, Gli rende incessantemente lode e intercede per la salvezza di tutto il mondo con il canto e la preghiera» (can. 1173)[132]. Questo sacramentale è entrato a pieno nella realtà digi-

[130] R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 275.

[131] Congregazione per la Dottrina della Fede, Istruzione *circa le preghiere per ottenere da Dio la guarigione*, 23 novembre 2000, il cui testo integrale è consultabile sul sito *vatican.va*.

[132] G. Parise, *Natura dell'Ufficio divino e obbligo giuridico sub gravi della sua celebrazione integrale e quotidiana*, in *Angelicum*, 1, 2018, 75 ss., evidenzia che la normativa prescrive l'obbligo di celebrare il sacramentale per i chierici (sacerdoti e diaconi che aspirano al presbiterato) e per i membri degli Istituti di Vita Consacrata nonché delle Società di Vita Apostolica (can. 1174 § 1). L'obbligo deve essere adempiuto quotidianamente, osservando i tempi e le modalità prescritte per la celebrazione. Il Concilio Vaticano II (Costituzione apostolica *Sacrosanctum Concilium*, nn. 83-101) ha esteso la celebrazione di questo sacramentale anche agli altri fedeli che «secondo le circostanze, sono caldamente invitati a partecipare alla liturgia delle ore, in

tale. La sostituzione dei testi cartacei di preghiere, antifone e cantici con edizioni digitali gratuitamente scaricabili da siti internet ed app[133] dimostra le potenzialità che gli strumenti digitali offrono per consentire ai fedeli di pregare. In questo, come in altri casi, la realtà *online* è strumento di diffusione della Parola di Dio e di evangelizzazione e non solleva alcuna questione circa la validità giuridica dell'azione liturgica compiuta.
Residuano dubbi invece circa la possibilità di celebrare nello spazio digitale le esequie ecclesiastiche (cann. 1176-1185)[134]. L'interrogativo nasce alla luce della recente tendenza di officiare funerali in *streaming*[135]. Spesso non è possibile partecipare fisicamente alle esequie per svariate ragioni (economiche, il viaggio ha un costo esoso; lavorative, non è possibile chiedere permessi; legislative, l'impossibilità deriva dall'assenza dei requisiti burocratici che limitano o impediscono ad un soggetto di spostarsi; fisiche). Il ministro di culto pertanto predispone sistemi digitali per la diffusione in *streaming* della celebrazione e fornisce le credenziali di accesso a quanti chiedano di assistervi, senza possibilità di registrazione o conservazione del video[136].

---

quanto è azione della Chiesa» (can. 1174 § 2).

[133] Tra queste, a titolo di esempio, si evidenziano: *App CEI – Liturgia delle ore*, ideata nel 2015 dalla Conferenza Episcopale Italiana, contiene tutti i testi dell'Ufficio liturgico della Chiesa italiana e la relativa versione audio registrata da un'assemblea reale per favorire la fruibilità anche di persone ipovedenti, oltre a consentire il semplice accesso alle preghiere di giorno attraverso la selezione della data di proprio interesse; *iBreviary TS Plus for Terra Sancta* è un breviario virtuale, programmato per diverse lingue (italiano, inglese, francese, spagnolo, portoghese, arabo, rumeno, turco e latino), con un'impaginazione e sfondi molto simili a quello cartaceo, consente l'accesso alla liturgia del rito ambrosiano, ai testi di molte Congregazioni (come i Salesiani, i Passionisti e i Francescani), nonché il *download* di intere giornate di preghiere qualora l'utente sappia di non avere possibilità di accesso alla rete; *Il Libro delle Ore* è una app a pagamento nata nel 2006 e aggiornata al 30 agosto 2023 che contiene salmi, inni e cantici per la preghiera quotidiana personale e comunitaria; *Pregaudio* è una app realizzata da un'associazione di giovani di Riccione, contiene la registrazione audio della liturgia delle ore e consente di ascoltare preghiere lette, cantate e musicate soltanto da giovani; *Il Messalino app* permette di trovare gratuitamente, sia in testo che in audio, la liturgia del giorno e delle ore, nonché le omelie e i commenti al Vangelo; *laChiesa.it* è una app gratuita ideata dal proprietario del corrispettivo sito internet che offre la fruibilità della Sacra Scrittura e della preghiera quotidiana; *ePrex Liturgia delle Ore* è una app gratuita particolarmente utilizzata perché non necessita della connessione internet ma sviluppa la liturgia in base al giorno, risolvendo le difficoltà di chi non dispone di *smartphone* di ultima generazione; *Letture del giorno*, creata dagli ideatori di DinDonDan – Orari Messe, consente di pregare la liturgia delle ore attraverso un calendario che giorno per giorno permette il *download* dei testi.
Per un approfondimento si rinvia al sito *comunicazionisociali.chiesacattolica.it*.

[134] Per un commento, G. Marchetti, *Le esequie ecclesiastiche*, in *Quaderni di diritto ecclesiale*, 2, 2002, 228 ss.

[135] A. Fuccillo, *Il paradiso digitale. Diritto e religioni nell'iperuranio del web*, Napoli, 2023, 15 ss.

[136] D. Sisto, *I funerali in streaming: le tecnologie digitali e i riti funebri online*, in M. Olzi-R. Revello

La disciplina canonica delle esequie ecclesiastiche prescrive come luogo di celebrazione la chiesa della parrocchia di appartenenza, salvo la possibilità di scegliere un'altra chiesa (can. 1177). Il criterio di individuazione del luogo di culto è il domicilio o quasi-domicilio del defunto per il quale quella chiesa è stata il punto di riferimento per la sua vita ecclesiale. L'esclusiva indicazione della chiesa come luogo di celebrazione dei funerali sembra inoltre escludere non solo oratori, cappelle private, ospedali, case di riposo per anziani e edifici simili[137], ma anche la possibilità di ricorrere ad un 'luogo' digitale per lo svolgimento di tale ritualità. Da una eventuale celebrazione *online* (parallela a quella reale) deriverebbe poi una serie di altri problemi: i video delle dirette *streaming* potrebbero essere conservati sui profili social degli utenti/defunti, ponendo il problema della tutela dei dati sensibili dei soggetti coinvolti (sia del protagonista della celebrazione che degli utenti che accedono alla stanza virtuale per commemorare il defunto)[138].

Il ricorso agli strumenti digitali per le celebrazioni liturgiche è stato certamente incoraggiato dall'emergenza sanitaria dilagata dal 2020. L'utilizzo delle piattaforme più evolute è dipeso da un fattore eccezionale, tant'è che la Conferenza Episcopale Italiana nel 2023 ha raccomandato che «tutte le attività ecclesiali, liturgiche, pie devozioni, possono tornare a essere vissute nelle modalità consuete precedenti all'emergenza sanitaria. Riteniamo sia altresì opportuno che cessino, o quantomeno siano diminuite nel loro numero, le celebrazioni trasmesse in *streaming*»[139].

La sovrapposizione tra digitale e reale dimostra tuttavia che l'utilizzo di

(a cura di), *Religioni e Media. Un'introduzione ad alcune problematiche*, Milano, 2021, 187 ss.; C. England, *Funeral live-streaming might encourage "lazy mourners"*, in *The Independent*, 2 October 2016, consultabile sul sito *independent.co.uk,* rileva che secondo alcuni dati statistici nel Regno Unito il 61% circa dei funerali è celebrato nella doppia modalità in presenza e in *streaming*.

137 B.F. Pighin, *I sacramenti. Dottrina e disciplina canonica*, cit., 322 ss., ritiene che tale possibilità potrebbe essere contemplata solo in presenza di una disposizione di diritto particolare o una consuetudine consolidata o un diritto acquisito o un privilegio concesso.

138 Ufficio Nazionale per le Comunicazioni Sociali della Conferenza Episcopale Italiana, *Celebrare in diretta tv o in streaming*, 27 marzo 2020, il cui testo integrale è consultabile sul sito *chiciseparera.chiesacattolica.it*., con cui sono state pubblicate le regole per il corretto utilizzo delle tecnologie digitali in occasione di celebrazioni durante la pandemia. Le dirette *streaming* non sono state escluse, ma considerate come una tipologia liturgica scontata e ammessa alla luce dell'emergenza epidemiologica: «La parola di Dio deve essere scandita lentamente, dopo essersi accertati del corretto funzionamento dell'audio e l'altare deve essere opportunamente illuminato (…). Anche i fedeli devono essere formati a una 'presenza', se pur mediata dai mezzi di comunicazione che non escluda il coinvolgimento del corpo, attraverso una inquadratura che non riprenda solo il primo piano ma sia ampia».

139 Presidenza della Conferenza Episcopale Italiana, *Lettera ai Vescovi circa l'annuncio dell'OMS sulla fine dell'emergenza sanitaria pubblica per il Covid-19*, 8 maggio 2023, consultabile sul sito *chiesacattolica.it*.

queste tecnologie è parte integrante della vita dell'uomo. Il possibile esercizio del *munus sanctificandi* della Chiesa attraverso la dimensione virtuale sembra essere ostacolato dalla constatazione che i sacramenti sono segni scanditi da norme giuridiche e liturgiche che associano funzioni specifiche a materia, forma, luoghi e ad ogni altro elemento materiale che diventa strumento per leggere la realtà trascendentale. In questa prospettiva si ritiene che lo spazio digitale può anche ricostruire ed integrare quello fisico, ma non può sostituirsi ad esso, né può rimandare al trascendente[140].
Inoltre, la liturgia è memoriale, non memoria. Non solo passato ma anche presente. La realtà digitale, di per sé priva di materia, rischierebbe di superare il passato, la storia, per concentrarsi solo sul presente, sul momento, interrompendo la millenaria azione salvifica della Chiesa. Quell'azione che connette il fedele a Dio può essere mortificata da algoritmi, che creano solo connessione spesso priva di una vera relazione[141].
La Chiesa deve continuare a perseguire la sua missione di salvezza contribuendo alla ricerca di un equilibrio tra l'osservanza della legge e la sua applicazione nel caso concreto, soprattutto dinanzi a quei fedeli che chiedono l'azione santificatrice della Chiesa ma sono comunque costretti a ricorrere alla realtà digitale per ottenere la salvezza della propria anima.

4. Governare con il digitale: il *munus regendi* nell'infosfera

La realtà digitale offre nuove modalità di esercizio anche alla funzione di governare della Chiesa cattolica[142]. Il processo di trasformazione che coinvolge la potestà legislativa, esecutiva e giudiziaria interroga sui limiti e sulle opportunità che derivano dall'interazione tra digitale e *munus regendi*.
Nell'ambito del diritto universale e di quello particolare è sempre più frequente il ricorso a forme di promulgazione digitale della legge canonica. L'inciso del can. 8 § 1 del Codice vigente, «a meno che in casi particolari non sia stato stabilito un modo diverso di promulgare», disciplina la possibilità di ricorrere a modalità alternative di promulgazione della legge canonica[143]. Tra

[140] L. Peyron-C. Tarditi, *Forme simboliche, liturgia e cultura digitale. Note filosofiche e teologiche*, cit., 210 ss.

[141] J. Rego Bárcena, *Celebrare i sacramenti e i sacramentali: tra materialità e virtualità?*, in D. Jurczak-O.M. Sarr-M. Tymister (a cura di), *Liturgia "virtuale"? Atti del XII Congresso Internazionale di Liturgia*, Napoli, 2022, 68 ss.

[142] Per un approfondimento generale del *munus regendi* si rinvia ampiamente a B. Maloko-Mana, *Le munus regendi de l'évêque diocésain comme «Munus patris et pastoris» selon le Concile Vatican II*, Roma, 1999; G. Dammacco, *Governare la Chiesa. La* Governance *e il governo*, Roma, 2013.

[143] In tal senso, basti pensare a *L'Osservatore Romano* che sempre più spesso pubblica gli atti

queste potrebbe includersi la dimensione *online*. L'utilizzo di strumenti digitali per l'esercizio dell'attività legislativa consentirebbe di conoscere il testo più velocemente di quello stampato[144], di diffonderlo superando gli ostacoli legati allo spazio in quanto le norme raggiungerebbero ogni territorio e diverrebbero così vincolanti.

In questo modo si supererebbero le problematiche insite alle modalità tradizionali di pubblicazione: ritardi del testo stampato, discrasie tra la data di promulgazione e quella di pubblicazione nel fascicolo degli *Acta Apostolicae Sedis*[145], incertezze circa il testo della legge pubblicata, possibilità di pubblicare simultaneamente anche i testi nelle traduzioni autorizzate[146]. In diverse occasioni è accaduto infatti che il testo normativo venisse pubblicato negli *A.A.S.*, decorsi già i tre mesi di *vacatio legis* previsti dal legislatore universale (can. 8 § 1), generando dubbi in merito all'entrata in vigore della legge. Allo

legislativi universali. Tra gli esempi si annovera il motu proprio *Quaerit semper* di Benedetto XVI del 30 agosto 2011, promulgato sul giornale il 28 settembre 2011. L'esplicita indicazione da parte di Benedetto XVI di tale modalità di promulgazione ha superato l'obiezione che una pubblicazione del genere potesse avere mera finalità divulgativa e non vincolante. Per un approfondimento sia consentito il rinvio a F. Gravino, *Leggi ecclesiastiche e pubblicazione digitale. Le nuove frontiere della promulgazione nel diritto canonico*, in *Stato, Chiese e pluralismo confessionale*, 15, 2021, 63 ss.

144 Circa le incertezze dei fedeli, i quali non conoscono o conoscono in ritardo una legge promulgata nelle modalità previste dal diritto e che è già per loro vincolante, G.P. Montini, *Il motu proprio Omnium in mentem e il matrimonio canonico*, in *Quaderni di diritto ecclesiale*, 1, 2012, 138 ss., evidenzia le incertezze legate alla data di entrata in vigore del motu proprio.

145 Già sotto il Codice pio-benedettino si registravano problemi in tal senso. Sul punto, V. Del Giudice, *Promulgazione ed obbligatorietà della legge canonica*, Milano, 1927, 80 ss., ha rilevato che la legge era giuridicamente esistente anche nell'intervallo di tempo intercorrente tra la data di promulgazione e quella di pubblicazione. A titolo di esempio egli ha riportato la Costituzione apostolica *Apostolicae romanorum pontificum* relativa alle diocesi suburbicarie, promulgata il 15 aprile 1910 ma pubblicata negli *AAS* il 30 aprile 1910, e la Costituzione apostolica *Si qua est in universo* per l'ordinamento della gerarchia ecclesiastica inglese, del 28 ottobre 1911 e pubblicata solo il 10 novembre dello stesso anno; parimenti la Bolla *Providentisima Mater*, con cui fu promulgato il previgente *Codex Iuris Canonici*, fu emanata il 27 maggio 1917 e pubblicata in *AAS* il 28 giugno 1917; in modo conforme, P. Pellegrino, *La pubblicazione della legge nel diritto canonico*, Milano, 1984, 176 ss., ha affermato che promulgazione e pubblicazione erano fasi distinte del procedimento genetico della legge e ciascuna produceva specifici effetti giuridici; *contra*, P. Gillet, *De lege data et nondum promulgata*, in *Jus pontificium*, 8, 1928, 216 ss.

146 In materia, un opportuno intervento chiarificatore si registra nell'ambito del diritto vaticano. A tale riguardo Francesco, *Decreto relativo alla pubblicazione dei provvedimenti normativi nello Stato della Città del Vaticano*, 16 gennaio 2024, il cui testo integrale è edito nel sito ufficiale della Santa Sede (*vatican.va*), ha stabilito che: «Fermo restando il disposto dell'art. 2 della Legge n. LXXI sulle fonti del diritto del 1° ottobre 2008, tutti i provvedimenti normativi, di qualsiasi natura, devono ritenersi pubblicati al momento della loro affissione presso il Cortile di San Damaso, alla porta degli Uffici Postali e del Palazzo del Governatorato e nel sito istituzionale dello Stato della Città del Vaticano, prescindendo dalla data di effettiva pubblicazione nel Supplemento degli *Acta Apostolicae Sedis*».

stesso modo si è verificata una discrasia del testo pubblicato a mezzo stampa da quello promulgato[147]. In tale prospettiva, la promulgazione mediante pubblicazione *online* potrebbe fornire garanzie rispetto ai tempi di entrata in vigore della norma e al contenuto della stessa, non potendo esistere due esemplari cartacei, talvolta difformi, della stessa disposizione di legge.
È opportuno rilevare che la pubblicazione di un file pdf su un sito istituzionale della Chiesa cattolica non costituisce attività di promulgazione mediante pubblicazione *online*. Per una corretta configurazione giuridica occorre che la modalità di pubblicazione offra certezze in merito all'obbligatorietà della legge, ai suoi destinatari e alla stabilità del suo contenuto[148]. Il ricorso alla pubblicazione digitale certificata e l'*upload* su siti istituzionali (come ad esempio *vatican.va*) potrebbero rappresentare una valida opportunità di utilizzo di Internet quale piattaforma di promulgazione della legge canonica[149]. Questa possibilità offrirebbe vantaggi anche alla normativa di diritto particolare. La maggiore libertà concessa per la pubblicazione delle leggi particolari, le quali «sono promulgate nel modo determinato dal legislatore» (can. 8 § 2), potrebbe permettere ad un vescovo diocesano o ad una Conferenza Episcopale (can. 455 § 3) di scegliere la promulgazione mediante pubblicazione *online* per obbligare i propri fedeli[150]. In tal senso, la Conferenza

147 G.P. Montini, *"Tres errores faciunt stilum"? La promulgazione delle leggi tra pubblicazioni e pubblicazione*, in *Anuario Argentino de Derecho Canónico*, 2, 2017, 9 ss.

148 U. Rhode, *Alcune questioni circa il motu proprio De concordia inter Codices*, in *Periodica de re canonica*, 4, 2019, 555 ss., rileva che il motu proprio *De concordia inter Codices* è stato promulgato il 31 maggio 2016 unitamente alla decisione di Francesco circa la relativa pubblicazione su *L'Osservatore Romano* e nel commentario ufficiale degli *A.A.S*. La pubblicazione a mezzo stampa è tuttavia avvenuta il 16 settembre 2016, mentre quella negli *Acta* nel fascicolo di giugno 2016, poi pubblicato nell'ottobre del 2017. La discrasia di pubblicazione è accentuata dall'incertezza dell'entrata in vigore della normativa, che non specifica nulla a riguardo. Potrebbe dunque ritenersi che il testo diventi vincolante decorsi tre mesi dalla pubblicazione negli *Acta*, così come disposto dal can. 8 § 1, oppure che esso sia obbligatorio, computandosi il decorso della *vacatio legis* dalla promulgazione su *L'Osservatore Romano*.

149 A. Giraudo, *La promulgazione delle leggi mediante pubblicazione online*, in *Quaderni di diritto ecclesiale*, 4, 2019, 414 ss., prende ad esempio la Gazzetta Ufficiale della Repubblica Italiana.

150 Nell'ambito del diritto particolare si sono registrate diverse iniziative inerenti alla pubblicazione digitale. La Conferenza Episcopale Belga individua sul proprio sito Internet (*cathobel.be*) una sezione dedicata alla legislazione complementare al Codice di Diritto Canonico e un'altra alle disposizioni di diritto particolare, precisando che la pubblicazione di tale normativa si aggiunge a quella cartacea nella rivista del *Centre Interdiocésan de Contact*. Tale forma di pubblicazione ha una finalità solo informativa, in quanto riproduce il testo promulgato sulla rivista ufficiale cartacea, pur avendo la Conferenza Episcopale Belga chiesto alla Santa Sede la *recognitio* della promulgazione digitale delle proprie leggi particolari. Allo stesso modo il sito *usccb.org* della Conferenza Episcopale Statunitense consente all'utente di consultare le leggi specifiche in relazione alla voce di interesse. In questo caso il limite dello strumento digitale potrebbe essere strutturale: la normativa infatti è riportata alla voce *Canon Law*, che è una sottosezione del menu principale e rinvia alla pagina in cui sono pubblicati i decreti

Episcopale Italiana ha utilizzato la pubblicazione *online* per la promulgazione del Decreto generale *Disposizioni per la tutela del diritto alla buona fama e alla riservatezza* del 31 maggio 2018. L'inciso dell'art. 16 § 3 dello Statuto C.E.I. «salva diversa applicazione» ha consentito di deliberare una modalità alternativa di promulgazione. L'art. 26 del Decreto generale disciplina infatti che «la promulgazione del Decreto ha luogo con la pubblicazione del relativo decreto di promulgazione del Presidente della C.E.I. sul sito web della Conferenza Episcopale Italiana» (*chiesacattolica.it*). In questo caso si sono registrate delle criticità. Il testo normativo è stato pubblicato anche nel *Notiziario della Conferenza Episcopale Italiana*[151], legittimando dubbi circa il valore legale della relativa pubblicazione digitale. Il file contenente il testo non certifica l'autenticità del documento, né la data di pubblicazione sul sito della C.E.I. Lo stesso pdf risulta creato il 25 maggio 2018 ma modificato l'8 giugno e ciò ha determinato una discrasia tra l'entrata in vigore della normativa e la sua corrispondenza al testo approvato in sede assembleare[152]. Tali difficoltà dipendono dall'assenza di una disciplina *ad hoc*, attualmente legata alla pubblicazione sugli *A.A.S.* della normativa di diritto universale (can. 8 § 1)[153]. È opportuno quindi che intervenga una riforma della materia affinché i *christifideles* possano beneficiare di una tutela più efficace dei propri diritti[154]. Dinanzi ai possibili vantaggi offerti dalla promulgazione della legge canonica mediante pubblicazione digitale si palesano alcuni interrogativi. L'attività di *upload* potrebbe esporre il documento normativo a rischi di autenticità. Basti pensare alla possibilità di apportare dolosamente delle modifiche al file pdf[155] con riflessi sulla certezza del testo di legge, l'autorità che l'ha ema-

della Conferenza con la data di approvazione, pubblicazione ed entrata in vigore. I Vescovi statunitensi hanno tuttavia previsto che le proprie disposizioni normative, dopo aver ottenuto la debita *recognitio* della Santa Sede, entrano in vigore dopo un mese dalla pubblicazione sul sito ufficiale. Per un approfondimento si rinvia ad A. Giraudo, *La promulgazione delle leggi mediante pubblicazione online*, cit., 418 ss.

151 Conferenza Episcopale Italiana, Decreto generale *Disposizioni per la tutela del diritto alla buona fama e alla riservatezza*, 24 maggio 2018, in *Notiziario della Conferenza Episcopale Italiana*, 52, 2018, 94 ss.

152 A. Giraudo, *La promulgazione delle leggi mediante pubblicazione online*, cit., 421 ss.

153 L'auspicio sembra essere già stato superato dal Codice dei Canoni delle Chiese Orientali, il cui can. 654 fa esplicito riferimento ai libri «riprodotti in qualsiasi modo mediante invenzioni tecniche». Per un approfondimento si rinvia a M. Mosconi, *Comunicazione ecclesiale e vigilanza canonica nel contesto degli attuali strumenti di comunicazione sociale*, in *Quaderni di diritto ecclesiale*, 1, 2018, 76 ss.

154 I. Valenzi, *Libertà religiosa e intelligenza artificiale: prime considerazioni*, in *Quaderni di diritto e politica ecclesiastica*, 2, 2020, 354 ss.

155 Questa condotta è potenzialmente idonea ad integrare il delitto di falsificazione di documenti ecclesiastici pubblici di cui al can. 1391. Per un approfondimento si rinvia a R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 341 ss.

nato, la data di sottoscrizione e la sua entrata in vigore. Per questo motivo è necessario utilizzare file non modificabili dall'utente, che garantiscano la corrispondenza tra il testo pubblicato e quello promulgato in forma cartacea. Si solleva altresì una questione di tutela di giustizia sostanziale in termini di sicurezza giuridica dei fedeli che hanno diritto a conoscere con certezza la normativa vigente, l'autorità che la emana e se agisce nell'ambito delle proprie competenze[156]: questo potenziale ostacolo potrebbe essere superato con l'utilizzo della firma digitale, come già sperimentato e previsto da alcuni ordinamenti civili[157].

È opportuno allora un intervento del legislatore a riforma della materia. La previsione al can. 8 § 1 di uno specifico sito Internet istituzionale attraverso il quale promulgare le leggi emanate consentirebbe la perfezione formale dell'atto[158] e il fedele-utente sarebbe garantito in termini di vigilanza e controllo da parte dell'autorità competente[159] senza correre il rischio che alterazioni del file o siti Internet poco attendibili rendano incerto un testo che vincola tutti i battezzati, un determinato fedele o un gruppo di fedeli.

Anche la relazione tra l'attività esecutiva della Chiesa e la realtà digitale potrebbe beneficiare di alcuni vantaggi. Il can. 37 del *Codex* prescrive che «l'atto amministrativo, che riguarda il foro esterno, si deve consegnare per scritto; così pure il relativo atto di esecuzione, se viene fatto in forma commissoria». La forma scritta non è richiesta a pena di invalidità. Pertanto, si ritiene che l'atto amministrativo può essere consegnato anche con altre modalità[160]. Secondo questa interpretazione è possibile ammettere che un atto amministrativo possa essere consegnato anche con gli strumenti digitali[161]. L'accompagnamento di quella forma di pubblicazione con credenziali di accesso individuali e l'utilizzo della firma digitale per sottoscrivere il documento po-

---

156 E. Baura, *La potestà legislativa universale*, in Gruppo Italiano dei Docenti di Diritto Canonico (a cura del), *Il diritto della Chiesa tra universale e particolare*, Milano, 2013, 67 ss.

157 In materia si rinvia ampiamente a M.P. Giovannini-M. Palmirani-E. Francesconi (a cura di), *Linee guida per la marcatura dei documenti normativi secondo gli standard Normeinrete*, Firenze, 2012; per la normativa italiana, F. Faini-S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, Torino, 2017, 25 ss.

158 G.P. Montini, *"Tres errores faciunt stilum"? La promulgazione delle leggi tra pubblicazioni e pubblicazione*, cit., 19 ss.

159 A. Migliavacca, *Comunicazione per la comunione: modi e contenuti*, in *Quaderni di diritto ecclesiale*, 1, 2018, 27 ss.

160 La forma scritta a pena di invalidità è richiesta dal legislatore nei singoli casi. Sul punto si rinvia *ex plurimis* a L. Chiappetta, *Il Codice di Diritto Canonico. Commento giuridico-pastorale*, vol. 1, cit., 63.

161 M. Mosconi, *Internet e la produzione e comunicazione di documenti canonici: un legame da approfondire*, in *Quaderni di diritto ecclesiale*, 4, 2001, 371 ss., precisa che le istruzioni richiedono solo la pubblicazione, non la promulgazione: in tal caso l'utilizzo di Internet potrebbe risultare prezioso.

trebbero garantire l'autenticità dell'atto e la certezza in relazione alla ritualità dell'avvenuta notifica.

In questa direzione sono stati già compiuti alcuni passi. La consumazione di un delitto impone, secondo l'ordinamento canonico, di adottare le misure idonee a ristabilire la giustizia, emendare il colpevole e riparare lo scandalo[162]. A tal fine il precetto penale e i rimedi penali rappresentano strumenti utilizzabili in via preliminare, integrativa o sostitutiva all'irrogazione o alla dichiarazione di una pena canonica, in quanto soddisfano «le esigenze di celerità dettate dalla necessità di tutelare la comunità dei fedeli dallo scandalo che il comportamento delittuoso ha prodotto»[163]. Tali atti potrebbero essere notificati con mezzi digitali dopo aver dotato il singolo utente di credenziali di accesso e di una firma digitale per sottoscrivere il documento al fine di garantire l'autenticità dell'atto e la certezza che la notifica sia stata ritualmente compiuta[164].

Il ricorso alle tecnologie digitali nell'espletamento dell'attività giudiziaria si presenta ad uno stadio piuttosto avanzato[165]. La possibilità di celebrare processi canonici da remoto è sempre più concreta[166] con effetti positivi sui

---

[162] Queste finalità sono strettamente connesse alla tutela della *salus animarum*, quale fine ultimo dell'ordinamento canonico. Sul punto si rinvia a D.G. Astigueta, *Lo scandalo nel CIC: significato e portata giuridica*, in *Periodica de re canonica*, 92, 2003, 589 ss.

[163] B.F. Pighin, *Il nuovo sistema penale della Chiesa*, Venezia, 2021, 147.

[164] In relazione alla consumazione nel *web* dei delitti *contra fidem* e l'unità della Chiesa (eresia, apostasia e scisma) e alla notifica digitale dei relativi provvedimenti, sia consentito il rinvio a F. Gravino, Delinquere online. *Prospettive digitali del diritto penale canonico*, in *Archivio giuridico*, 2, 2025, 472 ss., in merito al caso dell'Arcidiocesi di Palermo che, con avviso del 13 novembre 2018, ha comunicato, prima, la notifica del Decreto di scomunica emesso il 15 agosto 2018 con Prot. n. 046/18, per il delitto di eresia e di scisma commesso da un sacerdote, poi quella del Decreto della CDF del 13 gennaio 2022 di dimissioni dallo stato clericale *ex officio et pro bono Ecclesiae* (*chiesadipalermo.it*). Anche il Patriarca di Venezia, il 14 dicembre 2022, ha pubblicato digitalmente «perché abbia vigore immediato» un decreto (Prot. CUR-2022-1754), con cui ha proibito a persone scomunicate per eresia e scisma di celebrare sacramenti e sacramentali nel territorio del Patriarcato di Venezia e di ascoltare le confessioni, nonché ha revocato la facoltà di assolvere validamente in tutto il territorio, tranne che nel caso di pericolo di morte (*patriarcatovenezia.it*). Il Vescovo della diocesi di Livorno, il 1° gennaio 2024, ha emesso decreto di scomunica, di sospensione *a divinis* e di rimozione dall'ufficio di un parroco (Prot. n. 1/24/VD), ammonendo sacerdoti e fedeli a non partecipare alle celebrazioni della persona scomunicata o alle altre pratiche di culto, perché sarebbero incorsi *ipso facto* nella stessa gravissima pena (*diocesilivorno.it*). Una dichiarazione formale di censura è stata pubblicata anche dall'Arcidiocesi di Spoleto-Norcia sul proprio sito Internet in data 19 aprile 2024, corredando l'avviso del Decreto di scomunica per il delitto di scisma (Prot. n. 13104/A/24 del 17 aprile 2024) (*spoletonorcia.it*).

[165] A. Zambon, *Il processo canonico di fronte alle nuove tecnologie*, in H. Franceschi-A. Sammassimo (a cura di), *Sinodalità e processo canonico*, Città del Vaticano, 2023, 39 ss.

[166] Una rassegna dei regolamenti di alcuni Tribunali ecclesiastici è offerta da P. Palumbo, *Marriage and canonical process in the digital era*, in *Stato, Chiese e pluralismo confessionale*, 9, 2022, 126

tempi di giustizia e sull'attività istruttoria[167].
Nel primo caso l'utilizzo degli strumenti digitali consente alle parti di conoscere con facilità gli atti di causa, che sono inviati tramite Posta Elettronica Certificata (PEC) a garanzia di celerità e certezza della notifica[168]. Nel secondo caso l'emersione di nuove tipologie di prove[169], come quelle digitali, ha indotto un rinnovamento delle indagini e l'introduzione di nuove tipologie di perizie. Le divergenze dottrinali che qualificano queste prove come documentali[170], atipiche[171] o inammissibili[172] convergono nell'unanime considerazione che la loro valutazione necessita dell'ausilio di un perito informatico forense[173], il quale è in grado di attestarne l'autenticità e l'integrità alla luce della facilità di manipolazione cui esse sono soggette[174]. Si sta

ss.

167 M. d'Arienzo, *Zuckerberg e i nuovi rapporti tra diritto e religioni. A proposito di libertà di coscienza nell'era digitale*, in *Diritto e Religioni*, 1, 2019, 386 ss.

168 L'utilizzo della Posta Elettronica Certificata (PEC) è una prassi ben applicata da diversi Tribunali Ecclesiastici Interdiocesani e può rappresentare una idonea soluzione in grado di coniugare celerità e certezza della notifica.

169 Ai sensi del can. 1527 § 1, nel processo possono essere addotte prove di qualsiasi genere, sempre che appaiano utili per la decisione della causa e siano lecite. Per un commento si rinvia a M. Ferrante, *Le prove in generale (artt. 155-161)*, in P.A. Bonnet-C. Gullo (a cura di), *Il giudizio di nullità matrimoniale dopo l'istruzione "Dignitas Connubii". Parte terza: la parte dinamica del processo*, Città del Vaticano, 2009, 299 ss.

170 R. Palombi, *Valore probatorio dei mezzi di comunicazione elettronica nel processo matrimoniale canonico*, in G. Dalla Torre-C. Gullo-G. Boni (a cura di), Veritas non auctoritas facit legem. *Studi di diritto matrimoniale in onore di Piero Antonio Bonnet*, Città del Vaticano, 2012, 388 ss.

171 E.B.O. Okonkwo, *L'istruzione della causa di nullità matrimoniale fra il diritto e la prassi giudiziale*, Città del Vaticano, 2020, 111 ss.

172 A. D'Auria, *La prova per documenti (Dignitas Connubii: artt. 183-192)*, in P.A. Bonnet-C. Gullo (a cura di), *Il giudizio di nullità matrimoniale dopo l'istruzione "Dignitas Connubii". Parte terza: la parte dinamica del processo*, Città del Vaticano, 2009, 362 ss., ritiene che l'elenco dei mezzi di prova previsti dal Codice sia tassativo e, pertanto, non è possibile considerare come prove tipologie diverse da quelle già disciplinate; *contra*, A. Giraudo, *Prove e nuove tecnologie nel processo canonico*, in Aa.Vv., *Matrimonio e processo: la sfida del progresso scientifico e tecnologico*, Città del Vaticano, 2016, 277 ss., sostiene che occorre rispettare la specificità di tali strumenti che vanno considerati come file o archivi digitali, da ammettersi come prove anche nel silenzio del legislatore.

173 Per un approfondimento si rinvia ampiamente ad A. Ghirardini-G. Faggioli, *Digital forensics*, Andria, 2013.

174 Sul punto, R. Santoro-F. Gravino, *Web e matrimonio canonico: prospettive di analisi della perizia nelle dinamiche processuali*, in *Diritto e Religioni*, 2, 2019, 31 ss., evidenziano che il Consiglio Episcopale Permanente della C.E.I., nella sessione del 14 novembre 2018, ha approvato le determinazioni, in vigore dal 1° gennaio 2019, riguardanti il punteggio delle cause, il contributo delle parti, le perizie, le rogatorie e i costi ammissibili a contributo per le sedi in relazione ai Tribunali ecclesiastici italiani in materia di nullità matrimoniale. Al loro interno, per la prima volta, è stato stabilito anche il compenso per le perizie informatiche disposte dal tribunale e liquidate dal Presidente del collegio giudicante, tenendo conto della complessità

dunque assistendo alla realizzazione di un vero e proprio processo canonico telematico[175], che possa articolarsi attraverso la formazione di un fascicolo digitale composto da *file* nativi, muniti di firma elettronica e consultabili in modo sicuro[176].
Anche l'attività istituzionale della Chiesa cattolica presenta profili inediti nelle sue articolazioni digitali. In particolare, gli strumenti *online* sono preferiti per facilitare il processo di elezione dei rappresentanti di Ordini e Istituti religiosi e per l'adozione delle decisioni più rilevanti. Ne è un esempio la piattaforma *Eligo*, che è predisposta in diverse lingue per i contesti multiculturali che caratterizzano le comunità religiose. Essa favorisce la partecipazione e il coinvolgimento da remoto dei membri delle comunità religiose nazionali ed internazionali, garantendo senso di appartenenza, inclusione e rappresentatività degli Istituti e superando il limite della impossibilità di una presenza fisica[177]. Sono previsti inoltre meccanismi di sicurezza per proteggere l'integrità del voto e assicurare un processo elettorale equo ed affidabile. Gli strumenti offerti (registri elettorali, distribuzione dei voti, tabulazione dei risultati) promuovono efficienza e trasparenza delle operazioni.

5. La salvezza delle anime nella realtà digitale

Le opportunità offerte dalla realtà digitale coinvolgono pienamente l'attività pastorale e istituzionale della Chiesa cattolica, rinnovando l'esercizio dei suoi *tria munera*. Questa prospettiva dimostra che la Chiesa cattolica, che è «esperta in umanità»[178] e attenta ai «segni dei tempi»[179], non considera più il digitale come minaccia ma come strumento di evangelizzazione e pertanto

dell'accertamento e della eventuale necessità per il perito di avvalersi del contributo di altri specialisti.

175 Questa possibilità incontra favori già da una parte della dottrina: Redazione di QDE (a cura della), *Un dossier sul collegamento da remoto nei processi canonici*, in *Quaderni di diritto ecclesiale*, 3, 2021, 323 ss.

176 R. Santoro-P. Palumbo-F. Gravino, *Diritto canonico digitale*, cit., 435 ss., auspicano la creazione di portali di servizi telematici della giustizia ecclesiale per facilitare la comunicazione e lo scambio di documenti e di prassi tra i tribunali diocesani ed interdiocesani.

177 Questa modalità elettiva è stata adottata dalla 77° Assemblea Generale della Conferenza Episcopale Italiana nel maggio 2023. I vantaggi della votazione *online* sono stati rappresentati da una partecipazione degli aventi diritto al voto pari al 96%, una notevole riduzione dei tempi con un aumento dell'efficienza del 90% e la totale assenza di carta stampata che ha inciso sugli obiettivi di sostenibilità ambientale che la Chiesa cattolica si prefigge.

178 Paolo VI, Lettera enciclica *Populorum progressio*, 26 marzo 1967, n. 13, il cui testo integrale è consultabile sul sito *vatican.va*.

179 Francesco, Esortazione apostolica post-sinodale *Christus vivit*, 25 marzo 2019, 9, il cui testo integrale è consultabile sul sito *vatican.va*.

prova ad elaborare ed offrire soluzioni capaci di coniugare l'utilizzo di questi nuovi strumenti con i principi che governano il popolo di Dio.
L'esperienza spirituale, rituale e liturgica, come pure la teologia e il diritto canonico[180], sono chiamati a comprendere la portata di questa rivoluzione digitale nella fede, trovando, quando e se possibile, soluzioni di adattamento e offrendo spazi inediti al senso religioso[181].
Le trasformazioni in atto potrebbero consentire di parlare di un esercizio digitale del culto cattolico. Non bisogna dimenticare, tuttavia, che all'origine di questa fede vi è l'incarnazione di Dio in suo Figlio[182]. Questa "contrapposizione" necessita di un bilanciamento. La realtà *offline* è senza dubbio arricchita dalla dimensione *online*. Demonizzarla significherebbe estromettere la Chiesa da dinamiche relazionali e istituzionali che spesso trovano nell'infosfera l'unica modalità di realizzazione e di sviluppo. L'approccio ecclesiale non si muove in questa direzione, ma apprezza il progresso se è in grado di preservare il valore e la dignità dell'uomo[183].
La presenza sempre più numerosa di evangelizzatori digitali non priva la funzione di insegnare delle sue peculiarità e delle sue finalità. Partecipare a celebrazioni eucaristiche *online* permette in un certo senso al fedele di accostarsi al mistero di Dio, benché l'assenza della materia e dei segni disciplinati non consenta di vivere a pieno e validamente la grazia sacramentale. L'attività di governo trova nello spazio digitale nuove modalità di esercizio che consentono alla Chiesa di affermare la propria *governance* anche in questa dimensione.
Accogliere questi progressi come doni può consentire di considerare il digitale come opportunità[184], un nuovo mezzo con cui il fedele *online* può ottenere la salvezza della propria anima[185] nel rispetto del magistero e della normativa canonica.

---

[180] V. Pacillo, *La libertà di culto di fronte all'emergenza Covid-19. Profili di diritto canonico e di diritto ecclesiastico italiano*, in *Il diritto ecclesiastico*, 1-2, 2019, 14 ss.

[181] Per un approfondimento delle nuove modalità di esercizio del culto nella dimensione virtuale, sia consentito il riferimento a F. Gravino, *Nuovi Movimenti Religiosi (NMR) e metaverso*, in A. Fuccillo-V. Di Nuzzo-R. De Ritis (a cura di), *I diritti costituzionali nel metaverso*, Napoli, 2023, 315 ss.

[182] Sul punto si rinvia ampiamente a J.M. Castillo, *L'umanizzazione di Dio. Saggio di cristologia*, Bologna, 2020.

[183] L.G. Peyron, *Incarnazione digitale. Custodire l'umano nell'infosfera*, Torino, 2019, 33 ss.

[184] A. Fuccillo, *La vita eterna digitale (*digital afterlife*) tra diritto civile e ordinamenti religiosi*, in *Calumet – Intercultural Law and Humanities Review*, 12, 2021, 100 ss.

[185] Sulla salvezza delle anime come fine ultimo dell'ordinamento canonico, P. Erdö, *"Salus animarum: suprema lex". La funzione dei riferimenti della salvezza delle anime nei due Codici della Chiesa cattolica*, in B. Esposito (a cura di), *Il diritto canonico tra salvezza e realtà sociale. Studi scelti in venticinque anni di docenza e pastorale*, Venezia, 2021, 41 ss.

Federico Gravino

Abstract

La digitalizzazione della società ha inciso profondamente anche sulla *governance* della Chiesa cattolica. Essa è pienamente consapevole che l'utilizzo degli strumenti digitali può garantire un esercizio più efficace delle proprie funzioni e un incremento della propria autorevolezza anche nel web. Emergono profili evolutivi nell'esercizio dei *tria munera*: la funzione di insegnare si avvale della realtà *online* per le attività di evangelizzazione e di predicazione; la funzione di santificare interroga sulla validità dell'amministrazione dei sacramenti nei "luoghi" digitali; la funzione di governare utilizza con frequenza sempre maggiore l'infosfera per l'esercizio della potestà legislativa, esecutiva e giudiziaria. Il ricorso ai *new media* è ritenuto parte integrante della missione della Chiesa nel terzo millennio, purché essi contribuiscano «al servizio dell'umanità e alla protezione della nostra casa comune invece che per l'esatto opposto». Il contributo intende esaminare la possibilità che i fedeli possano ottenere anche attraverso la dimensione digitale la salvezza della propria anima.

The digitization of society had a profound impact on the governance of the Catholic Church. It is fully aware that the use of digital tools can ensure a more effective exercise of its functions and an increase in its authority, including on the web. Evolutionary profiles are emerging in the exercise of the *tria munera*: the function of teaching makes use of the online world for evangelization and preaching; the function of sanctifying questions the validity of the administration of the sacraments in digital "places"; the function of governing makes increasing use of the infosphere for the exercise of legislative, executive, and judicial power. The use of new media is considered an integral part of the Church's mission in the third millennium, provided that they contribute "to the service of humanity and the protection of our common home rather than the exact opposite". This contribution aims to examine the possibility that the faithful can also obtain salvation for their souls through the digital dimension.

Keywords

Catholic Church – digital revolution – teaching function – sanctifying function – governing function – salvation of souls

Note

Tempus commissi delicti del reato di omesso controllo *ex* art. 57 c.p.: tra natura istantanea ed effetti (potenzialmente) permanenti*

Federico Riboldi

Corte di cassazione, sez. V penale, ordinanza 11 luglio 2025, n. 32533

L'art. 573, c. 1-bis, c.p.c., introdotto dall'art. 33 d.lgs. 10 ottobre 2022, n. 150, si applica alle impugnazioni per i soli interessi civili proposte relativamente ai giudizi nei quali la costituzione di parte civile sia intervenuta in epoca successiva al 30 dicembre 2022, quale data di entrata in vigore della citata disposizione.
La fattispecie di cui all'art. 57 c.p. è reato d'evento. L'evento è quello che, cagionato dall'autore della pubblicazione a contenuto diffamatorio, il direttore responsabile del periodico, omettendo il controllo, non ha impedito.
Il reato di diffamazione a mezzo internet si consuma nel momento in cui la frase o l'immagine lesiva diventano fruibili da parte di terzi mediante l'inserimento nel "web", con la conseguenza che da quel momento inizia a decorrere il termine di prescrizione del reato.
Il prolungarsi della lesione del bene giuridico protetto dalla norma, derivante dalla perdurante presenza del contenuto diffamatorio on line, non incide sulla struttura del reato di diffamazione, trasformandolo in reato permanente, perché esso è estraneo alla consumazione del reato.

Sommario

1. L'oggetto del ricorso: il *tempus commissi delicti* del reato di cui all'art. 57 c.p. - 2. L'applicabilità *ratione temporis* dell'art. 573, c. 1-bis, c.p.p. e la conseguente devoluzione del ricorso al giudice civile competente. – 3. La ricognizione dei principi di diritto sulla struttura dei reati di omesso controllo e diffamazione e le conseguenze in tema d'individuazione del *tempus commissi delicti*. – 4. L'applicazione dei principi di diritto richiamati dalla Cassazione penale e i potenziali riflessi sul ricorso devoluto al giudice civile.

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

1. L'oggetto del ricorso: il *tempus commissi delicti* del reato di cui all'art. 57 c.p.

L'ordinanza n. 32533/2025, pronunciata dalla V sezione penale della Corte di cassazione, scaturisce dal ricorso della (sola) parte civile avverso una sentenza del Tribunale di Milano, con cui era stata dichiarata l'estinzione - per decorso del termine prescrizionale - dei reati di diffamazione aggravata e omesso controllo nei confronti dell'allora direttore de "Il Giornale".
Nel proprio ricorso, la parte civile aveva censurato la sentenza sul tema concernente l'individuazione del *tempus commissi delicti* con riguardo all'art. 57 c.p.
Secondo la prospettiva del ricorrente, la fattispecie avrebbe natura di reato omissivo permanente e, conseguentemente, la condotta (da correlare non tanto alla prima pubblicazione avvenuta nel 2012, ma alla successiva ripubblicazione, intervenuta nel 2015) sarebbe stata in atto fino alla rimozione dell'articolo dalla rete, operata solo nel 2020.
La decisione, pur rinviando al giudice civile (individuato nella competente sezione civile della Corte di cassazione) per la prosecuzione del giudizio, delinea la cornice giuridica in cui s'inserisce la questione posta dal ricorrente.

2. L'applicabilità *ratione temporis* dell'art. 573, c. 1-bis, c.p.p. e la conseguente devoluzione del ricorso al giudice civile competente

La premessa processuale attiene all'applicabilità dell'art. 573, c. 1-*bis*, c.p.p., introdotto dalla riforma Cartabia, secondo cui: «Quando la sentenza è impugnata per i soli effetti civili, […] la Corte di cassazione, se l'impugnazione non è inammissibile, rinvia [...] per la prosecuzione, [...] alla sezione civile competente, che decide sulle questioni civili utilizzando le prove acquisite nel processo penale e quelle eventualmente acquisite nel giudizio civile».
La Corte, dopo aver richiamato, adesivamente, il principio di diritto elaborato dalle Sezioni Unite nella sentenza n. 38481/2023[1] - secondo cui la nuova disposizione è applicabile alle impugnazioni per i soli effetti civili proposte in relazione ai giudizi in cui la costituzione di parte civile sia in-

[1] Sulla pronuncia delle Sezioni Unite cfr. M. Toriello, *Riforma Cartabia ed impugnazione per i soli interessi civili: le Sezioni Unite sulla non immediata applicabilità dell'art. 573, comma 1-bis c.p.p.*", in *Sistema Penale*, 12 ottobre 2023; F. Del Vecchio, *Applicabilità istantanea o differita dell'art. 573, comma 1-bis, c.p.p. ai giudizi in corso? Questioni (non solo) di diritto transitorio*", in *Processopenaleegiustizia.it*, 2, 2024.

tervenuta in epoca successiva al 30 dicembre del 2022 - e preso atto della data di formalizzazione della stessa (risalente al marzo del 2025), ha ritenuto applicabile - *ratione temporis* - la disposizione in oggetto.
Da qui, a mo' di decalogo, i giudici di legittimità - nel trattare la censura sollevata con l'impugnazione - richiamano numerosi precedenti in tema di diffamazione e omesso controllo del direttore responsabile, rilevanti nella prospettiva di definire la questione giuridica posta dal ricorrente.

3. La ricognizione dei principi di diritto sulla struttura dei reati di omesso controllo e diffamazione e le conseguenze in tema d'individuazione del *tempus commissi delicti*

La Corte, pur avendo escluso l'inammissibilità del ricorso (e, dunque, avendo scartato l'ipotesi di una sua manifesta infondatezza), propone una ricognizione dei principi di diritto elaborati dalla Cassazione – rispetto ai quali v'è, almeno implicitamente, adesione - che, di fatto, indirizza la risoluzione del *thema decidendum*.
Detta ricognizione muove dalla natura di reato istantaneo d'evento che caratterizza la fattispecie di cui all'art. 57 c.p. L'ordinanza, in particolare, ricorda come la giurisprudenza della Corte individui l'evento in quello cagionato dall'autore della pubblicazione a contenuto diffamatorio, che il direttore responsabile, omettendo il controllo, non ha impedito (tanto che, in ragione della coincidenza tra pubblicazione diffamatoria ed evento del reato omissivo, in caso di assoluzione del giornalista dall'imputazione di diffamazione perché il fatto non sussiste o non costituisce reato, deve escludersi la responsabilità penale in capo al direttore[2]).
Una volta richiamato detto inquadramento dogmatico, la Cassazione prosegue nella propria rassegna giurisprudenziale, concentrandosi sulle conseguenze – che da quell'inquadramento derivano - in punto di esatta individuazione del *tempus commissi delicti*. Tema, quest'ultimo, rilevante nell'economia dell'ordinanza, avuto riguardo alle censure proposte con l'impugnazione e incentrate, come visto, sulla decorrenza del termine prescrizionale.
Così, si ricorda, citando una pronuncia del 2022[3], che in caso di diffamazione commessa attraverso l'inserimento di un contenuto sul web, il momento consumativo va individuato in quello in cui la frase o l'immagine

[2] Nella motivazione vengono richiamati due precedenti (Cass. pen., sez. V, 29 aprile 2019, n. 22850, Rossi, Rv. 275556; Cass. pen., sez. V, 12 giugno 1992, n. 8418, Zatterin, Rv. 191929 – 01).

[3] Cass. pen., sez. V, 14 marzo 2022, n. 24585, Sanna, rv. 283400.

lesiva dell'altrui reputazione divengano fruibili per i terzi e, dunque, quando il collegamento sia attivato. Ciò senza possibilità di differire la consumazione in ragione della permanenza *on line* del contenuto diffamatorio, pena la trasformazione della fattispecie in un reato di natura permanente[4].

4. L'applicazione dei principi di diritto richiamati dalla Cassazione penale e i potenziali riflessi sul ricorso devoluto al giudice civile

Proprio il principio di diritto richiamato a conclusione del precedente paragrafo - che l'ordinanza conforta con due precedenti interni alla medesima sezione (oltre a quello già citato nella nota sub 2, anche una seconda pronuncia, sempre del 2022[5]) - appare decisivo per la risoluzione della fattispecie oggetto del ricorso.
Una volta istituita la stretta correlazione tra l'evento del reato di diffamazione e quello di omesso controllo e accolta, allo stesso tempo, l'impostazione elaborata in tema di diffamazione, che rifiuta l'ipotesi della permanenza del reato per il solo fatto che il contenuto diffamatorio rimanga visibile in rete, ad analoga conclusione dovrebbe giungersi anche per la fattispecie di cui all'art. 57 c.p., con la conseguente infondatezza del ricorso, incentrato - come visto - su un inquadramento della norma incriminatrice quale reato omissivo permanente.
Infatti, ove il competente giudice civile si attenesse a all'impostazione dogmatica accolta nell'ordinanza, escludendo che la perdurante presenza della pubblicazione sulla testata web (protrattasi fino al 2020) possa procrastinare il momento consumativo del reato di omesso controllo, la fattispecie di cui all'art. 57 c.p. risulterebbe commessa, al più tardi, nel 2015 (data di ripubblicazione dell'articolo di cui s'ipotizza valenza diffamatoria) e, dunque, la prescrizione sarebbe maturata ben prima della sentenza impugnata.
Né sarebbe decisiva, ai fini di accogliere l'impostazione proposta nel ricorso, la permanenza degli effetti lesivi del reato. Quegli effetti, invero, non conseguono alla reiterazione della condotta (in quanto l'omissione - che rappresenta il fatto tipico previsto dall'art. 57 c.p. - si verifica nel momento della pubblicazione, non prevedendo invece la norma, in capo al direttore

[4] Enfasi aggiunta. Ulteriore corollario di detta impostazione, di cui l'ordinanza fa menzione sempre attraverso la tecnica del rinvio a precedenti decisioni, è la ritenuta (tendenziale) contestualità - o almeno prossimità temporale - tra immissione in rete e cognizione del diffamato, ai fini del calcolo del *dies a quo* per la tempestività della querela (sempre che l'interessato non dia dimostrazione del contrario).

[5] Principio di diritto ribadito anche nella sentenza della Cass. pen., Sez. 5, del 29 novembre 2022, n. 1370, non massimata.

responsabile, obblighi di rimozione presidiati penalmente), ma sono l'effetto della perdurante consultabilità del contenuto web. Sul punto, in via analogica, può risultare utile l'elaborazione giurisprudenziale e dottrinale operata in relazione ad altre fattispecie - caratterizzate da una consumazione istantanea cui, però, si associano effetti permanenti - che hanno affrontato proprio il tema del momento consumativo del reato.
Si veda, ad esempio, la sentenza della Cass. pen., sez. V, 14 febbraio 2020, n. 12929[6], in tema di omesso deposito di bilanci e scritture contabili e fiscali obbligatorie, previsto dagli artt. 220 e 16, c. 1, n. 3 L. Fall., fattispecie che la Suprema Corte delinea come reato omissivo proprio istantaneo, con effetti eventualmente permanenti, che si consuma all'atto dell'inadempimento dell'obbligo di deposito nei tempi previsti dalla legge[7].
Altrettanto significativa risulta la decisione della Cass. pen., sez.un., 28 febbraio 2001, n. 8[8], secondo cui il delitto di trasferimento fraudolento di valori integra un'ipotesi di reato istantaneo con effetti permanenti e si consuma nel momento in cui viene realizzata l'attribuzione fittizia, senza che possa assumere rilevanza il permanere della situazione antigiuridica conseguente alla condotta criminosa.
Da ultimo, risulta pertinente il richiamo a una recente pronuncia in tema di deposito e abbandono incontrollato di rifiuti (Cass. pen., Sez. III, 7 marzo 2022, n. 8088) ove si affronta il tema, controverso, della natura istantanea o permanente della fattispecie e si fornisce un criterio per la distinzione tra le due ipotesi; criterio che può rappresentare un parametro di carattere generale utile, in una prospettiva analogica, anche nel caso di specie. In particolare, i giudici di legittimità, chiariscono che:

«ogni qualvolta l'attività di abbandono ovvero di deposito incontrollato di rifiuti sia prodromica ad una successiva fase di smaltimento o di recupero del rifiuto stesso, caratterizzandosi essa, pertanto, come una forma, per quanto elementare, di gestione del rifiuto (della quale attività potrebbe dirsi che costituisce il "grado zero"), la relativa illiceità penale permea di sé l'intera condotta (quindi sia la fase prodromica che quella successiva), integrando, pertanto, una fattispecie penale di durata, la cui permanenza cessa soltanto con il compimento delle fasi ulteriori rispetto a quella di ri-

[6] In *Dir. Pen. e Processo*, 1, 2021, 42.

[7] La Cassazione, dopo aver precisato che l'eventuale consegna postuma della contabilità non assume efficacia interruttiva di una condotta permanente, bensì rileva in ordine ai profili circostanziali del fatto, ha ritenuto erroneo l'approdo dei giudici di merito che avevano ritenuto sussistere una pluralità di reati in relazione alle annualità a cui si riferiva la contabilità di cui era stata omessa la consegna, e la conseguente applicazione della disciplina della continuazione, in presenza di un'unica violazione, penalmente rilevante.

[8] CED Cassazione, 2001, RV218768

lascio; tutto ciò con le derivanti conseguenze anche a livello di decorrenza del termine prescrizionale. *Nel caso in cui, invece, siffatta attività* non costituisca l'antecedente di una successiva fase volta al compimento di ulteriori operazioni, aventi ad oggetto appunto lo smaltimento od il recupero del rifiuto, ma *racchiuda in sé l'intero disvalore penale della condotta, non vi è ragione di ritenere che essa sia idonea ad integrare un reato permanente; ciò in quanto, essendosi il reato pienamente perfezionato ed esaurito in tutte le sue componenti oggettive e soggettive, risulterebbe del tutto irragionevole non considerarne oramai cristallizzati i profili dinamici fin dal momento dei rilascio del rifiuto, nessuna ulteriore attività e residuando alla descritta condotta di abbandono*»[9].

Ebbene, proprio il criterio utilizzato in quella decisione appare dirimente anche nel caso oggetto della pronuncia qui commentata. Se, infatti, la struttura della fattispecie è incentrata su un dovere di controllo che deve essere esercitato per impedire che col "mezzo della pubblicazione" siano commessi reati, è evidente come il disvalore si manifesti ed esaurisca proprio all'atto della pubblicazione (in questo caso di un contenuto diffamatorio), allorché il direttore abbia omesso, appunto, di esercitare quel dovere impostogli dalla norma incriminatrice.
D'altra parte, nella propria requisitoria, la Procura Generale aveva insistito per il rigetto del ricorso, qualificando la fattispecie di cui all'art. 57 c.p. come reato omissivo improprio che si consuma nel momento in cui si omette il controllo sull'articolo pubblicato e, quindi, alla stessa data dell'articolo (con richiamo alla sentenza della Cass. pen., sez. V, n. 22850 del 24 settembre 2019, Rv. 275556).
In attesa del pronunciamento della Cassazione civile, dunque, la decisione della Suprema Corte rappresenta un utile riferimento al fine di ricostruire la struttura del reato di omesso controllo, i confini della responsabilità del direttore di testata giornalistica e la collocazione temporale della condotta sanzionata dall'art. 57 c.p.

Keywords
editor's failure to exercise control - online defamation - tempus commissi delicti - instantaneous offence - statute of limitations.

[9] Enfasi aggiunta.

Diritto di cronaca giudiziaria: obbligo di verifica degli sviluppi processuali al momento della pubblicazione*

Marco Milani

Corte di cassazione, sez. V penale, 14 gennaio 2026, n. 1589

Il criterio della verità della notizia necessario per integrare l'esimente del diritto di cronaca giudiziaria deve tenere conto degli sviluppi di indagine ed istruttori nonché degli esiti giudiziali al momento della pubblicazione della notizia, onde accertare se la notizia stessa si sia poi rivelata priva di fondamento.

Sommario

1. La vicenda processuale. – 2. L'obbligo di "aggiornamento" della verifica delle fonti. – 3. La "gerarchia" delle fonti utilizzabili dal cronista giudiziario.

1. La vicenda processuale

La sentenza in commento, pronunciata dalla Corte di cassazione, sez. V penale (n. 1589 del 14 gennaio 2026), affronta un caso di diffamazione a mezzo stampa offrendo chiarimenti sui limiti del diritto di cronaca (e di critica) giudiziaria, in particolare riguardo all'onere di verifica delle fonti da parte del giornalista.

Il procedimento trae origine da una querela per diffamazione a mezzo stampa presentata da un soggetto, A.A., contro un giornalista, B.B. Quest'ultimo, in una serie di articoli pubblicati su una testata online, aveva definito A.A. come «capomafia».

Nei primi due gradi di giudizio, il giornalista era stato assolto. La Corte d'Appello di Catania, confermando la decisione di primo grado, aveva ritenuto la condotta dell'imputato scriminata dall'esercizio del diritto di

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

cronaca e di critica, ai sensi dell'art. 51 c.p.
La parte civile, A.A., proponeva ricorso per cassazione, lamentando principalmente la violazione dell'art. 51 c.p.
Il fulcro della doglianza risiedeva nel fatto che i giudici di merito avessero erroneamente applicato la scriminante, non considerando che il giornalista aveva omesso di riportare l'esistenza di sentenze che escludevano l'appartenenza del ricorrente ad associazioni mafiose
La Suprema Corte ha accolto il ricorso della parte civile, annullando la sentenza impugnata ai soli effetti civili e rinviando la causa al giudice civile competente per valore in grado di appello.
Il ragionamento della Corte, dopo aver ribadito i consolidati principi giurisprudenziali secondo cui l'esercizio del diritto di cronaca e di critica, per essere legittimo, deve rispettare tre requisiti (la verità del fatto narrato, l'interesse pubblico alla notizia e la continenza espressiva) si articola su due punti fondamentali: l'errata applicazione del principio sulla verità della notizia nonchè l'inadeguatezza delle fonti utilizzate dal giornalista.

2. L'obbligo di "aggiornamento" della verifica delle fonti

Nel caso di specie, la Corte di Cassazione ha rilevato che il requisito della verità del fatto storico non era stato rispettato. La Corte d'Appello aveva giustificato la condotta del giornalista affermando che la verifica delle fonti «non implica che si debba tener conto di tutti i successivi accertamenti giudiziali»[1]. La Suprema Corte, pur riconoscendo la correttezza di tale principio in linea generale, lo ha giudicato "inconferente" al caso specifico.
La ragione di tale inconferenza è cruciale:
«Ora, in motivazione è asserito che la verifica delle fonti circa la verità della notizia "non implica che si debba tener conto di tutti i successivi accertamenti giudiziali". Tale principio, di per sé corretto [...], è richiamato dalla Corte territoriale in maniera inconferente, posto che, come già osservato, nel caso in scrutinio l'accertamento giudiziale (la sentenza di assoluzione per il delitto di cui all'art. 416-bis cod. pen. pronunciata in appello) non era successivo alla pubblicazione degli articoli, bensì precedente».
La sentenza di assoluzione di A.A. dall'imputazione di associazione mafiosa era stata pronunciata dalla Corte d'Appello di Catania il 27 luglio 2018, mentre gli articoli diffamatori erano stati pubblicati tra il 1° e il 4 dicembre 2018. Pertanto, al momento della pubblicazione, la notizia dell'appartenenza di A.A. ad un'associazione mafiosa era già stata smentita da una pronuncia giudiziale definitiva.
La Corte sottolinea che il giornalista ha un «particolare onere di verificare

[1] Cass. pen., sez. V, 16 novembre 2010, n. 43382, Rv. 248950-01;

gli esiti giudiziali» di un procedimento, specialmente se risalente nel tempo, «onde accertare se la notizia stessa si sia poi rivelata priva di fondamento, tanto da comportare l'assoluzione dell'accusato». Omettendo di verificare e riportare l'assoluzione, il giornalista ha violato il dovere di diligenza e ha presentato una realtà fattuale non veritiera.
La pronuncia in commento si pone in conformità con precedenti sentenze di legittimità secondo le quali il giornalista ha l'obbligo di accertare se la notizia si sia successivamente rivelata priva di fondamento, particolarmente nel caso in cui sia intervenuta l'assoluzione dell'imputato.[2]

3. La "gerarchia" delle fonti utilizzabili dal cronista giudiziario

Il secondo punto di censura accolto dalla Corte riguarda la natura delle fonti su cui il giornalista aveva basato i suoi articoli. L'imputato aveva attinto le informazioni da relazioni della Direzione Investigativa Antimafia (DIA) e dalla testimonianza di un membro della Commissione parlamentare antimafia.
La Corte di Cassazione ha stabilito che tali fonti, di natura amministrativa e politica, non sono sufficienti a fondare con certezza la qualifica di «appartenente a un'associazione mafiosa». La Corte afferma in modo netto:
«[...] resta il fatto 1) che la misura di prevenzione non è stata applicata per il reato di associazione mafiosa e 2) che la qualifica di appartenente a un'associazione mafiosa (in qualità di partecipe ovvero con ruolo di vertice), data per assodata negli articoli incriminati, non può farsi derivare né da una testimonianza di un membro di una Commissione parlamentare né da una relazione della Direzione investigativa antimafia, bensì soltanto da un provvedimento giurisdizionale, come correttamente ritenuto dal ricorrente».
Questo passaggio stabilisce una chiara gerarchia: la qualificazione giuridica di un soggetto come «mafioso» può derivare unicamente da un accertamento giudiziario. Le relazioni investigative o le dichiarazioni politiche, pur potendo costituire una fonte di notizia, non possono prevalere su una sentenza passata in giudicato né possono essere utilizzate per attribuire a un individuo uno status criminale che la giustizia ha escluso.
La sentenza in commento, dunque, consolida e precisa importanti principi

[2] Cass. pen., sez. V, 3 giugno 2021, n. 21703, V., *CED,* 281211-01; Cass. pen., sez I, 2 aprile 2015, n. 13941, C., *CED*, 263064. In dottrina Pezzella, *La diffamazione*, Milano, 2026, 646 ha sottolineato che «quando si offre il resoconto di fatti distanti nel tempo, in relazione ai quali è legittimo pretendere una attenta verifica di tutte le fonti disponibili» vi è come conseguenza «l'obbligo di accertare e rappresentare compiutamente lo sviluppo degli esiti processuali" delle vicende giudiziarie di cui il giornalista abbia dato conto».

in materia di diffamazione e diritto di cronaca.
Innanzitutto, la verità del fatto va Intesa come "verità storica aggiornata": il requisito della verità non si esaurisce nella corrispondenza tra il narrato e il contenuto di una fonte originaria (es. un atto di indagine), ma impone al giornalista un dovere di diligenza e aggiornamento, specialmente in ambito giudiziario. Se un fatto giudiziario ha avuto un'evoluzione (in questo caso, un'assoluzione), il giornalista è tenuto a darne conto, soprattutto se tale evoluzione è precedente alla pubblicazione della notizia.
In secondo lugo, individua una "gerarchia" delle fonti giornalistiche: un provvedimento giurisdizionale ha un peso probatorio e una valenza superiore rispetto a fonti di natura amministrativa (relazioni DIA) o politica (Commissioni parlamentari) quando si tratta di attribuire qualifiche giuridiche precise, come l'appartenenza a un'associazione mafiosa.

Keywords
defamation by the press – judicial reporting privilege – verification of sources – hierarchy of journalistic sources – statute of limitations

Cronache e commenti

La Direttiva anti-SLAPP tra libertà di espressione, abuso del processo e tutela del pluralismo democratico*

Carlo Melzi d'Eril

Non leggo mai i giornali al mattino
perché stampano solo quello che voglio io
Napoleone III di Francia

Sommario

1. Premessa – 2. Partecipazione pubblica, libertà di espressione e tutela della reputazione nella giurisprudenza europea – 3. Le SLAPP tra abuso del processo e finalità dissuasive – 4. Il contrasto all'abuso del processo nella direttiva (UE) 2024/1069 – 4.1. Gli strumenti di tutela anticipata e la prevenzione del *chilling effect* – 5. Gli effettivi della Direttiva nell'ordinamento italiano – 6. Considerazioni conclusive

1. Premessa

Anche nell'ordinamento italiano si va progressivamente consolidando il dibattito relativo ai limiti che i principi dello Stato costituzionale di diritto impongono all'esercizio del potere punitivo e, più in generale, all'impiego di strumenti giurisdizionali suscettibili di incidere sull'effettivo esercizio di libertà fondamentali. In tale prospettiva, assume crescente rilievo l'esigenza che le disposizioni sostanziali e processuali siano formulate dal legislatore e applicate dall'autorità giudiziaria in modo tale da evitare che, oltre a condotte effettivamente illecite, siano disincentivati anche comportamenti leciti nei quali si concreta l'esercizio di diritti costituzionalmente garantiti. È in questo quadro che si colloca la categoria del *chilling effect* o "effetto di raffreddamento", tradizionalmente impiegata per descrivere quelle situazioni nelle quali il timore della sanzione o dell'esposizione al contenzioso

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

induce i destinatari della norma a forme di autocensura e di autolimitazione nell'esercizio delle proprie libertà fondamentali[1]. L'effetto deterrente prodotto dall'ordinamento eccede, pertanto, l'ambito delle condotte vietate e finisce per incidere anche su comportamenti pienamente leciti, determinando una compressione indiretta dello spazio di esercizio dei diritti fondamentali.

Il problema assume particolare rilevanza nei settori in cui l'effetto dissuasivo derivante dal ricorso a strumenti giudiziari non si riflette soltanto sulla posizione individuale del destinatario, ma incide sulle condizioni strutturali del sistema democratico. Emblematico è il caso della libertà di espressione e della libertà di stampa, quali presupposti essenziali del pluralismo informativo e del controllo diffuso sull'esercizio del potere pubblico[2]. In tale contesto, la funzione di *watchdog of democracy* propria del giornalismo impone all'ordinamento di assicurare un equilibrato contemperamento tra tutela della reputazione, diritto di azione e salvaguardia del dibattito pubblico[3].

È precisamente in questo spazio di tensione che si colloca il fenomeno delle *Strategic Lawsuits Against Public Participation* (SLAPP): azioni giudiziarie promosse non tanto per ottenere la tutela di diritti soggettivi asseritamente lesi, quanto piuttosto per intimidire, silenziare o scoraggiare chi diffonde informazioni, opinioni o svolge attività di interesse pubblico. Le SLAPP costituiscono, dunque, una forma particolarmente sofisticata di abuso del processo, nel quale lo strumento giurisdizionale viene piegato a mezzo di pressione indiretta sulla libertà di espressione, con l'effetto di trasformare il diritto di azione in uno strumento di intimidazione.

La questione è di recente tornata al centro dell'agenda dell'Unione europea con l'adozione dell'*European Democracy Action Plan*[4]*,* tra i cui obiettivi fi-

---

[1] G. Manca, *Il raffreddamento di diritti fondamentali come limite alla politica criminale*, Milano, 2024, *passim*.

[2] Ivi, 29-30. Un altro ambito in cui l'effetto di raffreddamento non si limita a compromettere libertà fondamentali del singolo, ma si riflette sul funzionamento stesso del sistema democratico, concerne il dibattito relativo al reato di abuso d'ufficio e al suo rapporto con il principio di buona amministrazione della *res publica*.

[3] Per stare solo alla giurisprudenza europea, *ex multis* CEDU, *Goodwin c. Regno Unito,* ric. 28957/95 (2011); CEDU, *Cumpănă c. Romania*, ric. 33348/96 (2004); CEDU *Katrami c. Grecia,* ric. 19331/05 (2007).

[4] Il Piano d'azione per la democrazia europea, presentato dalla Commissione il 3 dicembre 2020, evidenzia l'importanza di un sistema mediatico libero e pluralistico nel garantire ai cittadini la possibilità di assumere decisioni consapevoli, nonché nel contrastare i fenomeni di manipolazione dell'informazione e le interferenze nello spazio informativo, inclusa la disinformazione. In tale quadro, la Commissione ha adottato la raccomandazione (UE) 2021/1534, volta a garantire la protezione, la sicurezza e l'*empowerment* dei giornalisti e degli altri professionisti dei media nell'Unione europea, successivamente integrata dalla raccomandazione (UE) 2022/758, finalizzata a fronteggiare la specifica minaccia rappresentata dai procedimenti

gurano la promozione della libertà di espressione e la tutela del pluralismo dei media[5], e la direttiva (UE) 2024/1069[6].

2. Partecipazione pubblica, libertà di espressione e tutela della reputazione nella giurisprudenza europea

Le norme di riferimento in materia sono l'art. 10 CEDU e l'art. 11 della Carta dei diritti fondamentali dell'Unione europea, entrambe nella lezione della Corte europea dei diritti dell'uomo ai sensi dell'art. 52, par. 3, della Carta.

In tale prospettiva, la Corte EDU ha elaborato un'interpretazione particolarmente ampia della libertà di espressione, estendendone la tutela sia sul piano soggettivo sia su quello oggettivo. La protezione convenzionale si applica, infatti, non soltanto alle persone fisiche, ma anche ad associazioni, organizzazioni non governative, operatori dell'informazione e persone giuridiche, indipendentemente dal mezzo di comunicazione (stampa tradizionale, servizi radiotelevisivi, piattaforme digitali)[7]. Parallelamente, anche le nozioni di "informazione", "opinione" e "idea" sono state interpretate in senso ampio, sino a ricomprendere qualsiasi forma di manifestazione del pensiero rivolta alla sfera pubblica, indipendentemente dalla natura politica, economica, scientifica, artistica o commerciale del contenuto[8]. In questa prospettiva, la libertà di espressione non si configura soltanto come un diritto individuale, ma assume una funzione essenziale per il pluralismo democratico e la formazione di un'opinione pubblica libera e informata.

La giurisprudenza convenzionale ha così valorizzato, accanto alla dimensione individuale della libertà di espressione, anche la funzione collettiva della libertà di stampa, quale condizione indispensabile per il corretto svolgimento del dibattito democratico.

---

giudiziari manifestamente infondati o abusivi diretti a ostacolare la partecipazione al dibattito pubblico.

[5] Nel discorso di presentazione del Piano d'azione per la democrazia europea, la Presidente della Commissione Europea Ursula von del Leyen ha dichiarato: «Con la rivoluzione digitale in corso, i cittadini devono poter compiere le loro scelte esprimendo liberamente le proprie opinioni. La realtà va distinta dalla finzione, e mezzi di informazione liberi e la società civile devono poter partecipare a un dibattito aperto e libero da interferenze malevoli. Per questo l'UE prende misure per rendere più resilenti le nostre democrazie».

[6] S. Riccardelli, *La tutela della libertà di stampa nell'Unione europea: recenti passi avanti alla luce del caso Real Madrid Club de Futbol e della direttiva anti-SLAPP,* in *DeS*, 4, 2024, 11.

[7] B. Nascimbene - F. Rossi Dal Pozzo, *L'evoluzione dei diritti e delle libertà fondamentali nel settore dei media. Diritto dell'Unione europea, orientamenti giurisprudenziali e recenti interventi normativi,* in *Eurojus*, 1, 2023, 3.

[8] *Ex multis* CEDU, *Radio France c. Francia*, ric. 53984/00 (2003).

La stessa direttiva (UE) 2024/1069 recepisce espressamente tale impostazione, precisando al considerando 7:
I giornalisti svolgono un ruolo importante nel facilitare il dibattito pubblico e nello scambio di informazioni, opinioni e idee. Dovrebbero essere in grado di svolgere la loro attività in modo efficace e senza timori al fine di garantire che i cittadini abbiano accesso a una pluralità di opinioni nelle democrazie europee. Un giornalismo indipendente, professionale e responsabile, nonché l'accesso a un'informazione pluralistica, sono pilastri fondamentali della democrazia. È essenziale che i giornalisti dispongano dello spazio necessario per contribuire a un dibattito aperto, libero ed equo e per contrastare la disinformazione, la manipolazione delle informazioni e le ingerenze, conformemente all'etica del giornalismo, e che sia accordata loro protezione quando agiscono in buona fede.
Parallelamente, la tutela della reputazione ha acquisito crescente rilevanza con il suo inquadramento nell'ambito di applicazione dell'art. 8 CEDU e dell'art. 7 della Carta, quali espressione del diritto all'identità personale e alla vita privata. Il rapporto tra libertà di espressione e tutela reputazionale viene quindi affrontato dalla Corte EDU mediante un giudizio di bilanciamento fondato sul criterio della "necessità in una società democratica", interpretato alla luce dei principi di proporzionalità e *pressing social need*[9].
È in questo contesto che il *chilling effect* assume rilievo sistematico quale parametro di valutazione della compatibilità delle restrizioni con le esigenze della democrazia pluralista.

3. Le SLAPP tra abuso del processo e finalità dissuasive

Le *Strategic Lawsuits Against Public Participation* (SLAPP) non sono che una manifestazione paradigmatica dell'uso distorto dello strumento processuale quale mezzo di pressione indiretta sull'esercizio delle libertà fondamentali. La nozione, originariamente elaborata dalla dottrina statunitense alla fine degli anni Settanta[10], individua le azioni giudiziarie promosse con

[9] Da ultimo CEDU, *Morice c. Francia,* ric. 29369/10 (2025); CEDU, *Belpietro c. Italia*, ric. 43612/10 (2013).

[10] Negli Stati Uniti, i primi interventi legislativi risalgono al 2008 nello Stato di New York e al 2010 a livello federale. L'Unione europea ha avvertito l'esigenza di introdurre una normativa anti-SLAPP solo dopo l'assassinio della giornalista maltese Daphne Caruana Galizia nell'ottobre 2017. Al momento della sua morte, Caruana Galizia era convenuta in ben 47 procedimenti giudiziari a Malta e all'estero, intentati per lo più da influenti attori economici e politici in ragione delle sue rivelazioni, pubblicate su carta e/o online, riguardanti presunte pratiche corruttive. Sul punto, C. Kohler, *Private international law aspects of the European Commission's proposal for directive on SLAPPs ("Strategic Lawsuits Against Public Participation"),* in *Rivista di Diritto Internazionale Privato e Processuale*, 4, 2022, 813; E. Benvenuti, *Azioni strategiche*

l'obiettivo di intimidire o scoraggiare soggetti che abbiano espresso opinioni critiche o diffuso informazioni di interesse pubblico suscettibili di incidere sugli interessi economici, politici o reputazionali dell'attore[11].
La peculiarità del fenomeno risiede nella dissociazione tra la funzione dichiarata dell'azione e l'effetto concretamente perseguito. Sebbene in apparenze dirette alla tutela della reputazione o di altri diritti della personalità, tali iniziative mirano in realtà a produrre un effetto dissuasivo sull'esercizio della libertà di espressione e sulla partecipazione al dibattito pubblico. In questa prospettiva, il processo viene piegato a finalità diverse da quella propriamente giurisdizionale, trasformandosi da sede di composizione del conflitto a mezzo di pressione nei confronti di chi esercita attività di informazione o partecipazione pubblica.
Da ciò consegue che l'effetto intimidatorio tipico delle SLAPP non dipende tanto della fondatezza della pretesa azionata, quanto dal semplice coinvolgimento del destinatario nel circuito processuale. L'onerosità del contenzioso, la durata del procedimento, l'incertezza dell'esito e il pregiudizio reputazionale derivante dall'esposizione giudiziaria concorrono infatti a generare forme di autocensura, suscettibili di trascendere il caso concreto e di incidere più ampiamente sulle condizioni di esercizio della libertà di informazione.
Sotto il profilo strutturale, le SLAPP presentano elementi ricorrenti, valorizzati anche dal legislatore europeo: la manifesta infondatezza, totale o parziale, della domanda; la sproporzione delle pretese risarcitorie; l'asimmetria di potere tra le parti[12]; il ricorso a strategie dilatorie; la proliferazione di procedimenti; nonché il frequente ritiro dell'azione in una fase avanzata del giudizio, una volta prodotto l'effetto intimidatorio.
Particolarmente significativa è la dimensione transnazionale assunta dal

tese a dissuadere la partecipazione pubblica e tutela delle libertà di espressione e informazione nel diritto internazionale privato dell'Unione europea, in *Freedom, Security & Justice: Europea Legal Studies*, 1, 2024, 131 ss.

[11] P. Mazza, *La Direttiva UE 1069/2024 (meglio nota come anti-SLAPP): ovvero, il diritto processuale civile al servizio della "partecipazione pubblica". Un commento a prima lettura,* in *DPCIeC*, 3, 2024.

[12] Nel considerando 15 della Direttiva in esame si legge: «Le SLAPP sono generalmente avviate da entità potenti, ad esempio individui, gruppi di lobby, società, politici e organi statali, nel tentativo di mettere a tacere il dibattito pubblico. Sono spesso caratterizzate da una situazione di squilibrio tra le parti, in cui l'attore si trova in una posizione finanziaria o politica più forte rispetto al convenuto. Un simile squilibrio di potere, pur non essendo un elemento indispensabile di tali casi, ove presente, aumenta in misura significativa le conseguenze negative e l'effetto dissuasivo dei procedimenti giudiziari tesi a bloccare la partecipazione pubblica. Ove presente, l'abuso del vantaggio economico e dell'influenza politica da parte dell'attore nei confronti del convenuto, unitamente all'assenza di fondatezza giuridica, desta particolare preoccupazione se i procedimenti giudiziari abusivi in questione sono finanziata direttamente o indirettamente dai bilanci statali e sono combinati con altre misure statali indirette e dirette contro organizzazioni di media indipendenti, il giornalismo indipendente e la società civile».

fenomeno nell'ambiente digitale. La diffusione di contenuti online, se da un lato amplia il potenziale offensivo della comunicazione, dall'altro consente all'attore di sfruttare la circolazione globale per finalità strategiche. L'accessibilità da una pluralità di ordinamenti consente infatti la selezione del foro ritenuto più favorevole alla tutela della reputazione rispetto alla libertà di espressione (c.d. *forum shopping*), nonché la promozione di azioni parallele dinanzi alle autorità giudiziarie di diversi Stati[13].

La rilevanza costituzionale del fenomeno emerge nella misura in cui esso altera il tradizionale paradigma di bilanciamento tra libertà di espressione e tutela della reputazione. Nella configurazione classica, tale conflitto è composto dal giudice mediante una valutazione caso per caso, fondata su criteri quali la verità della notizia, l'interesse pubblico all'informazione e la continenza espressiva, secondo parametri consolidati dalla giurisprudenza e sintetizzati nel c.d. "decalogo del giornalista"[14]. In tale prospettiva, il processo rappresenta il luogo fisiologico di mediazione tra diritti concorrenti. Le SLAPP alterano tale assetto. Il processo non opera più quale strumento neutrale di tutela giurisdizionale, ma diviene esso stesso fattore di compressione della libertà di espressione. L'abuso del processo assume così una dimensione ulteriore rispetto alla mera violazione dei doveri di correttezza processuale ed efficienza, incidendo indirettamente sulle condizioni di funzionamento dello spazio pubblico.

4. Il contrasto all'abuso del processo nella direttiva (UE) 2024/1069

La Direttiva in commento si inserisce coerentemente nel percorso evolutivo delineato dalla giurisprudenza convenzionale ed eurounitaria in materia di tutela della libertà di espressione e di contrasto agli effetti dissuasivi derivanti dall'uso distorto dello strumento processuale.

Ai sensi dell'art. 1, la Direttiva «stabilisce garanzie contro domande manifestamente infondate o procedimenti giudiziari abusivi in materia civile con implicazioni transfrontaliere avviati nei confronti di persone fisiche o giuridiche in ragione della loro partecipazione pubblica». La tutela della *public participation* costituisce, dunque, il baricentro assiologico dell'intervento europeo, nella misura in cui la partecipazione al dibattito pubblico è intesa come espressione diretta delle libertà democratiche garantite dall'ordina-

[13] E. Benvenuti, *Azioni strategiche tese a dissuadere la partecipazione pubblica e tutela delle libertà di espressione e informazione nel diritto internazionale privato dell'Unione europea,* cit., 135 ss.

[14] Da ultimo V. Pezzella, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca delle fake news, degli hate speeches e dell'intelligenza artificiale,* Milano, 2026, 376 ss.

mento dell'Unione.
La Direttiva ovviamente non mette in discussione il diritto di accesso alla giustizia, tutelato dall'art. 6 CEDU e dall'art. 47 della Carta, ma introduce un controllo sulle modalità di esercizio del diritto di azione per impedirne un utilizzo incompatibile con la funzione propria del processo. Il legislatore europeo guarda non solo alla legittimità astratta della domanda giudiziale, ma a una serie di indici sintomatici dell'abusività dell'azione, quali la sproporzione delle pretese, la reiterazione delle iniziative giudiziarie, il ricorso a condotte intimidatorie o moleste e l'utilizzo in mala fede di strategie dilatorie.
Particolarmente significativo è il considerando 29 della Direttiva, secondo cui anche domande parzialmente fondate assumono carattere abusivo ove accompagnate da richieste manifestamente eccessive o sproporzionate. Il legislatore europeo introduce così una sorta di bilanciamento "di secondo livello", nel quale oggetto di scrutinio non è soltanto il conflitto tra libertà di espressione e tutela della reputazione, ma anche la compatibilità delle modalità di esercizio della tutela giurisdizionale con le condizioni strutturali del pluralismo democratico.
Permangono, tuttavia, alcune criticità connesse all'ambito applicativo della Direttiva. Pur riconoscendo espressamente che pratiche volte a prevenire, limitare o penalizzare la partecipazione pubblica possano manifestarsi in qualunque settore (considerando 17), essa circoscrive il proprio ambito di applicazione alle sole controversie di natura civile e commerciale.
Ulteriori profili problematici emergono con riferimento alla nozione di "implicazioni transfrontaliere" di cui all'art. 5, secondo cui: «Ai fini della presente direttiva si ritiene che una questione presenti implicazioni transfrontaliere a meno che entrambe le parti siano domiciliate nello stesso Stato membro in cui è situato l'organo giurisdizionale adito e tutti gli altri elementi pertinenti alla situazione in questione siano situati unicamente in tale Stato membro». Quanto al requisito del domicilio delle parti, non sembrano porsi particolari difficoltà interpretative. Controversa appare, invece, la seconda condizione. Sul punto, la dottrina si è interrogata sulla effettiva estensione della nozione di transnazionalità rilevante ai fini dell'applicazione della Direttiva. Da un lato, la rubrica dell'art. 5 – "Questioni con implicazioni transfrontaliere" – sembra favorire una lettura ampia della disposizione, suscettibile di includere anche controversie nelle quali la dimensione transfrontaliera attenga non tanto alla struttura della fattispecie, quanto piuttosto alle relative conseguenze. In tale prospettiva, il requisito transfrontaliero potrebbe ritenersi integrato anche quando gli effetti della decisione siano destinati a prodursi in un altro Stato membro, pur in presenza di una vicenda sostanzialmente interna. Dall'altro lato, la formulazione dell'art. 5 pare orientare verso un'interpretazione più restrittiva. La disposizione richiede, infatti, che tutti gli altri elementi pertinen-

ti alla situazione considerata non «siano situati unicamente» nello Stato membro dell'autorità adita, lasciando intendere che il carattere transfrontaliero debba riferirsi agli elementi costitutivi della fattispecie concreta e non tanto ai suoi effetti[15].

4.1. Gli strumenti di tutela anticipata e la prevenzione del *chilling effect*

La prospettiva delineata dalla Direttiva trova concreta attuazione negli strumenti di tutela anticipata predisposti dal legislatore europeo per neutralizzare tempestivamente gli effetti dissuasivi delle SLAPP. La nuova disciplina muove, infatti, dalla consapevolezza che il pregiudizio prodotto da tali iniziative giudiziarie non coincide con l'accoglimento della domanda, ma si realizza al momento della semplice instaurazione del procedimento e si nutre della sua pendenza. È verosimile che il convenuto, in pendenza di giudizio, si astenga dal proseguire l'attività informativa o divulgativa oggetto del contenzioso, sia per il timore delle conseguenze economiche e reputazionali derivanti dalla lite, sia per l'incertezza connessa all'esito del procedimento[16]. A ciò deve aggiungersi che spesso l'effetto deterrente prodotto dall'azione giudiziaria si proietta oltre la posizione del singolo destinatario, inducendo anche altri soggetti coinvolti nel dibattito pubblico ad adottare forme di autocensura rispetto a temi analoghi.

In questa prospettiva, gli strumenti di tutela anticipata introdotti dalla Direttiva, con la compressione del tempo del giudizio che portano con sé, perseguono l'obiettivo di impedire che il processo stesso possa essere usato come strumento di pressione indiretta. Particolare rilievo assumono, in tal senso, la possibilità per il convenuto di richiedere la costituzione di una cauzione a copertura delle spese processuali e, se del caso, dei danni derivanti dal procedimento (art. 10), il rigetto anticipato delle domande manifestamente infondate (art. 11), nonché la previsione di sanzioni o altre misure altrettanto efficaci nel dissuadere l'attore dal promuove un giudizio abusivo (art. 15). La Direttiva impone agli Stati membri di garantire che tali richieste siano trattate secondo modalità accelerate conformemente al diritto nazionale, proprio in ragione della necessità di limitare gli effetti del contenzioso.

La funzione deterrente di tali strumenti emerge con particolare evidenza dalla previsione secondo cui i rimedi introdotti operano indipenden-

[15] P. Mazza, *La Direttiva UE 1069/2024 (meglio nota come anti-SLAPP): ovvero, il diritto processuale civile al servizio della "partecipazione pubblica". Un commento a prima lettura,* cit., 686.

[16] L. Ricchiuti, *La Direttiva 2024/1069/UE sulle azioni giudiziarie temerarie*, in *Cassazione Penale*, 9, 2025, 2987.

temente da eventuali successive modifiche della domanda o da atti processuali depositati in seguito dall'attore, compreso il ritiro dell'azione. La scelta normativa risponde all'esigenza di preservare l'effettività della tutela ed evitare che la natura temeraria del processo possa sottrarsi al controllo giurisdizionale mediante il ricorso a strategie elusive.
Con riferimento alla libertà di espressione, dunque, l'introduzione di strumenti di tutela anticipata riflette una concezione del processo attenta non soltanto alla protezione delle posizioni soggettive delle parti, ma anche alla salvaguardia delle condizioni strutturali del pluralismo informativo e della partecipazione democratica. La prevenzione dell'effetto dissuasivo prodotto dal contenzioso abusivo diviene così parte integrante della tutela delle libertà fondamentali garantite dall'ordinamento.
Accanto ai meccanismi di tutela anticipata, la Direttiva introduce forme di protezione *ex post*. L'art. 16 impone infatti agli Stati membri di negare il riconoscimento e l'esecuzione delle decisioni emesse dalle autorità giudiziarie di Stati terzi all'esito di procedimenti avviati contro persone attive nella partecipazione pubblica e domiciliate nell'Unione europea. Più precisamente, la norma si riferisce a quei procedimenti che sarebbero considerati manifestamente infondati o abusivi secondo il diritto nazionale dello Stato membro nel quale sono richiesti il riconoscimento o l'esecuzione.
La disciplina europea introduce infine un criterio speciale di giurisdizione, in base al quale è consentito alla vittima di SLAPP di agire in giudizio dinanzi alle corti dello Stato membro di domicilio per chiedere il risarcimento dei danni e delle spese patiti a causa dell'azione temeraria avviata in uno Stato terzo.

5. Gli effetti della Direttiva nell'ordinamento italiano

Il fenomeno delle SLAPP nell'ordinamento italiano si colloca all'interno di un quadro normativo articolato, caratterizzato dalla coesistenza di strumenti di tutela di natura penale, civile e settoriale, posti a presidio della reputazione e della riservatezza personale (si pensi al reato di diffamazione, alle azioni risarcitorie o ai rimedi cautelari e inibitori). Sebbene rispondano all'esigenza di garantire interessi costituzionalmente rilevanti, tali strumenti possono prestarsi a un impiego distorto, orientato alla neutralizzazione del dibattito pubblico e alla dissuasione dell'attività informativa e partecipativa[17].
I rimedi attualmente previsti dall'ordinamento interno, pur astrattamen-

[17] I dati raccolti dalla *Coalition Against SLAPPs in Europe* (CASE) rivelano che negli ultimi due anni l'Italia ha registrato il numero più alto di azioni temerarie.

te configurabili[18], trovano nella pratica un'applicazione giurisprudenziale limitata e una scarsa capacità di incidere sulle dinamiche strutturali del fenomeno Si tratta, infatti, di strumenti che operano *ex post,* ossia in una fase successiva all'avvio dell'azione giudiziaria, quando l'effetto deterrente si è già prodotto. Per questo motivo risultano poco efficaci nel prevenire l'uso strategico del processo.

Quanto all'attuazione della Direttiva, il quadro italiano presenta profili di particolare criticità[19]. Il termine per il recepimento, fissato al 7 maggio 2026, è decorso senza che il legislatore nazionale abbia provveduto a una piena implementazione della disciplina europea. La recente Legge 17 maggio 2026, n. 36, ha infatti conferito al Governo una delega per il recepimento della Direttiva, indicando quale unico criterio direttivo specifico la necessità di «definire la nozione di "questioni con implicazioni transfrontaliere" di cui all'articolo 5 della direttiva (UE) 2024/1069, sulla base della condizione negativa prevista dal paragrafo 1 del medesimo articolo 5» (art. 6 l. 36/2026), riproponendo così le problematiche interpretative già evidenziate in precedenza.

Il legislatore nazionale, nonostante le sollecitazioni provenienti dall'Ordine dei giornalisti e dalla società civile, ha pertanto circoscritto l'operatività delle garanzie previste dalla Direttiva alle sole controversie transfrontaliere, sebbene la maggior parte delle SLAPP presenti carattere esclusivamente interno[20]. Una simile impostazione appare difficilmente conciliabile con la *ratio* dell'intervento europeo: l'obiettivo di proteggere i soggetti coinvolti nel dibattito pubblico da procedimenti giudiziari manifestamente infondati o abusivi risulta, infatti, del tutto indipendente dalla dimensione transfrontaliera della controversia.

In questa prospettiva, anche la raccomandazione (UE) 2022/758 dell'aprile 2022 nel considerando 21 invita gli Stati membri «a inserire nei rispettivi ordinamenti giuridici nazionali garanzie per i casi interni analoghe a quelle previste dagli strumenti dell'Unione volti ad affrontare i procedimenti giu-

[18] Un esempio è dato dall'art. 96 c.p.c., ai sensi del quale: «Se risulta che la parte soccombente ha agito o resistito in giudizio con mala fede o colpa grave, il giudice, su istanza dell'altra parte, la condanna, oltre che alle spese, al risarcimento dei danni, che liquida, anche d'ufficio nella sentenza». Tuttavia, si tratta di un rimedio scarsamente applicato che interviene solo *ex post*, ossia una volta che il giudizio si è concluso e l'effetto deterrente si è prodotto. A ciò deve aggiungersi che l'accertamento della responsabilità aggravata risulta particolarmente complesso, in ragione dell'onere probatorio gravante sulla parte istante, la quale deve dimostrare la sussistenza del dolo o della colpa grave in capo al soggetto agente.

[19] G.E. Vigevani – N. Canzian – M. Cecili, *Monitoraggio del pluralismo dell'informazione nell'Unione europea. Risultati di MPM2025. Paese: Italia*, Centre for Media Pluralism and Media Freedom (CMPF), European University Institute, Firenze, 2025.

[20] Dal Report CASE 2025 si evince che oltre il 90% dei casi registrati assume una dimensione puramente domestica.

diziari civili manifestamente infondati o abusivi tesi a bloccare la partecipazione pubblica che presentano implicazioni transfrontaliere». Se è vero che i procedimenti avviati in uno Stato membro nei confronti di una persona residente in un altro Stato membro comportano, di regola, maggiori oneri economici e processuali per il convenuto, soltanto un'estensione delle medesime garanzie anche alle controversie interne assicurerebbe una tutela realmente coerente ed efficace.
Parimenti disatteso è rimasto il richiamo contenuto nel considerando 20 della medesima Raccomandazione, secondo cui: «[…] gli Stati membri dovrebbero garantire che i rispettivi quadri giuridici disciplinanti i procedimenti civili, penali, commerciali e amministrativi prevedano le garanzie necessarie per affrontare tali procedimenti giudiziari, nel pieno rispetto dei valori democratici e dei diritti fondamentali […]». Tale profilo assume rilievo ancora maggiore ove si consideri che la Direttiva non trova applicazione nei casi in cui l'esame dell'azione civile esercitata in sede penale non sia integralmente disciplinato dal diritto processuale civile. Poiché, infatti, nell'ordinamento italiano l'azione civile esercitata nell'ambito del processo penale resta assoggettata alla disciplina processualpenalistica, la normativa europea non sembra destinata a trovare applicazione.
Ne deriva il rischio che il recepimento nazionale si traduca in una sostanziale riproduzione minimale della Direttiva, priva di un'effettiva capacità innovativa e inidonea a incidere in modo significativo sulle dinamiche strutturali del fenomeno delle SLAPP.

6. Considerazioni conclusive

La direttiva (UE) 2024/1069 si inserisce in una più ampia traiettoria evolutiva dell'ordinamento europeo e convenzionale, progressivamente orientata a rafforzare la tutela della libertà di espressione rispetto agli effetti dissuasivi derivanti dall'uso distorto degli strumenti processuali. L'attenzione dell'interprete non si concentra più soltanto sul contenuto limitativo della misura, ma anche sulla sua capacità di incidere indirettamente sulle condizioni di esercizio delle libertà democratiche, scoraggiando la partecipazione al dibattito pubblico.
La Direttiva anti-SLAPP contribuisce a ridefinire il tradizionale bilanciamento tra libertà di espressione, tutela della reputazione e diritto di azione. Il giudizio di proporzionalità tende pertanto a investire non soltanto la fondatezza della pretesa azionata, ma anche le modalità concrete di esercizio del diritto di azione, nella misura in cui esse possono compromettere il pluralismo informativo e la partecipazione democratica.
Un esempio di bilanciamento tra interessi contrapposti che valorizza il rilievo del *chilling effect* è dato dalla sentenza n. 150/2021 della Corte costi-

tuzionale[21], con la quale è stata dichiarata l'illegittimità costituzionale della previsione cumulativa della pena detentiva e della pena pecuniaria per il delitto di diffamazione a mezzo stampa aggravata. La Corte ha infatti riconosciuto che la minaccia della privazione della libertà personale potesse produrre un effetto dissuasivo non soltanto rispetto alla commissione dell'illecito, ma anche rispetto all'esercizio della libertà di informazione, valorizzando una concezione sostanziale dell'effettività della libertà di stampa[22].

La Direttiva anti-SLAPP si colloca nel medesimo orizzonte assiologico, ma ne sviluppa ulteriormente le implicazioni sistematiche, spostando l'attenzione dal momento sanzionatorio all'impatto stesso dell'instaurazione del procedimento giudiziario sulle condizioni di esercizio della partecipazione pubblica.

Tale evoluzione non è tuttavia priva di tensioni sistematiche. Se l'esigenza di contrastare il contenzioso abusivo appare indispensabile per garantire davvero la libertà di espressione, permane al contempo il rischio che una protezione indiscriminata del discorso pubblico possa tradursi in un indebolimento dell'affidabilità dell'informazione e dei diritti della personalità. La sfida consiste ancora una volta nell'elaborazione di modelli di bilanciamento capaci di preservare pluralismo informativo, qualità del dibattito

---

[21] Corte cost., 12 luglio 2021, n. 150. In dottrina cfr. V. Pezzella, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca delle fake news, degli hate speeches e dell'intelligenza artificiale,* cit., 110 ss; G. Manca, *Il raffreddamento di diritti fondamentali come limite alla politica criminale,* cit., 80 ss.

[22] Basti qui ricordare, per i limitati fini di questo contributo, che con la celeberrima sentenza n. 150 del 2021, la Corte costituzionale ha tuttavia dichiarato infondate le questioni sollevate sull'art. 595, c. 3, c.p. in riferimento agli artt. 3, 21 e 117, c. 1, precisando: «L'art. 595, terzo comma, cod. pen. configura una circostanza aggravante del delitto di diffamazione, integrata allorché l'offesa sia recata col mezzo dello stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico. La pena prevista è quella della reclusione da sei mesi a tre anni ovvero della multa non inferiore a 516 euro. La previsione in via, questa volta, soltanto alternativa della pena detentiva da parte della norma censurata non può ritenersi di per sé in contrasto con la libertà di manifestazione del pensiero, tutelata dagli artt. 21 Cost. e 10 CEDU. Come rammentato nell'ordinanza n. 132 del 2020, se è vero che la libertà di espressione – in particolare sub specie di diritto di cronaca e di critica esercitato dai giornalisti – costituisce pietra angolare di ogni ordinamento democratico, non è men vero che la reputazione individuale è del pari un diritto inviolabile, strettamente legato alla stessa dignità della persona […] Si deve infatti ritenere che l'inflizione di una pena detentiva in caso di diffamazione compiuta a mezzo della stampa o di altro mezzo di pubblicità non sia di per sé incompatibile con le ragioni di tutela della libertà di manifestazione del pensiero nei casi in cui la diffamazione si caratterizzi per la sua eccezionale gravità». La Corte di Strasburgo ritiene integrate simili ipotesi eccezionali con riferimento a discorsi d'odio e di istigazione alla violenza, nonché a campagne di disinformazione condotte attraverso la stampa, internet o i social media, caratterizzate dalla diffusione di addebiti gravemente lesivi della reputazione della vittima, e compiute nella consapevolezza da parte dei loro autori della falsità degli addebiti (*ex multis* CEDU, *Sallusti c. Italia*, ric. 22350/13 (2019); CEDU, *Belpietro c. Italia,* ric. 43612/10 (2013)).

pubblico e garanzie individuali, evitando che la protezione dell'uno si traduca nella compressione indebita dell'altro.

In tale contesto, l'esperienza italiana appare paradigmatica delle difficoltà che accompagnano il recepimento della disciplina anti-SLAPP negli ordinamenti nazionali. Da un lato, la giurisprudenza costituzionale ha mosso i primi passi nella direzione di prevenire effetti deterrenti incompatibili con l'effettività della libertà di stampa; dall'altro, il legislatore sembra orientato verso un recepimento minimale della Direttiva. Una simile impostazione rischia tuttavia di ridurre sensibilmente l'incidenza concreta della disciplina europea soprattutto in un ordinamento nel quale la maggior parte delle azioni temerarie si sviluppa entro confini interni.

In questa prospettiva, la categoria del *chilling effect* sembra destinata ad assumere una rilevanza crescente quale criterio interpretativo autonomo e trasversale del costituzionalismo europeo. Essa consente infatti di cogliere una trasformazione più profonda del rapporto tra libertà, potere e giurisdizione: non basta che le restrizioni ai diritti fondamentali risultino formalmente legittime o astrattamente giustificate, ma occorre altresì verificare che esse non producano effetti incompatibili con le condizioni di effettività della democrazia pluralista.

Abstract

Il contributo analizza la direttiva (UE) 2024/1069, i principi ispiratori e le principali disposizioni, nonché i suoi effetti sull'ordinamento italiano, anche in seguito all'approvazione della legge n. 36 del 2026.

This article analyses directive (EU) 2024/1069, its underlying principles and key provisions, as well as its impact on Italian law, particularly following the adoption of Law No. 36 of 2026.

Keywords

freedom of information – Anti-SLAPP Directive – abuse of process – *chilling effects* – journalism

EU Enlargement: What Regulatory Landscape for Copyright and Artificial Intelligence?*

Anna Vasylchenko

Table of contents

1. Introduction. – 2. EU Regulatory Experience in Copyright and AI. – 2.1. Input Dimension: On the Copyright-Related Legal Issues Arising from AI Training. – 2.2. Economic Benefits "Value Gap" and Possible Solutions: A Proposed Fixed-Core, Dynamic Attribution Hybrid Model for Equitable Compensation of Authors in AI Training Pipelines. – 2.3. Outputs Beyond Human Authorship. – 3. Reflecting on AI in UkrAIne and its Implications for Copyright Law on the Path to EU Accession. – 3.1. Navigating the Copyright-Related Legal Issues Arising from AI Training in Ukraine. – 3.2. Ukraine's Regulatory Approach to AI-Generated Content. – 3.3. Advancing the AI-Relevant Implementation of the EU Copyright *Acquis* in Ukraine. – 4. Concluding Perspectives on AI and Copyright Regulation in an "Augmented" Union.

1. Introduction

The global economy is undergoing an unprecedented transformation driven by rapid technological advancements. Innovations in automation, AI, and digital platforms are profoundly impacting production workflows, labor markets, and value creation. This technological shift brings both opportunities for growth and efficiency, as well as challenges related to inequality, workforce disruption, and regulatory adaptation. Amidst these developments, artificial intelligence, and in particular, generative AI[1],

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

[1] This analysis refers to generative AI models, within the meaning of the EU AI Act. Recital 99 of the EU AI Act foresees that: «Large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of

stands out as a pivotal force driving contemporary economic transformation. AI is dramatically transforming creative processes and creative expression, introducing a new paradigm where the medium itself is capable of generating new outputs. Indeed, for instance, generative models abandon the idea of mere classification or analysis of existing data, and go further – where text, audio, images, and more are created by algorithms frequently without direct human involvement in the creation of the output. This breakthrough raises a series of controversial issues concerning the relationship between AI and copyright, and the adequacy of the current EU copyright *acquis* in addressing these challenges remains a subject of ongoing debate. Ensuring legal certainty in this domain is crucial, especially in light of the EU enlargement process, which must account for possible different regulatory approaches among candidate countries.

This urgency is reflected in the 2025 data, as the Stanford University AI Index Report 2025 shows that businesses' concerns have grown notably in recent years about certain risks, in particular, concerns over compliance and lawfulness risks (particularly regarding intellectual property and copyright violations) increased by +27 percentage points in 2025 compared to 2024[2].

In this context the article also reflects on Ukraine's experience, as the EU opened accession negotiations with the country in 2024. The significance of copyright law in the EU enlargement process lies in both legal and economic considerations. First, candidate countries must align their national legislation with the EU *acquis communautaire* which comprises strict rules on intellectual property rights. Furthermore, a robust copyright regime would attract investment by companies and would contribute to long-term sustainable growth. In Ukraine's case, a solid copyright framework could also accelerate economic integration into the EU Single Market. A well-functioning single market is not possible without a coherent regulatory framework for artificial intelligence, a phenomenon which has ushered in a new era in intellectual property law and, in particular, copyright. On the one hand, the rapid development of artificial intelligence has been addressed by the EU, *inter alia*, through the adoption of the European regulation on artificial intelligence (the AI Act). On the other hand, there is an ongoing

distinctive tasks». See 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 (EU AI Act), in *eur-lex.europa.eu*.

[2] N. Maslej – L. Fattorini – R. Perrault – Y. Gil – V. Parli – N. Kariuki – E. Capstick – A. Reuel – E. Brynjolfsson – J. Etchemendy – K. Ligett – T. Lyons – J. Manyika – J. C. Niebles – Y. Shoham – R. Wald – T. Walsh – A. Hamrah – L. Santarlasci – J. Betts Lotufo – A. Rome – A. Shi – S. Oak, *The AI Index 2025 Annual Report*, in *hai.stanford.edu*, April 2025, 181 ff.

debate about legislative gaps concerning AI and copyright, which highlights the necessity of swift legislative action. In its recent "AI Continent Action Plan"[3], the European Commission emphasizes the importance of candidate and potential candidate countries for the EU in promoting safe and trustworthy AI development in multilateral fora.

Before tackling issues of regulatory adaptation, however, it is useful to examine the nature of the interactions between copyright and AI from a theoretical perspective, which will serve as the basis for analyzing problematic questions and proposing possible solutions. It is possible to identify three primary dimensions that are crucial to understanding the AI-copyright relationship[4]. These dimensions can be represented along a conceptual continuum: at one end lies creative material produced entirely by humans; at the other, content generated exclusively by AI. The intermediate dimension represents hybrid forms of AI-copyright interaction. In particular, this intermediate dimension can be subdivided into two subtypes. The first subtype concerns at least two phases of the AI lifecycle, specifically, the training of AI models and machine learning operations (which are crucial for maintaining and updating a model after deployment), that involve the use of massive quantities of data, which may include protected materials. The second subtype of the intermediate dimension addresses the question of the role that AI models may assume in the production of artistic and intellectual works, including, but not limited to, music, sculpture, literature, painting, and industrial design. For a significant period, such involvement was conceptualized exclusively within the framework of computer-assisted creation, wherein software served merely as an auxiliary tool, facilitating but not replacing the human author's creative agency[5]. Nowadays, AI has emerged as a new actor capable of imitating human creativity through a combination of advanced machine learning techniques, such as deep learning. One of the main differences between AI and traditional media of creativity (e.g., charcoal or paint in visual arts; poetry or plays in literature etc.) lies in who creates content, how it is created, and the role of the instrument in the creative process. As a result, a discernible trend has emerged toward distinguishing between AI-generated works and those resulting from human creativity augmented by algorithms, posing significant

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *"AI Continent Action Plan*", in *eur-lex.europa.eu*, Brussels, 9 April 2025, Document 52025DC0165.

[4] This concept has been inspired by the "Missing Middle" theory developed by Paul R. Daugherty and H. James Wilson in their work "Human + Machine: Reimagining Work in the Age of AI". See P. R. Daugherty – H.J. Wilson, *Human + Machine: Reimagining Work in the Age of AI*, Harvard Business Review Press, Boston, Massachusetts, 2024.

[5] P.-Y. Gautier, *De la propriété des créations issues de l'intelligence artificielle*, in *La Semaine Juridique – Edition Générale*, 37, 2018, 1570 ff.

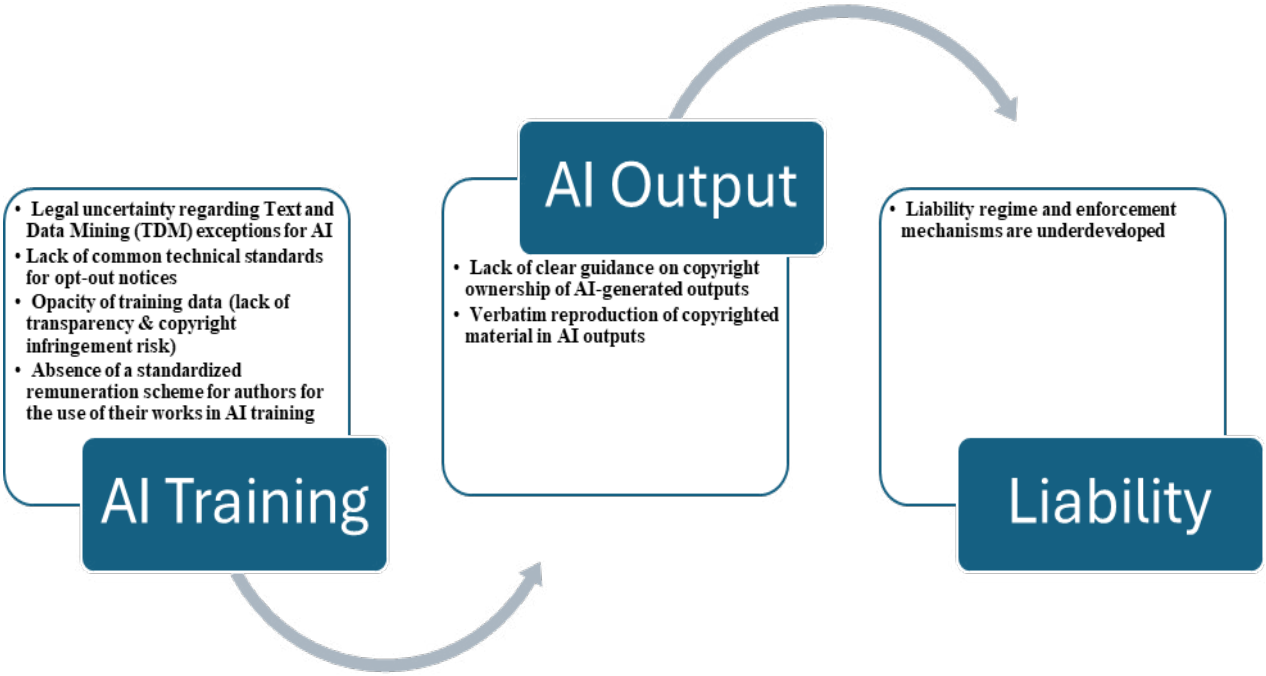
challenges for legislators.
Although the interaction between AI and copyright frequently appears as a challenging issue, it may, in fact, help define the boundaries of copyright itself, boundaries that are constantly evolving in response to the ongoing metamorphosis of digital technologies. The role of courts, we believe, will also be crucial in striking a balance between copyright regulation and AI-driven innovation.
Taking into account the abovementioned theoretical considerations, the purpose of this analysis is to contribute to ongoing debates about regulatory approaches to AI-copyright relations, as promoted by the EU and Ukraine (as one of the candidate countries for EU membership), and to explore their potential future implications.

2. EU Regulatory Experience in Copyright and AI

The complex and often uneasy relationship between artificial intelligence and copyright law brings to mind a fable attributed to Aesop, the legendary Greek storyteller: The Two Pots. In this tale, an iron pot invites a clay pot to set out on a journey together. The clay pot, aware of its fragility, hesitates, knowing that even a minor collision with the robust iron pot could be fatal. The iron pot downplays the peril, and after some persuasion, the clay pot agrees. However, as they travel, an impact eventually occurs, and the clay pot shatters. This fable offers a strikingly relevant moral for today's legal and technological landscape: AI, like the iron pot, is powerful, fast-moving, and often disruptive; copyright, akin to the clay pot, is more rigid and vulnerable to unintended consequences.
In today's highly competitive international environment, the EU is advancing the AI Continent Action Plan, which focuses on five strategic objectives, namely:
1) building a large-scale AI data and computing infrastructure;
2) increasing access to large and high-quality data;
3) developing algorithms and fostering AI adoption in strategic sectors;
4) strengthening AI skills and talents; and
5) regulatory simplification[6].
Copyright-related issues have the potential to impact all five of these strategic vectors. As illustrated in the premises, the contemporary debate surrounding AI and copyright primarily revolves around two key issues, namely:
1) potential copyright infringement during the AI training phase due to

[6] *"AI Continent Action Plan"*, in *eur-lex.europa.eu*, Brussels, 9 April 2025, Document 52025DC0165.

the use of copyrighted input data; and
2) questions of authorship concerning AI-generated output.
Unsurprisingly, liability concerns can arise from both of these aspects (see Diagram 1).



2.1. Input Dimension: On the Copyright-Related Legal Issues Arising from AI Training

There are several significant gaps and uncertainties in the European Union's current approach to AI training regulation.
The major legal tools referred to in discussions of AI and copyright issues are the Copyright in the Digital Single Market Directive (Directive (EU) 2019/790) and the AI Act. In the opinion of the author, it is possible to hypothesize that Directive (EU) 2019/790, although crafted with the aim of supporting a robust Digital Single Market and reflecting the technological developments of its time, nonetheless contains rules that are not flexible enough to accommodate ongoing technological evolution, particularly the legal challenges posed by AI. The Directive introduced two text and data mining (TDM) exceptions:
art. 3 permits TDM for scientific research purposes, applicable to research organizations and cultural heritage institutions that have lawful access to the content, and
art. 4 allows TDM by anyone, provided that rightsholders have not exercised their opt-out rights appropriately.
The concept of "text and data mining" is defined in art. 2 of the Direc-

tive as «[…] any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations […]»[7]. Two major interpretations have emerged from this definition regarding whether AI training constitutes TDM. A recent study commissioned by the European Parliament's Policy Department for Justice, Civil Liberties and Institutional Affairs at the request of the Committee on Legal Affairs and published in July 2025, titled "Generative AI and Copyright - Training, Creation, Regulation"[8], serves as a paradigmatic example of the interpretation that TDM exceptions are ill-suited for AI training. However, some academics argue that the Directive's definition of TDM does, in fact, cover AI training processes.

To contextualize these copyright provisions within the AI domain, they must be read alongside Recital 105 and art. 53(1)(c) of the EU AI Act. Indeed, in accordance with Recital 105, general-purpose generative AI models offer unique opportunities for innovation but also raise challenges for creators, whose content may be used in AI training. While TDM can be used to collect and analyse such content, any use of protected works normally requires authorisation of the rightsholder unless a copyright exception applies. Under Directive (EU) 2019/790, TDM is permitted under certain conditions, but rightsholders can opt out of such uses, except when TDM is conducted for scientific research[9].

Obligations for providers of general-purpose AI models concerning copyright are envisaged under Article 53(1)(c) AI Act:

«1. Providers of general-purpose AI models shall: […] (c) put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790»[10].

There are several critical points to highlight regarding the afore-mentioned

[7] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, in *eur-lex.europa.eu*.

[8] *Generative AI and Copyright - Training, Creation, Regulation*, in *europarl.europa.eu*, July 2025, PE 774.095

[9] This Recital continues as follows: «Where the rights to opt out has been expressly reserved in an appropriate manner, providers of general-purpose AI models need to obtain an authorisation from rightsholders if they want to carry out text and data mining over such works». See EU AI Act, in *eur-lex.europa.eu*.

[10] *Ibid.*

recital and article. First, while they underscore the AI Act legislator's assumption that TDM exceptions extend to AI training, they do not clarify whether the entirety of AI training processes qualifies under the TDM exceptions of Directive (EU) 2019/790, or only certain parts. Nor does it extend the scope of the Directive's exceptions and limitations (E&L) to AI training[11].

Second, it remains unclear what constitutes "an appropriate manner" for exercising the opt-out right. At the time of the Directive's adoption, the technological capabilities of AI differed significantly from today's landscape. As such, the TDM exceptions under Directive (EU) 2019/790 were not tailored to account for the AI training nuances[12]. In this regard recent research claims that AI training constitutes acts of reproduction rather than mining[13]. Furthermore, divergent implementation of the TDM exceptions by Member States only exacerbates the complexity of complying with Directive (EU) 2019/790.

As generative AI training may potentially undermine authors' exclusive rights, such as reproduction, distribution, communication to the public etc., and legislation fails to offer clear regulatory solutions, courts will play an increasingly significant role in interpreting the evolving relationship between generative AI and copyright law. In the EU, the pending Case C-250/25, *Like Company v. Google Ireland*, currently before the CJEU, is expected to shed light on the conditions under which AI training might be deemed lawful[14].

2.2. Economic Benefits "Value Gap" and Possible Solutions: A Proposed Fixed-Core, Dynamic Attribution Hybrid Model for Equitable Compensation of Authors in AI Training Pipelines

While the EU has made significant progress in setting the rules for the digital and AI-driven economy, through such legislative tools as the Directive (EU) 2019/790 (the Digital Single Market Directive) and the AI

[11] For more on this topic see M. Leistner - L. Antoine, *TDM and AI Training in the European Union – From 'LAION' to Possible Ways Ahead?*, in *papers.ssrn.com*, 14 March 2025.

[12] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025, PE 774.095, 26 ff.

[13] Ivi, 30-31 ff.

[14] In the Case C-250/25 the CJEU will decide on the issues related to the display, in the LLM chatbot, of a partially verbatim text of a press publisher website, as well as the communication to the public, reproduction and possible free use of that material. See CJEU, C-250/25, *Like Company v Google Ireland Limited* (2025).

Act, several challenges remain unresolved. In the context of Directive (EU) 2019/790, perhaps even more interesting than rules it provides are the regulatory solutions it omits. One significant omission concerns the emergence of a new "value gap" resulting from AI training on copyrighted material included in training datasets, frequently without remuneration to authors[15]. The issue of industries benefiting from protected material without compensating rightsholders is not new in the EU copyright history. Indeed, similar concerns surfaced during the Internet's early days with the rise of the so-called "value gap" concept, which was linked to certain online service providers profiting from the commercial value of copyright-protected works without compensating rightsholders, often under the protection of "safe harbor" provisions, in particular, art. 14 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market[16] (hereinafter the "eCommerce Directive"). The rationale behind such "safe harbors" was to promote the growth of the emerging Internet economy. Nowadays, in the AI age, we are witnessing concerns sharing common features with those earlier debates, albeit in a new context. Generative AI models raise, *inter alia*, two major issues:

a lack of legal certainty regarding the lawfulness of generative AI models training on copyrighted datasets, especially when such datasets are extracted from web content that is neither licensed nor explicitly exempted; and

a lack of transparency (e.g., provenance tracking), which makes it nearly impossible for rightsholders to determine whether their works have been used without authorisation.

What is particularly striking, however, is the clear disparity between the regulatory regime for service providers and that for AI industries, marked by a *de jure* "safe harbor" for service providers, and a *de facto* "safe harbor" for AI companies, arising from a regulatory vacuum. Generative AI practices often fail to account for the interests of actual human authors. This has contributed to a shift in perspective, in which remuneration is increasingly viewed as a privilege than a right[17]. As a result, creators lack effective

---

[15] *Generative AI and Copyright - Training, Creation, Regulation*, in *europarl.europa.eu*, July 2025, PE 774.095, 8 ff.

[16] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Document 32000L0031, in *eur-lex.europa.eu*.

[17] A theory of a reward for the uses of works protected by intellectual property as a result of labor was developed by Locke. The work "The Philosophy of Intellectual Property" of Justin Hughes delivers one of the most thorough study available of the Lockean justification of intellectual property. See J. Hughes, *The Philosophy of Intellectual Property*, in *77 Georgetown Law Journal*, 287, 1988.

mechanisms to obtain fair remuneration for the use of their works in AI training, while AI industries continue to profit from the commercial exploitation of protected content. An initial attempt to address this *de facto* "safe harbor" for providers of general-purpose AI models can be found in the AI Act, particularly in its transparency obligations, which, however, are insufficient to resolve the major copyright challenges at stake. As for Directive (EU) 2019/790, it is becoming increasingly apparent that, while the Directive aligned reasonably well with the technological landscape at the time of its adoption, it is not flexible enough to accommodate the rapid evolution of AI technologies. There are growing strong concerns among academics, rightsholders, and policymakers that Artt. 3 and 4 of the Directive (EU) 2019/790, concerning TDM rules, are poorly suited to the realities of AI[18]. Moreover, the fragmented implementation of TDM exceptions across EU Member States reflects deeper structural issues rooted in legislative choices made during the adoption of Directive (EU) 2019/790. The Treaty on European Union (TEU) not only sets out the scope of the Union's actions but also the form such action should take. In particular, it defines the types of legal acts that the EU can adopt, with a general principle that compulsory regulatory measures must be limited to what is necessary. Thus, if a regulation (a binding legislative act that must be applied in its entirety across the EU) is not necessary, a directive (a legislative act that sets out objectives, but allows Member States discretion on how to achieve them) should be adopted instead[19]. With this in mind, it becomes evident how the patchwork implementation of the TDM exceptions by EU Member States has contributed to legal uncertainty and compliance complexity, thereby fueling calls for reform.

By contrast, the AI Act is a binding legislative tool intended to be applied in its entirety across all Member States. Among other objectives, it introduces progressively stricter obligations for providers of general-purpose AI models[20].

Given that authors whose works are used for AI training are frequently in a weaker bargaining position, they need access to information about

[18] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025, PE 774.095, 12 ff.

[19] U. Villani, *Istituzioni di diritto dell'Unione Europea*, Bari, 2024

[20] Parallels can be drawn with the earlier platforms' "safe harbors". Indeed, historically, intermediary liability exemptions were coined to serve as an incentive for the nascent Internet market. The United States was at the forefront of this development with the adoption of the 1996 Communications Decency Act and, subsequently, the 1998 Digital Millennium Copyright Act, both marked by the gradual introduction of more restrictive requirements for intermediaries. The European Union, in a comparable way, adopted the eCommerce Directive to limit liability of certain categories of online intermediaries. See OECD, *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, in *oecd.org*, OECD Publishing, 2011, 72-78.

how their works are used, in order to fully benefit from rights harmonized under Union law. To this end, art. 53(1)(d) of the AI Act establishes a transparency obligation:
«1. Providers of general-purpose AI models shall: […] (d) draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office»[21].
This provision may be interpreted as a legislative effort to align with the existing principle of fair remuneration set out in Artt. 18 to 23 of Chapter 3, Title IV of Directive (EU) 2019/790[22]. In the opinion of the author, for the purpose of establishing fair remuneration of authors in the field of AI training, such exploitation-related information should be up-to-date, comprehensible to the author and cover relevant sources of revenues too. In cases where TDM exceptions cannot be legitimately applied to AI training, the principle of equitable remuneration emerges as a legal instrument aimed at preserving a fair balance between the rights of authors and the interests of AI developers[23]. Considering that the remuneration of creators should be appropriate and proportionate to the economic value of their work, and that Directive (EU) 2019/790 and the AI Act do not provide a coherent mechanism for distributing the economic value of AI-generated content, there has been a broad discussion regarding possible remuneration schemes. One potential solution to the value gap problem could be the introduction of a statutory remuneration mechanism that allocates a portion of profits from the commercialization of AI outputs to rightsholders.[24].
In the opinion of the author, the remuneration mechanism should be structured in a systematic yet adaptable way, where multiple "layers" must be aligned to achieve a complete solution. This remuneration framework proposes a fixed-core statutory remuneration level and a dynamic attribution level. The former establishes a mandatory and unwaivable right to a one-time payment[25], potentially administered by Collective Management Organisations. The latter envisages incremental payments based on the value and volume of the works within the AI model (e.g., frequency of ref-

[21] EU AI Act, in *eur-lex.europa.eu*.

[22] *Directive (EU) 2019/790*, in *eur-lex.europa.eu.*

[23] M. Senftleben, *Are the European TDM Exceptions Applicable to GenAI Training? Despite the Three-Step Test?*, in *Kluwer Copyright Blog*, 1 October 2025.

[24] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025, PE 774.095, 10 ff.

[25] For a statutory remuneration solution see also C. Geiger – B. J. Jütte, *Limitation-Based Remuneration Rights: An Underexplored Approach to Balancing Copyright Interests in the EU,* in *legalblogs.wolterskluwer.com,* 30 April 2025.

erence to a work)[26]. This approach aligns with the principles and purposes of the contract adjustment mechanism ("best seller clause") envisaged under art. 20 of the Directive (EU) 2019/790[27]. The proposed remuneration model would adopt an algorithmic approach to ensure adaptability across different types of works used in AI training. To account for the possible incremental value of the work, a feedback loop for authors could be introduced to allow them to track how the value of their work increases and to claim the adjustment to their compensation if necessary. The proposed remuneration scheme should be modular to accommodate different types of creative works (e.g., text, images, music, etc.) and different kinds of AI training use cases. Such modularity would ensure that authors are fairly compensated across different sectors and models. However, the transparency obligations provided for in the AI Act appear insufficient to achieve this level of fair remuneration for authors. This issue could benefit from the solutions advanced by the European Parliament in its resolution of 10 March 2026 regarding copyright and generative artificial intelligence[28]. In particular, the transparency required for the practical feasibility of the proposed remuneration scheme can be met where:

1. Rightsholders are enabled to watermark their works, AI providers are required to keep such watermarking unaltered, and search tools are made available to detect these watermarks in AI training materials;
2. A detailed list of each item of protected content used for AI training is made available;
3. Crawlers are obligated to identify themselves to web operators;
4. AI providers or deployers are obligated to maintain detailed records of their crawling activities;
5. A trusted intermediary (such as the European Union Intellectual Property Office) is introduced to notify rightsholders when their content is used[29]

Where this level of transparency is maintained *mutatis mutandis* for future uses of protected content, such as retrieval-augmented generation (RAG)

---

[26] This layer is grounded in the remuneration principles suggested in the following research: J. T. Wang – Z. Deng – H. Chiba-Okabe – B. Barak – W. J. Su, *An Economic Solution to Copyright Challenges of Generative AI*", in *arxiv.org*, 3 September 2024. While the aforementioned authors apply cooperative game theory, the remuneration model proposed in this work is inspired by the mechanics of the Rubik's Cube algorithm. See, D.-X. Zeng – M. Li – J.-J. Wang – Y.-L. Hou – W.-J. Lu – Z. Huang, *Overview of Rubik's Cube and Reflections on Its Application in Mechanism*, in *Chinese Journal of Mechanical Engineering,* 31, 77, 2018, 1 ff.

[27] Art. 20 *Directive (EU) 2019/790*, in *eur-lex.europa.eu.*

[28] European Parliament resolution of 10 March 2026 on copyright and generative artificial intelligence – opportunities and challenges (2025/2058(INI)), in *europarl.europa.eu*, 2026.

[29] Recitals Y, Z, AA, *ibid.*

or fine-tuning, the introduction of a residual remuneration right merits further consideration.

2.3. Outputs Beyond Human Authorship

The EU copyright *acquis* does not provide an explicit definition of "author," and instead refers to international legal tools such as the Berne Convention[30]. While the European Parliament, in its Resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)), recognized the need for a legal framework addressing creations generated by AI technology, it recommended that ownership of rights, if any, should be assigned only to natural or legal persons. This position reflects a cautious approach that maintains the human (or corporate) foundation of intellectual property rights and resists extending authorship or ownership to AI systems themselves[31].

With regard to the "output side", the EU currently does not provide for the attribution of rights, for instance *sui generis* rights, to entirely AI-generated content, and therefore such material remains in the public domain. The rationale behind this choice lies in the potential risk of undermining the coherence of the copyright system[32]. As repeatedly underscored by the Court of Justice of European Union in its landmark case law, one of the *sine qua non* principles of the EU copyright law is that a work must be original, i.e. the expression of the author's own intellectual creation, thus requiring a human intellectual effort and creativity in order to qualify for copyright protection[33]. This means that fully AI-generated material does not fall under the EU originality standard for copyright protection. This criterion is inherently linked to the human-centered approach to the definition of creativity established in the EU. Even though the challenges faced by EU copyright law have contributed to the emergence of alternative visions, such as *sui generis* right for AI-generated outputs[34], these

[30] For more on this topic see P. B. Hugenholtz - J. P. Quintais, *Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?*, in *International Review of Intellectual Property and Competition Law*, 52, 2021.

[31] European Parliament, *Resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies*, in *europarl.europa.eu*, P9_TA(2020)0277, 2020.

[32] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025, PE 774.095, 9 ff.

[33] See, for instance, CJEU, *C-5/08, Infopaq International A/S v Danske Dagblades Forening,* in *curia.europa.eu* (2009).

[34] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025,

approaches have not yet found official legal application.
Another important issue related to AI-generated outputs concerns cases of verbatim or near-verbatim reproduction of certain elements of copyrighted material included in the training process[35]. Such acts may qualify not only as reproduction but also as communication to the public, as provided for under art. 3(2) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (hereinafter the "InfoSoc Directive")[36].
In order to enhance legal certainty, regulatory clarification is needed regarding permissible AI training processes, the status of AI-generated content, the development of dataset traceability, and fair remuneration mechanisms.

3. Reflecting on AI in UkrAIne and its Implications for Copyright Law on the Path to EU Accession

In many senses, Ukraine's path toward accession to the European Union marks not only a pivotal political milestone but also a complex legal undertaking grounded in the provisions of EU primary law. This process raises critical questions in the domain of intellectual property, particularly in the context of emerging technologies such as artificial intelligence. Key issues comprise: What is the current state of Ukraine's copyright framework? Are there legal tools that specifically address AI? How does Ukrainian law regulate the intersection between AI and copyright? Can AI-generated material be protected by copyright? Does the use of copyrighted content to train AI models constitute infringement? These questions are of paramount importance for both Ukraine and the EU as they work to shape a responsible and forward-looking AI ecosystem aligned with the broader EU enlargement process. Recognizing this, the European Union Intellectual Property Office (EUIPO), in its EUIPO Strategy 2030, highlights the strategic importance of supporting EU candidate countries through intel-

PE 774.095

[35] A notable example is the New York Times v. OpenAI lawsuit, where the key allegation concerns the OpenAI's unlicensed and unauthorized, and thus infringing, use of Times's articles, followed by their subsequent near-verbatim reproduction. See United States District Court, S.D. New York, *the New York Times Company v. OpenAI* (2025).

[36] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, in *eur-lex.europa.eu*.

lectual property cooperation under its external action framework[37]. While the European Commission's Ukraine 2024 Report acknowledges progress made by Ukraine, it also underscores only "limited progress" in aligning copyright legislation. The Report specifically refers to the adoption of implementing legislation for the Law on Copyright and Related Rights and recommends, *inter alia*, that Ukraine «[…] continue alignment with the EU acquis on copyright […]» throughout 2025[38].

Indeed, Ukraine has recently faced major shifts in its copyright landscape. The adoption of the new Law on Copyright and Related Rights (Law (Ukraine) 2811-IX/2022) in December 2022, which entered into force on 1 January 2023, marks a significant legal development. The new piece of legislation tackles a broad range of issues, from core concepts such as the definition of a "work" and an "author" to more sophisticated mechanisms like exceptions and limitations (E&Ls). To date, Ukraine has not adopted a specific law on artificial intelligence. Instead, issues related to AI are addressed within existing relevant sectoral legislation. Nevertheless, the country's European integration aspirations are clearly shaping the national AI policy agenda. The most significant developments include:

- The Concept of AI Development in Ukraine (approved by the Cabinet of Ministers on 2 December 2020),
- The 2024 Recommendations for the Responsible Use of Artificial Intelligence: Intellectual Property Rights Issues, and
- The 2024 White Paper on Artificial Intelligence Regulation in Ukraine, promoted by the Ministry of Digital Transformation.
- The White Paper sets out Ukraine's AI regulatory priorities, which include:
    - supporting business competitiveness,
    - protecting human rights, and
    - advancing European integration[39].

Copyright-related issues intersect all three of these objectives. Ukraine's approach to AI regulation follows a bottom-up methodology, beginning with non-binding extra-legal tools based, *inter alia*, on stakeholders' experience (civil society, businesses) and moving toward binding regulation, eventually aiming to align with the EU's Artificial Intelligence Act. In support of this trajectory, Ukraine seeks to build regulatory and institutional capacity in line with international standards. In particular, like the EU, it

[37] EUIPO, *EUIPO Strategy 2030*, in *euipo.europa.eu,* 2025.

[38] European Commission, Directorate-General for Neighbourhood and Enlargement Negotiations, *Commission Staff Working Document Ukraine 2024 Report,* in *eur-lex.europa.eu*.

[39] Ministry of Digital Transformation of Ukraine, *White Paper on Artificial Intelligence Regulation in Ukraine: Vision of the Ministry of Digital Transformation of Ukraine*, in *storage.thedigital.gov.ua*, June 2024.

has signed the 2024 Council of Europe's Framework Convention on AI, Human Rights, Democracy, and Rule of Law (STCE n.225[40]), and aims to apply the HUDERIA methodology (Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law), adopted by the Council of Europe's Committee on Artificial Intelligence (CAI) on 28 November 2024[41]. Further reinforcing this direction, the Recommendations for the responsible AI-driven systems development[42], published in June 2025, offer valuable insights into Ukraine's regulatory vision and serve as a foundational document in the formation of national AI policy.

3.1. Navigating the Copyright-Related Legal Issues Arising from AI Training in Ukraine

Against this backdrop, a core area requiring attention is the set of copyright-related regulatory implications arising from AI training, a topic that lies at the center of Ukraine's current copyright debate. As Ukraine moves toward alignment with EU and international standards, it must clarify the copyright rules governing the large-scale data collection, processing, and TDM practices that underpin modern AI development. Accordingly, this section examines how Ukraine is navigating these issues, drawing on both EU practice and its own evolving legal framework.

To generate high-quality outputs, AI systems depend on the input data that must be both up-to-date and of high quality[43]. As a result, AI can potentially engage in processes of mining texts, images, music, and other content that may be protected by copyright. Nowadays, TDM is an important research practice across many scientific areas both in the EU and in Ukraine. Reflecting this importance, Ukraine has recently addressed this issue by introducing a TDM exception in the new Law on Copyright and Related Rights[44]. While this exception is inspired by the EU's Digital Single Market Directive, there are some notable differences between the two regimes. The EU's TDM regime is built on two mandatory provisions of

[40] Council of Europe, Council of Europe Framework Convention on AI, Human Rights, Democracy, and Rule of Law (STCE n.225), in *rm.coe.int*, November 2024.

[41] Committee On Artificial Intelligence (CAI), Council of Europe, *Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA methodology)*, in *rm.coe.int*, Strasbourg, November 2024.

[42] Ministry of Digital Transformation of Ukraine, *Recommendations for the responsible AI-driven systems development* (Ukrainian only), in *thedigital.gov.ua*, June 2025.

[43] *Ibid.*

[44] *Law of Ukraine on Copyright and Related Rights, 2811-IX/2022* , in *zakon.rada.gov.ua*, 2022.

the Directive (EU) 2019/790, namely:

- art. 3, which provides a mandatory exception for TDM by research organizations, and
- art. 4, which introduces a broader exception allowing anyone, individuals and institutions, to perform TDM on two conditions:
    - individuals or institutions have lawful access to protected works; and
    - rightsholders have not expressly prohibited such acts[45].

In essence, this means that art. 4 includes an opt-out clause and that rightsholders are granted a possibility to prohibit TDM for commercial purposes by using, e.g. metadata tools like robots.txt files to indicate such restrictions online[46]).

In other words, the Directive extends the scope of the TDM exception beyond research organizations and makes beneficiaries of this exception all those who enjoy lawful access to copyright-protected content. While commercial research institutes do not fall within the scope of art. 3, they may still be covered by art. 4 of the Directive (EU) 2019/790. In contrast, the Ukrainian TDM exception, as introduced by the national legislature, permits the making of copies of works contained in or related to academic publications, and applies only for research purposes. As of now, there is no case law in Ukraine addressing the relationship between the TDM exception and AI, nor is there a clear legislative stance on whether AI training may qualify as copyright infringement. It is therefore likely that Ukraine will address this issue in order to establish robust thresholds as to the allowed uses of protected works in digital environment. Moreover, there is no AI training specific legislation in Ukraine, so such activities are conducted within a *de facto* "safe harbor", similar to the situation in the EU. Emerging tendencies in this field were addressed in the ministerial document "Recommendations for the Responsible Development of AI-Driven Systems", published in June 2025. In particular, since input data may be used for reproduction purposes during AI training, such uses can potentially infringe copyright, related rights or *sui generis* right, as they do not always fall within the scope of free use cases set out in the Law (Ukraine) 2811-IX/2022. Ergo, the aforementioned document proposes two regulatory approaches that distinguish between small and large GenAI systems: For the training of small GenAI models, it is recommended that the use of protected content be subject to explicit permission, ideally based on

[45] Arts. 3 and 4, Directive (EU) 2019/790, in *eur-lex.europa.eu.*

[46] P. B. Hugenholtz, *The New Copyright Directive: Text and Data Mining (Articles 3 and 4)'*, in *Kluwer Copyright Blog*, 2019.

agreements with lawful rightsholders.
By contrast, the training of large GenAI models may be allowed provided that AI developers implement opt-out mechanisms, enabling rightsholders to exclude their works. These mechanisms may include a standardized electronic form that rightsholders can use to provide AI developers with all necessary information to unambiguously identify the protected material.
Additionally, transparency regarding the datasets, used to train AI models (e.g. introduction of a mandatory notice to be submitted to public authorities regarding works protected by copyright used for AI training), should be actively promoted by public authorities, and upheld as a general principle by AI model developers[47].
Copyright and AI training issues are expected to grow in importance in light of Ukraine's ambitious AI development goals, comprising its commitment to developing a national Large Language Model (LLM). This LLM is intended for use in digital government services and the business sector. In this context, key advantages include enhanced quality (achieved through training the LLM on Ukrainian data), improved security as (all data is stored domestically) and cost-effectiveness (since the national LLM would be more affordable than foreign alternatives)[48].
As of now, however, Ukraine, like the EU, lacks an unambiguous regulatory framework regarding the suitability of TDM exceptions for AI training.

3.2. Ukraine's Regulatory Approach to AI-Generated Content

Pursuant to art. 1(1) of the new Law of Ukraine on Copyright and Related Rights (Law (Ukraine) 2811-IX/2022), the author is defined as a natural person, who creates a work as a result of their own creative activity[49]. Therefore, this provision excludes the possibility of attributing authorship of a creative material to AI, reaffirming, first, that the concept of authorship in Ukraine is not based on legal fiction, and second, that it adopts a human-centric approach in line with the EU copyright legal tradition, which requires human creativity and authorship[50]. Pursuant to art. 1 of the

[47] Ministry of Digital Transformation of Ukraine, *Recommendations for the responsible AI-driven systems development* (Ukrainian only), in *thedigital.gov.ua,* June 2025.

[48] Ministry of Digital Transformation of Ukraine, *Ministry of Digital Transformation works to develop a national Large Language Model (LLM) to be used in digital government and business products,* in *kmu.gov.ua,* June 2025.

[49] *Law of Ukraine on Copyright and Related Rights, 2811-IX/2022* , in *zakon.rada.gov.ua*, 2022.

[50] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025, PE 774.095, 12 ff.

Law (Ukraine) 2811-IX/2022, a work is defined as an original intellectual creation of an author or co-authors in the scientific, literary, artistic or other domain, expressed in an objective form. With regard to the notion of originality, which is the central concept of copyright law, art. 1(35) defines it as a feature (or criterion) characterizing a work as a result of the author's own intellectual creative activity, reflecting the creative choices made by the author in the course of creating the work. This provision aligns with the EU *acquis*, where the notion of "own intellectual creation" derives from the jurisprudence of the CJEU, specifically the case Infopaq International A/S v Danske Dagbaldes Forening, in which the CJEU held that copyright applies only to works that reflect «[…] the author's own intellectual creation […]»[51].

To specifically address the regulation of AI-generated outputs, the Ukrainian legislator introduced a novel concept in art. 33 of Law (Ukraine) 2811-IX/2022, namely a *sui generis* right for non-original computer-generated object. This is defined as content that differs from existing, similar subject matter and is generated by the functioning of a computer program without the direct involvement of a natural person in its creation[52]. Accordingly, under art. 8 of the same law, non-original computer-generated object is expressly excluded from copyright protection[53]. This approach differs significantly from the EU regulatory model, where fully machine-generated outputs belong in the public domain[54].

Art. 33(3) of the law also addresses the issue of moral rights. From a legal standpoint, moral rights are traditionally defined as the legally protected link between a creator and their work, which grants the author a prevalent position over users of the work. However, in the case of the *sui generis* right, rightsholders are denied moral rights to non-original computer-generated object[55].

Under the Law (Ukraine) 2811-IX/2022, the definition of subjects of the *sui generis* right to non-original objects generated by a computer program includes the authors of such a computer program, their heirs, persons to whom the authors or their heirs have transferred (alienated) the economic rights to the computer program, or lawful users of the computer program[56]. This provision, however, introduces a degree of legal uncertainty,

---

[51] CJEU, C-5/08, *Infopaq International A/S v Danske Dagblades Forening* (2009).

[52] *Law of Ukraine on Copyright and Related Rights, 2811-IX/2022* , in *zakon.rada.gov.ua*, 2022.

[53] Ivi, art. 8.

[54] *Generative AI and Copyright - Training, Creation, Regulation,* in *europarl.europa.eu,* July 2025, PE 774.095, 9 ff.

[55] *Law of Ukraine on Copyright and Related Rights, 2811-IX/2022* (Ukrainian only), in *zakon.rada.gov.ua*, 2022.

[56] Art. 33(2), *Law of Ukraine on Copyright and Related Rights, 2811-IX/2022* , in *zakon.rada.*

because it does not clearly identify a single rightsholder[57]. The scope of economic rights under this *sui generis* right coincides with economic rights typically granted to authors of original works[58]. The *sui generis* right vests at the time of generation of the object[59] and lasts for 25 years, starting from 1 January of the year following its creation[60].
In 2024 the Ukrainian National Office for Intellectual Property and Innovations registered several composite works which included copyrightable content and AI-generated images. Notably, state copyright registration was granted to the collection of images "Easter Cards" by Margarita Boyko, the children's book "The Enchanted Adventure of Rufus" by Anna Khorolska, and collection "Poems of an Unfinished War" by Andriy Sitnikov, which was illustrated with AI-generated images[61]. Notably, the introduction of the *sui generis* right marks a departure from the EU *acquis* and is attributable to the fact that the law was drafted prior to June 2022, when Ukraine was granted candidate status for EU membership[62].

3.3. Advancing the AI-Relevant Implementation of the EU Copyright Acquis in Ukraine

Currently, Ukraine's regulatory actions must comply with the "Action Plan for the Implementation of the Recommendations of the European Commission", approved by the Order of the Cabinet of Ministers of Ukraine No. 300-r, dated 28 March 2025.
In particular, under the section "Ukraine's Capacity to Fulfill the Obligations of EU Membership – Cluster 2: Internal Market, Section 7: Intellectual Property Law," the European Commission's recommendations include:

«Recommendation 93:
Ukraine should continue aligning its legislation with EU legal acts on cop-

gov.ua, 2022.

[57] See also A. Kyrylenko, *Ukrainian IP Office registers works incorporating AI-generated content protected under new sui generis right*, in *ipkitten.blogspot.com*, September 2024.

[58] Art. 12, *Law of Ukraine on Copyright and Related Rights, 2811-IX/2022* , in *zakon.rada.gov.ua*, 2022.

[59] Ivi, art. 33(5).

[60] Ivi, art. 33(6).

[61] *For the first time in Ukraine, copyright is registered for works that include AI-generated images*, in *ukrpatent.org*, October 2024.

[62] A. Kyrylenko, *Ukrainian IP Office registers works incorporating AI-generated content protected under new sui generis right,* in *ipkitten.blogspot.com*, September 2024.

yright, industrial property rights, and trade secrets. This includes drafting amendments to the Law of Ukraine "On Copyright and Related Rights" and submitting the draft law to the European Commission for recommendations and/or comments […]
The bodies responsible for implementation of Recommendation 93 are Ministry of Economy and Ukrainian National Office of Intellectual Property and Innovation with the implementation deadline set for July 2025.
Recommendation 94:
Improve the functioning of collective management organizations and the distribution of royalties to rightsholders. Specifically, this includes (1) developing and adopting an order by the Ministry of Economy entitled "On Amendments to Order No. 1827 of the Ministry for Development of Economy, Trade and Agriculture dated September 18, 2020," aimed at enhancing the procedures of the accreditation commission for collective management organizations, taking into account the requirements of the Law of Ukraine "On Administrative Procedure"[…]
The body responsible for implementation of Recommendation 94(1) is Ministry of Economy with the implementation deadline set for August 2025»[63].

The European Commission, in its recent Ukraine 2025 Report, expressed concerns that the accreditation procedures for Collective Management Organisations remain suspended under martial law, negatively affecting the collection and distribution of royalties to rightsholders. Moreover, although the Report highlighted the lack of alignment of Ukrainian legislation with the EU's AI Act, it also acknowledged Ukraine's efforts toward achieving such alignment[64].
Furthermore, nuanced discussions are currently underway regarding the incorporation into national law of the Directive (EU) 2019/790 provisions concerning "appropriate and proportionate" remuneration for authors and performers. Core elements proposed for consideration in determining such remuneration comprise the economic value of the licensed rights, the contribution of the creator, and prevailing market practices. Additionally, discussions are focused on proposed amendments to the Law (Ukraine) 2811-IX/2022, specifically the introduction of definitions

[63] *Action Plan for the Implementation of the Recommendations of the European Commission*, approved by the Order of the Cabinet of Ministers of Ukraine, No. 300-r., in *zakon.rada.gov.ua*, 28 March 2025.

[64] European Commission, *Commission staff working document Ukraine 2025 Report, accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2025, Communication on EU enlargement policy*, in *enlargement.ec.europa.eu*, Brussels, 4 November 2025.

for the terms "text and data mining" and "research organization"[65].

4. Concluding Perspectives on AI and Copyright Regulation in an "Augmented" Union

The persistent tension between copyright and AI is a common contemporary issue that connects the EU and Ukraine, a country aspiring to EU accession. Ukraine's ongoing legislative reform, in particular, the Law (Ukraine) 2811-IX/2022 on Copyright and Related Rights, represents a concrete example of genuine effort to align with the EU copyright *acquis*. The adoption of a human-centric definition of authorship, the introduction of text and data mining exceptions for research purposes, and the promotion of a transparency-focused framework in Ukraine all reflect the shared vision of policy solutions in this domain in the EU and Ukraine. Moreover, the Law (Ukraine) 2811-IX/2022 serves as a legislative tool that anticipates, in the form of a *sui generis* right, a possible solution to the issue of AI-generated outputs, crafted to protect investments in AI-generated material, meaning that Ukraine has sought to attribute value to content that may be commercially or culturally valuable. Ukraine's experience can thus serve as a real-world sand-box for the implementation of a *sui generis* right, offering valuable insights into its strengths, limitations, and potential next steps, in other words it may provide useful guidance for the EU, where AI-generated material currently belongs to the public domain.
Another core issue, echoed across both Ukrainian and EU legal debates, concerns the input dimension of AI, in particular, whether the training of AI models constitutes allowed TDM or qualifies as unlawful acts of reproduction and communication to the public of protected content. It is becoming increasingly evident that the TDM exceptions provided under Artt. 3 and 4 of Directive (EU) 2019/790 were not tailored to address the nuances of training general-purpose AI models. The AI Act, in its copyright-relevant provisions, leaves critical uncertainties unresolved, notably regarding the scope of TDM applicability and the technical standards for opt-out notices. These legal gaps, when coupled with the fragmented implementation across EU Member States, exacerbate compliance burdens and deepen legal uncertainty.
The so-called "value gap" represents another pressing concern linked to AI training. It refers to the imbalance created when AI systems scrape datasets containing protected works without remunerating authors, who

[65] Ukrainian National Office for Intellectual Property and Innovations (UANIPIO), *Implementation of the EU acquis on copyright and related rights: a discussion was held on upcoming legislative changes* (Ukrainian only), in *nipo.gov.ua*, June 2025.

consequently find themselves in a structurally disadvantaged position. Current transparency obligations envisaged under art. 53 of the AI Act while mark some progress, fail to bridge this economic divide. In light of this, proposals for remuneration schemes, such as the aforementioned Fixed-Core, Dynamic Attribution model, offer promising avenues to ensure fair compensation for creators whose works are absorbed into AI training pipelines.

Ukraine's transition toward a fully digital and IP-aware economy is on a constructive trajectory and, given the inherently transnational nature of both copyright and AI regulation, by addressing these complex issues Ukraine can position itself as not only as a legal harmonizer, but also as a constructive contributor to the EU's evolving AI governance landscape. Ukraine's adoption of AI governance principles, including transparency and human-centric copyright regulation, already aligned and further alignment with the EU AI Act and copyright *acquis*, strengthens the Union's model of ethical, rights-respecting AI. Moreover, Ukraine's approximation to EU copyright law and digital regulation is likely to reduce compliance burdens for technology companies, enable shared research infrastructure and datasets under aligned copyright regimes, support the creation of a joint remuneration framework or collective licensing model, and offer more effective IP enforcement across both the EU and Ukrainian markets.

Abstract

The article explores the intersection of copyright and AI in the context of EU enlargement, focusing on Ukraine, with which the EU opened accession negotiations in 2024. Aligning national law with the EU *acquis*, including stringent IP rules, is both a legal obligation and an economic opportunity for candidate countries. A robust copyright regime would support investment and Ukraine's integration into the EU Single Market. As AI reshapes IP law, a cohesive regulatory framework becomes essential. Despite the EU's adoption of the AI Act, significant gaps persist regarding AI and copyright. The EU's 2025 "AI Continent Action Plan" stresses the role of candidate countries in advancing safe and trustworthy AI. The article identifies these gaps and outlines possible regulatory solutions for the EU and Ukraine.

Parole chiave

copyright – artificial intelligence – AI Act – Ukraine – Copyright Directive

A Comparative Analysis of Regulatory Sandboxes: Models, Evolution, and Strategic Implications in the UAE and Singapore*

Andrea Stazi, Riccardo Jovine

Table of contents

1. Introduction: Research Objective and Scope. – 2. Regulatory Sandboxes in the United Arab Emirates. – 3. Regulatory Sandbox in Singapore. – 4. Approaches and Future Perspectives: a Comparative Framework.

1. Introduction: Research Objective and Scope

The comparative analysis of legal systems proposed in this paper examines how different legal systems respond to the challenges posed by technological innovation.

In civil law jurisdictions, regulatory models typically originate from codified statutes and institutional frameworks, whereas in common law systems, such as that of Singapore, the legal order is fundamentally shaped by case law, judicial precedent, and incremental development.

Despite these structural differences, both traditions are increasingly influenced by transnational commercial practices and technological standards, often conceptualized as a form of *lex mercatoria*[1] or, more recently, *lex digitalis*.[2]

---

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

While maintaining unity, paras. 1 and 4 are to be attributed to Andrea Stazi, 2 and 3 to Riccardo Jovine.

[1] In literature, see B. Goldman, *La lex mercatoria dans les contrats et l'arbitrage internationaux: réalité et perspectives*, in *Droit international privé: Travaux du Comité français de droit international privé*, 2e année, 1980, 221 ff., stressing that the lex mercatoria constitutes an autonomous and evolutionary body of rules grounded in commercial custom and transnational arbitral legitimacy.

[2] In literature, see C. Reed – A. Murray, *Rethinking the Jurisprudence of Cyberspace*,

These norms, shaped by market actors, technological innovations, and industry standards, tend to evolve outside formal legal systems and frequently outpace legislative processes.

Such a dynamic creates a recurring tension between legal certainty and innovation. As technological advancements emerge, regulatory frameworks often lag behind, resulting in a regulatory gap that must be bridged to facilitate innovation while preserving public interest objectives such as market integrity, consumer protection, and systemic stability.

In this context, the concept of "sandbox",[3] intended as "regulatory sandbox", represents an innovative and growing approach to managing the intersection of technological advancement and existing regulatory frameworks.

The concept of regulatory sandboxes emerged in 2015 with the UK's Financial Conduct Authority (FCA), which launched the first formalized regulatory sandbox to foster fintech innovation while managing risks to consumers and markets.[4]

Unlike traditional innovation models driven by private-sector competition, sandboxes represent a paradigm shift in regulatory philosophy, emphasizing collaboration between regulators, companies, and IT specialists to

Cheltenham, 2018, stressing that digital normativity increasingly emerges outside traditional state-based legal systems, through technical standards, platform rules, and code-based architectures, a phenomenon that can be conceptualized as *lex digitalis*.

[3] See National Institute of Standards and Technology (NIST), *"Sandbox"*, in *csrc.nist.gov*, 6 February 2026, defining the concept of sandbox as: «A system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions. In particular, an application in a sandbox is usually restricted from accessing the file system or the network».

[4] Cfr: Financial Conduct Authority (FCA), *Regulatory Sandbox*, in *fca.org.uk*, 2015, providing the foundational framework for the UK's regulatory sandbox initiative. It outlines the rationale, implementation strategies, and potential benefits of establishing a "safe space" where businesses can test innovative financial products, services, and business models without immediately incurring the full weight of regulatory requirements. The document highlights how regulatory sandboxes can promote fintech innovation by reducing time-to-market and costs for startups, facilitating access to funding, and enabling financial regulators to work closely with innovators to embed consumer protection mechanisms early in product development. It also discusses various implementation strategies, including tailored authorization processes, no-action letters, and individual regulatory guidance, all aimed at fostering responsible experimentation within financial markets. Furthermore, the report explores industry-led initiatives such as virtual sandboxes and sandbox umbrella companies, which could further enhance the fintech ecosystem by offering collaborative testing environments and structured oversight mechanisms. The FCA's recommendations also consider potential legislative changes that could provide greater regulatory flexibility to sandbox participants. The report underscores the FCA's commitment to balancing financial innovation with consumer protection, ensuring that regulatory frameworks evolve alongside technological advancements.

test novel products in controlled environments.
This way, instead of rigidly applying pre-existing regulations to new business models or technologies, sandboxes create a controlled experimentation space where companies can test their innovations under the supervision of regulatory authorities.[5]
This testing environment enables the evaluation of a new product or service's innovative potential and adherence to current regulations, allowing for adjustments and changes that would not be possible under normal operating conditions.
This methodology is particularly relevant in highly regulated sectors such as finance, energy, real estate, and healthcare, where regulation is intense and innovation may encounter obstacles due to the rigidity of regulation.[6]
The concept of regulatory sandbox can be interpreted as a practical application of the adaptive regulation theory, which recognizes how regulations must evolve in response to new technological challenges and opportunities.[7]
Rather than defining static and immutable rules, sandboxes facilitate the process of mutual learning between innovators and regulators.[8]
Developers have the opportunity to test their creations in a real-world context, receiving direct feedback on the practical implications of their ideas, while regulators become familiar with new technologies, gaining a more accurate understanding of the associated risks and benefits.
In this sense, the sandbox acts as a laboratory for regulatory experimentation, where different regulatory approaches are studied to understand which are most efficient and effective in fostering innovation and protecting

[5] See R. Plato-Shinar, *The Contribution of the Regulatory Sandbox to the Development of Artificial Intelligence Applications in the Financial Sector*, in *the journal Law, Society and Culture*, Vol. H, 2024, stressing how entrepreneurs gain mutual learning opportunities with the regulator, studying its approach to develop products tailored to regulatory requirements. At the same time, the regulator learns about new products early in their development, enabling a better understanding of their nature and the level of regulation needed.

[6] In this regard, see R. Markellos – S. Ennis – B. Enstone – A. Manos – D. Pazaitis – D. Psychoyios, *Worldwide Adoption of Regulatory Sandboxes: Drivers, Constraints and Policies*, in *SSRN*, 2024, 10 ff., stressing the relevant role of regulatory sandboxes in enabling innovation within highly regulated sectors such as finance, energy, healthcare, and transport, providing a space to test new products or services under controlled conditions, allowing adjustments that would be unfeasible under usual regulatory constraints. Conversely, this approach addresses systemic challenges where rigid rules often stifle experimentation. In this regard, see H. J. Allen, *Regulatory Sandboxes*, in *The George Washington Law Review*, 2019, 579 ff.

[7] See I. Ayres – J. Braithwaite, *Responsive regulation: Transcending the deregulation debate*, Oxford, 1992, 162, highlighting the relevance of participatory models in regulatory design by fostering collaboration between regulators and industry stakeholders.

[8] See R. Plato-Shinar, *The Contribution of the Regulatory Sandbox to the Development of Artificial Intelligence Applications in the Financial Sector*, cit., 6.

public interests.
The theory behind regulatory sandboxes acknowledges the importance of regulatory flexibility for technological advancement. Instead of blocking innovation with outdated rules, sandboxes allow regulatory authorities to adopt a more open and collaborative approach.
This creates an environment where industry operators can experiment, learn, and refine their strategies without being immediately constrained by existing rules. Such a model is particularly useful in areas such as artificial intelligence or blockchain, where the pace of change is so rapid that traditional regulatory frameworks struggle to keep up.[9]
In this sense, sandboxes are not considered spaces for deregulation but controlled environments for experimentation, where the main goal is to identify the right balance between promoting innovation and protecting the public through the direct observation of the effects of new technologies.
Thus, the sandbox acts as a bridge between theory and practice, providing an empirical basis for developing regulations that effectively foster innovation while ensuring the safety and transparency of markets.[10] This approach aims for evidence-based regulation, where rules are shaped by direct observation of the impacts of new technologies and by experience gained in the sandbox.
The controlled testing environment can also allow the development of "regulation as code", embedding regulatory obligations directly into the computer code of the tested products and services, and so enhancing adherence to the rules.[11]
This study undertakes a comparative analysis of the regulatory sandbox frameworks in the United Arab Emirates and Singapore, with the aim of examining how differing legal traditions, institutional configurations, and governance models in successful pro-innovation countries shape the desi-

[9] See.: T. Moraes, *Regulatory Sandboxes as Tools for Ethical and Responsible Innovation of Artificial Intelligence and their Synergies with Responsive Regulation: The Quest for AI Sovereignty, Transparency and Accountability - Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition*, in *SSRN*, 2023, 8.

[10] In this regard, see.: L. M. Santos – J. M. Rožanec, *Fostering Research & Innovation in AI through Regulatory Sandboxes*, in *16th International Technology Transfer Conference, Ljubljana, October 11th 2023*, 2023, 4, stressing how regulatory sandboxes facilitate evidence-based lawmaking, providing flexibility, adaptability, and innovation-friendliness required by new technologies.

[11] See also A. Stazi, *Smart Contracts and Comparative Law: A Western Perspective*, Cham, 2021, stressing how smart contracts and distributed ledger technologies facilitate legal and regulatory compliance automation. These mechanisms, by embedding legal obligations directly into their execution framework, present new regulatory challenges and require controlled testing environments to ensure adherence to existing legal frameworks.

gn, implementation, and evolution of regulatory sandboxes.
The central objective of the research is to identify and critically assess how these frameworks reconcile the dual imperatives of fostering technological innovation, particularly in fast-evolving sectors such as fintech, blockchain, and artificial intelligence, while safeguarding regulatory stability and systemic integrity.
Through this analysis, the study seeks to extract key insights and best practices that may inform the development of future regulatory strategies in diverse jurisdictions, offering a normative and practical contribution to the broader discourse on innovation governance in a comparative legal context.
The choice of the United Arab Emirates and Singapore as case studies is both deliberate and methodologically strategic. These jurisdictions, while sharing a common ambition to position themselves as global hubs for technological innovation, represent two distinct legal systems and regulatory philosophies.
The UAE operates within a mixed legal system: it combines elements of civil law, influenced by continental European legal traditions, with features of common law in certain emirates, and incorporates aspects of Sharia law in its broader legal landscape. Its regulatory architecture is characterized by a polycentric and pluralistic model, in which multiple sector-specific sandboxes, overseen by different regulatory bodies, coexist within a federal framework that promotes localized experimentation while aligning with national strategic objectives in digital transformation and economic diversification.[12]
By contrast, Singapore's legal system is firmly rooted in the common law tradition, and its regulatory sandbox model is governed in a centralized manner by the Monetary Authority of Singapore.
This monocentric approach reflects a regulatory philosophy grounded in standards-based, experimentalist governance, emphasizing regulatory coherence, transnational interoperability, and iterative learning.
Singapore's model is frequently cited as a benchmark for regulatory innovation in the Asia-Pacific region, while the UAE's multi-layered governance structure offers a unique laboratory for examining how legal pluralism

[12] In literature, see D. Zetzsche – R. P. Buckley – D. W. Arner – J. N. Barberis, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, in *Fordham Journal of Corporate & Financial Law*, 23(1), 2017, 45 ff. This observation aligns with a growing trend in jurisdictions such as the UAE, where regulatory sandboxes are not only used to test novel technologies, but are embedded within broader national strategies for economic diversification, foreign direct investment attraction, and post-oil development models. By offering controlled legal environments with temporary regulatory relief, these frameworks serve as catalysts for cross-sectoral innovation and long-term structural change.

interacts with regulatory experimentation.[13]
The comparative analysis of these two jurisdictions thus provides a compelling framework for exploring how legal traditions, institutional configurations, and strategic priorities shape the operation and impact of regulatory sandboxes.
By juxtaposing the UAE's polycentric and sectoral approach with Singapore's unified, standards-driven model, the study aims to elucidate the strengths and confines of each system, offering a nuanced understanding of how sandbox frameworks function not merely as regulatory tools but as instruments of broader economic, technological, and geopolitical strategy.
Ultimately, the research seeks to contribute to the practice of a comparative regulatory innovation, highlighting how legal systems can adapt to the challenges of the digital age by designing sandbox models that balance flexibility and oversight, experimentation and stability, innovation and public interest.

2. Regulatory Sandboxes in the United Arab Emirates

The United Arab Emirates has emerged as a regional and global leader in developing regulatory sandboxes that support innovation, entrepreneurship, and digital transformation in finance and other high-tech sectors.
As a federation composed of seven emirates, each with considerable autonomy, the UAE's regulatory sandbox landscape reflects a combination of national-level strategy and emirate-specific initiatives.
Since the mid-2010s, the UAE government has pursued a coordinated approach to regulatory innovation, driven by federal entities such as the Central Bank of the United Arab Emirates, the Securities and Commodities Authority, and the Telecommunications and Digital Government Regulatory Authority, alongside pioneering efforts by individual emirates like Abu Dhabi and Dubai.
In November 2016, the Abu Dhabi Global Market introduced its regulatory sandbox through the Financial Services Regulatory Authority.
The Abu Dhabi Global Market RegLab provided a key node in the UAE's sandbox ecosystem, with a strong focus on digital banking, sustainable finance, and cross-border innovation.
The Financial Services Regulatory Authority encouraged experimentation

[13] *Ibid.*, 40 ff. This regulatory design embodies a shift away from static rule-making toward iterative and empirical governance, whereby regulators observe, evaluate, and recalibrate rules in response to real-time feedback from sandbox participants. Such a model not only facilitates more nuanced risk assessment but also allows legal systems to co-evolve with technological change, enabling the emergence of more agile and context-sensitive regulatory responses.

while maintaining strong consumer protection and AML/CFT standards, and it regularly coordinated with international regulators.[14]
This initiative positioned Abu Dhabi as an early leader in regulatory innovation, aligning closely with the UAE's broader national objectives.
A major milestone in the UAE's regulatory sandbox journey followed in 2017, with the launch of the Innovation Testing Licence by the Dubai Financial Services Authority within the Dubai International Financial Centre.
The Innovation Testing Licence was designed to provide fintech firms with a structured, controlled environment in which to test innovative products, services, and business models under tailored regulatory oversight.
This initiative mirrored the sandbox model first introduced by the UK's Financial Conduct Authority, but it was adapted to Dubai's legal and business environment, emphasizing international best practices, business-friendly regulation, and technology-driven growth.[15]

[14] Applications to the ADGM RegLab are accepted in cohorts, with the ADGM announcing publicly when each new application window opens. The RegLab is open to all entities operating in the FinTech sector, ranging from startups to established, regulated firms. To be eligible, FinTech applicants must present an innovative technological solution that is sufficiently developed and ready for testing. Additionally, the solution should support the advancement of the UAE's financial sector. As outlined in the Financial Services Regulatory Authority, *FinTech Regulatory Laboratory Guidance*, in *assets.adgm.com*, 2016, 3 ff., this framework demonstrates ADGM's commitment to enabling innovation in financial technology by offering a controlled environment where eligible firms can develop and live-test innovative solutions under customized regulatory requirements. By adopting a tailored, risk-based approach to regulation, the RegLab not only fosters market entry and experimentation but also ensures critical safeguards are in place to protect consumers, maintain market integrity, and support compliance with international standards such as anti-money laundering and counter-terrorism financing measures.

[15] Dubai Financial Services Authority, *Innovation Testing Licence*, in *dfsa.ae*, 2017 (updated May 2025). The Innovation Testing License (ITL) is a restricted financial services license that functions as Dubai's formal regulatory sandbox, allowing eligible firms to test innovative financial products, services, or business models in or from the Dubai International Financial Centre without being subject to the full regulatory requirements normally imposed on Authorized Persons. As detailed, firms must demonstrate a genuine need for testing, the use of innovative technology, operational readiness, and an intention to scale following successful testing. The ITL process comprises several structured stages: pre-application, full application with a detailed test plan, supervised live testing under a simplified regulatory framework, and exit, either through graduation to an unrestricted license or a controlled withdrawal. The DFSA may grant temporary waivers or modifications to certain regulatory rules (e.g., capital requirements, conduct rules) while maintaining essential obligations related to integrity, consumer protection, and anti-money laundering. The test plan must outline risk mitigation strategies, customer engagement practices, performance benchmarks, and contingency measures. Typically, the ITL is valid for 6-24 months, during which firms are closely supervised by the DFSA. After the testing phase, firms must either prove readiness for full authorization or cease operations, thus ensuring a robust but flexible regulatory approach that encourages innovation without compromising market integrity or consumer safety.

The Innovation Testing Licence process included defined stages, from application and evaluation to restricted live testing and potential graduation to full regulatory licensing, allowing firms to innovate safely while offering regulators insights into how emerging technologies function in real-world conditions.[16]

Dubai's regulatory sandbox quickly became a magnet for firms in the Fintech, Insurtech, and RegTech sectors, including digital payment providers, AI-driven risk platforms, and blockchain startups.

In this framework, artificial Intelligence represents a key area of focus for sandbox-enabled innovation. The UAE National Strategy for Artificial Intelligence 2031, launched in 2018, emphasized regulatory flexibility as a prerequisite for AI development across multiple sectors, including finance, transportation, and healthcare.[17]

A foundational component of the UAE's regulatory innovation strategy is RegLab, the national Regulations Laboratory launched in 2019 in partnership with the Dubai Future Foundation.

Designed to pre-emptively craft legislation for emerging technologies, RegLab has played a pivotal role in piloting projects such as electric cargo aircraft, self-driving vehicles, fractional bonds, and national health data

[16] DFSA, *DFSA Annual Report 2019*, in *dfsa.ae*, 2019, 4-5, 8-9, 42-43. The 2019 Annual Report provides a detailed account of the DFSA's continued commitment to fostering innovation through its regulatory sandbox framework, specifically the ITL program. In 2019, the DFSA admitted eight new applicants to the ITL, reflecting a steady interest in the program across diverse fintech verticals, including digital payments, robo-advisory, RegTech, and crowdfunding. The report notes that the ITL follows a structured yet flexible process comprising pre-application, application, restricted live testing, and eventual exit, either through full authorisation or withdrawal. One significant milestone highlighted in the report was the successful graduation of a property crowdfunding firm from the ITL to become a fully authorised entity, illustrating the programme's role as a launchpad for innovative business models. The DFSA underscores its dual role in encouraging fintech innovation and ensuring consumer protection, financial stability, and market integrity. The DFSA's engagement with the Global Financial Innovation Network (GFIN) and its leadership in cross-border testing initiatives also exemplify how the ITL contributes to international regulatory harmonisation. The Annual Report also emphasizes how the DIFC's geographic and strategic positioning has made it an attractive jurisdiction for firms aiming to scale across the Middle East, Africa, and South Asia (MEASA) region. Through its sandbox, the DFSA gathers valuable regulatory insights, enabling it to assess potential policy adaptations in response to emerging financial technologies and business models

[17] UAE Government, *UAE National Strategy for Artificial Intelligence 2031,* in *u.ae*, 2018, 22–25, 40, 42–43. The strategy identifies regulatory flexibility as a critical enabler for the development and deployment of AI across sectors, including finance, transportation, and healthcare. It promotes the UAE as a global testbed for AI by encouraging adaptive governance, sector-specific pilot programs, and collaborative efforts through the UAE Artificial Intelligence and Blockchain Council.

registries.[18]

Its mission to align regulation with innovation directly has supported the UAE's role as a global testbed for future technologies.

In response, the Dubai Financial Services Authority expanded the Innovation Testing Licence in 2021 to include AI-powered financial tools, such as algorithmic trading systems, credit scoring engines, and customer service chatbots.[19]

---

[18] UAE Regulations Lab, or RegLab, was created to spark new markets in the UAE by fast-tracking the adoption of emerging technology. It's where regulators enable new business activity based on agile regulations. RegLab aligns the government with the private sector's intent to create regulatory frameworks that accelerate Industry 4.0. Launched in Jan 2019 in partnership with DFF, collaborates with business leaders and tech innovators, works closely with lawmakers from local and federal authorities to develop legislation governing technology, incubates and creates new markets based on technology pilots, supports the UAE's role as a testbed for emerging technology. Among its key initiatives is the licensing of electric cargo aircraft, granted in March 2023, as part of a national push toward sustainable and environmentally friendly transportation. This move aims to reduce carbon emissions in the logistics sector by encouraging the use of clean energy and reimagining traditional freight practices through innovation. In parallel, RegLab issued a temporary licence to UPS to test electric vertical takeoff and landing (eVTOL) aircraft within the UAE. This initiative is designed to support the development of new, sustainable air cargo solutions while establishing a legislative framework that can accommodate next-generation aviation technologies. It reflects the UAE's broader commitment to environmentally conscious economic competitiveness. Within the healthcare sector, the Ministry of Health and Prevention, in collaboration with RegLab, launched two pioneering projects: a national health data repository and a disease registry system. The repository seeks to connect stakeholders and harness advanced tools such as artificial intelligence to conduct data-driven health studies. The disease registry focuses on improving the quality and comprehensiveness of national patient data, beginning with developing interactive dashboards and progressing toward automated reporting systems. The UAE also took a significant step in mobility by approving a temporary licence to test self-driving vehicles, making it the first country in the Middle East and the second globally to do so. This initiative underlines the country's dedication to integrating advanced technologies into public infrastructure and transport systems. In financial innovation, a pilot licence was issued for the fractional bonds project under the oversight of the Securities and Commodities Authority. This initiative aims to introduce flexible, secure financial instruments that meet investor needs while adhering to international standards of transparency and confidentiality. In this regard, see UAE, *Regulatory sandboxes in the UAE*, in ***u.ae***, 2024.

[19] See R. Plato-Shinar, *The Contribution of the Regulatory Sandbox to the Development of Artificial Intelligence Applications in the Financial Sector*, cit., providing a comparative and conceptual analysis of how regulatory sandboxes, particularly in tightly regulated sectors such as finance, have become essential for fostering responsible innovation in AI. It highlights the sandbox's role in enabling AI-based services such as algorithmic trading, credit scoring, robo-advisory, and chatbots, under the regulator's oversight. The author emphasizes the sandbox's mutual-learning dynamic: while startups gain insight into compliance needs, regulators observe emerging technologies early and adapt rules accordingly. These insights reinforce the expanded scope of sandboxes like the DFSA's

The establishment of the Artificial Intelligence Lab at the Dubai International Financial Centre FinTech Hive provided a dedicated venue for simulating and assessing AI-driven use cases before full-scale deployment, thereby integrating regulatory foresight with technical experimentation.
The Emirate of Dubai's broader innovation ecosystem, which includes the Dubai Future Accelerators[20], the Smart Dubai initiative[21] and the Dubai Universal Blueprint for AI[22], complements the regulatory sandbox model by promoting collaboration between startups, regulators, and government agencies involved in implementing, overseeing, or complementing these programs such as the Dubai Future Foundation, Digital Dubai Authority, Dubai Centre for Artificial Intelligence and the Dubai Financial Services Authority.
This integrated approach is further formalized by the launch of Sandbox Dubai in August 2024 by the Dubai Future Foundation. Conceived under the ambitious Dubai Economic Agenda D33,[23] this initiative represented a major step toward a unified regulatory experimentation framework for

ITL, which began with fintech and evolved to accommodate AI-driven financial solutions.

[20] Dubai Future Accelerators is a government-led initiative designed to foster collaboration between startups, private entities, and government agencies to address specific challenges through innovative technologies. While DFA is not a regulatory sandbox like the DFSA's Innovation Testing Licence (ITL) program, it plays a complementary role by facilitating the development and testing of cutting-edge solutions, including blockchain technologies, within Dubai's innovation ecosystem. Startups participating in DFA have the opportunity to work closely with government entities, which can pave the way for regulatory engagement and potential integration into programs like the ITL.

[21] Following the successful implementation of its initial goal to transform the city into a Smart City by 2017, the Dubai Government advanced its digital agenda by launching the "Smart Dubai 2021 Strategy". This comprehensive strategy aimed to elevate the city's standing by focusing on four strategic pillars designed to enhance the quality of life and business environment. Specifically, the strategy was structured around making services "Seamless", by providing integrated daily life services; "Efficient", by optimizing the use of city resources; "Safe" by anticipating risks and protecting people and information; and "Personalised", by enriching life and business experiences for all. The launch of this strategy provided a clear roadmap for the emirate's continued digital transformation, building directly on the foundation laid by its predecessor. In this regard, see UAE, *Smart Dubai 2021 Strategy*, in *u.ae*, 2024

[22] See UAE, *Dubai Universal Blueprint for Artificial Intelligence*, in *u.ae*, 2024, a comprehensive plan designed to accelerate the adoption of AI applications across the emirate. As a key part of the Dubai Economic Agenda D33, it aims to boost Dubai's economy by an annual AED 100 billion and increase productivity by 50% through innovative digital solutions. The blueprint serves as a roadmap to enhance the quality of life by incorporating AI across all strategic sectors, attracting global AI talent and companies, delivering superior government services, and transforming Dubai into a global hub for AI governance and legislation. Initial actions include appointing a Chief AI Officer in every government entity and introducing a specialized AI commercial license.

[23] Government of Dubai, *Dubai Economic Agenda D33*, in *u.ae*, 2023.

emerging technologies. Spearheaded by the Dubai Future Foundation in collaboration with various government entities, Sandbox Dubai was designed to foster innovation in key areas such as AI, Web3, biotechnology, the metaverse, and sustainability. Unlike traditional regulatory sandboxes limited to a single sector or authority, Sandbox Dubai functions as a cross-sector, multi-stakeholder platform that facilitates public-private collaboration in both testing new technologies and co-developing adaptive regulatory frameworks.[24]

Notably, Dubai's Blockchain Strategy, launched in 2016, set the ambitious target of becoming the first city powered entirely by blockchain technologies.[25] While full implementation was not achieved by the original 2020 deadline, significant strides were made, with blockchain-based firms admitted into the Innovation Testing Licence sandbox to explore applications such as decentralized finance, supply chain verification, and tokenization.

The UAE's commitment to innovation-friendly regulation was reinforced with the creation of the Virtual Assets Regulatory Authority in Dubai in

[24] Dubai Future Foundation, *Sandbox Dubai*, in *sandboxdubai.gov.ae*, August 2024. The Sandbox Dubai initiative, launched in August 2024 by the Dubai Future Foundation, is a specialized digital hub designed to enhance the effectiveness of the Emirate's regulatory ecosystem. Its creation is explicitly tied to the goals of the Dubai Economic Agenda D33, which seeks to double Dubai's economic size and cement its position among the world's top three urban economies by 2033. The sandbox aims to achieve this by acting as a central mechanism to connect innovators, regulators, and investors, significantly streamlining the process from innovative ideation to achieving formal regulatory approval. By late 2024, thematic sandboxes had already been launched under its umbrella, including for the Gig Economy and PropTech, demonstrating early implementation success. In 2025, Sandbox Dubai entered a phase of full-scale operation, signing its first international memorandum of understanding with the Artificial Intelligence Center Hamburg, and establishing itself as a global reference point for scalable experimental governance. The platform reinforces Dubai's vision of becoming a leading urban testbed for future technologies, while aligning regulatory flexibility with economic transformation.

[25] Smart Dubai, *Dubai: The First City on the Blockchain*, in *digitaldubai.ae*, January 2017, outlining the launch and ambition of the Dubai Blockchain Strategy, introduced in October 2016 with the goal of making Dubai the first city fully powered by blockchain technology by 2020. Developed jointly by the Smart Dubai Office and the Dubai Future Foundation, the strategy is built on three pillars: government efficiency (implementing blockchain in public sector services), industry creation (fostering a blockchain ecosystem with startups, accelerators, and regulatory support), and international thought leadership (positioning Dubai as a global hub for blockchain knowledge and innovation). The document stresses implementation plans involving over a dozen government entities and outlines a governance framework to support pilot projects in sectors such as energy, tourism, real estate, and health. Also describes Dubai's plans for policy development, global startup competitions, training programs, and public–private collaboration through the Global Blockchain Council. The strategy reflects Dubai's broader vision of embracing emerging technologies to transform government operations, stimulate economic growth, and export its blockchain model globally.

2022.

As a specialized body dedicated to the oversight of virtual assets, the Virtual Assets Regulatory Authority has introduced a bespoke regulatory framework covering crypto-assets, NFTs, and emerging use cases such as metaverse platforms.

Operating independently from the Dubai Financial Services Authority, but aligned with the UAE's overarching legal and compliance objectives, VARA enables sector-specific regulation while addressing the unique risks posed by decentralized digital economies.[26] This layered, multi-regulator model supports adaptive and coherent regulatory responses, even as technologies evolve at different speeds across domains.

At the federal level, regulatory sandboxes are increasingly being used in the UAE to facilitate innovation across sectors beyond finance. These initiatives are guided by principles of transparency, proportionality, risk mitigation, and inter-agency collaboration, enabling faster regulatory learning and agile policy responses to emerging technologies.

The UAE has rapidly expanded its capacity for regulatory innovation, moving beyond simple frameworks to establish comprehensive ecosystems that actively shape its future economy. In 2020, the Central Bank of the UAE significantly amplified these efforts by launching a broad regulatory sandbox program to support advancements in banking, payments, and open finance.

Crucially, this drive extended to targeted sectoral transformation. The

[26] Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai. The law states that the Dubai Virtual Assets Regulatory Authority (VARA) is established as an independent public authority affiliated with the Dubai World Trade Centre Authority, endowed with legal personality and financial and administrative autonomy (art. 4). Its jurisdiction covers all virtual asset activities in the Emirate of Dubai, excluding the Dubai International Financial Centre (art. 3). The stated objectives of VARA include promoting Dubai as a regional and global hub for virtual assets, encouraging innovation and investment in the sector, and developing a digital economy (art. 5). To achieve these objectives, VARA is empowered to issue permits for a defined set of virtual asset-related activities, such as the operation of exchanges, custodianship, wallet provision, and token issuance, and to supervise compliance through ongoing regulatory oversight (Arts. 15-16). Of particular relevance to innovation governance, the law enables VARA to classify new activities and define regulatory requirements accordingly, allowing for adaptive responses to emerging technological developments (art. 16(c)). Moreover, VARA has the authority to suspend activities or trading operations if public interest or market integrity so requires (art. 18), reflecting a responsive and risk-sensitive regulatory posture. The legislation further mandates coordination with domestic and international stakeholders, and expressly empowers VARA to propose new legislation and establish legal entities to support its regulatory functions (art. 6(11), 6(14), 6(15)). Taken together, these provisions form a flexible regulatory infrastructure that, while not explicitly labeled a "sandbox," mirrors the structure and purpose of regulatory sandboxes by enabling limited, supervised experimentation in rapidly evolving domains such as digital assets, blockchain technologies, and related fintech innovations.

Central Bank of the UAE simultaneously introduced a specialized insurance sandbox, not merely to test products, but with the stated ambition of turning the entire insurance sector into a smart, technology-driven marketplace. The initiative is highly strategic, focused on both safeguarding consumers and actively nurturing Emirati FinTech leadership in the Insurtech space. The focused regulatory experimentation allows the Central Bank of the UAE's Insurance sector to gain vital insight into the risks of new digital products, ensure customer protection, and foster an innovation-friendly environment that collaborates with FinTech firms, as detailed in the Sandbox Conditions Regulation.[27]

Such a spirit of proactive, collaborative regulation has only intensified. In January 2024, the United Arab Emirates demonstrated its international leadership by launching the Global TradeTech Sandbox in partnership with the Ministry of Economy, the Abu Dhabi Department of Economic Development, and the World Economic Forum. Such a move positions the Emirates at the forefront of establishing global best practices for trade technology adoption, underscoring the country's commitment to international regulatory cooperation.

The focus on enabling technological growth continued into February 2024, when the Telecommunications and Digital Government Regulatory Authority introduced the ICT Regulatory Sandbox. This initiative directly addresses the backbone of the digital economy by fostering a proactive legislative environment necessary for developing and deploying innovative Information and Communications Technology services, ensuring the long-term sustainability and growth of the digital sector itself. Together, these sandboxes form a cohesive targeted strategy to ensure that regula-

[27] The Central Bank of the UAE introduced its regulatory sandbox within the insurance sector as part of its response to the fast-paced digital transformation reshaping the global economic and financial environment. These technological advancements, driven primarily by the private sector and global digitization trends, are revolutionizing industries while also presenting both opportunities and challenges for insured individuals, policyholders, beneficiaries, companies, stakeholders, related professionals, and regulators alike. To address these shifts, the Central Bank's Insurance Sector has implemented the Sandbox Regulation, which outlines the regulatory framework governing the operation and oversight of this experimental environment. The key objectives of this initiative include: Gaining insight into new insurance products and identifying associated risks to ensure customer protection and satisfaction during testing phases; Transitioning the UAE insurance market into a smart, technology-driven marketplace; Encouraging the growth of emerging Emirati FinTech firms; Establishing a supportive, innovation-friendly environment for the insurance industry, one that fosters collaboration with FinTech companies, enhances regulatory practices, and contributes to broader economic development and effective risk management. Central Bank of the U.A.E., *Sandbox Conditions Regulation*, in *rulebook.centralbank.ae*, April 15, 2024

tion is a catalyst, not a constraint, for the nation's economic ambitions.[28]
As of today, the UAE's regulatory sandbox ecosystem stands as one of the most sophisticated and integrated in the world.
Rather than treating sandboxes as isolated experiments, the UAE embeds them into a national innovation framework that includes accelerator programs, public-private partnerships, and strategic legal reforms. Each emirate contributes to this ecosystem in alignment with federal priorities, creating a collaborative environment for testing, learning, and scaling innovation.
The country's proactive, forward-looking approach to sandbox governance, anchored in flexibility, inclusivity, and international best practice, has positioned the UAE as a global reference point for smart regulation in the digital age.
While the United Arab Emirates' framework is undeniably comprehensive, the challenge lies in its very sophistication. The proliferation of specialized and geographically distinct sandboxes, such as those managed by the Dubai Financial Services Authority, the Central Bank of the United Arab Emirates, the Telecommunications and Digital Government Regulatory Authority, and the newly established Sandbox Dubai, presents a critical operational hurdle.
The major ongoing challenge is managing decentralization and ensuring seamless modernization and cooperation, in line and on top of what increasingly occurs among companies[29], authorities and sandboxes.
True systemic success requires these regulatory and governmental autho-

[28] TDRA, *ICT Regulatory Sandbox*, in *tdra.gov.ae*, February 2024, emphasizing that the initiative is a strategic regulatory tool developed to support the UAE's national priorities by enabling safe experimentation with emerging ICT technologies in a controlled environment. It stresses the importance of regulatory agility to accommodate innovation without compromising consumer protection or market stability. The Sandbox offers selected participants, particularly start-ups and SMEs, a temporary regulatory respite to test novel digital services and business models, provided they deliver clear added value and meet specific eligibility and performance criteria. Through a structured lifecycle and with TDRA's oversight, the initiative gathers evidence to shape future regulatory frameworks, ensuring that technological advancement proceeds in tandem with responsible governance.

[29] See G. Ghidini – A. Stazi, *Coopetition: the role of IPRs*, in *Innovation, Competition and Collaboration*, 2015, 15 ff., which highlight that effective cooperation and collaboration among competitors, or coopetition, is increasingly essential for innovation and business in complex technological environments. It emphasizes the creation of value networks that reduce costs, foster R&D, expand markets, address technological challenges, and comply with regulations developing new industry standards. The authors frame coopetition as a balanced interaction of competition and collaboration, grounded in contractual freedom and legal protections, which provides a strong basis and incentive for decentralized actors such as authorities and sandboxes to modernize and cooperate effectively.

rities to not merely cooperate with the external private companies utilizing the sandboxes, but to effectively cooperate with each other.
Without robust, standardized protocols for sharing data, findings, and best practices across different jurisdictions and specialized regulators, the risk of fragmentation remains.
Overcoming this internal coordination complexity is the key to maintaining the ecosystem's agility and ensuring that the United Arab Emirates' impressive regulatory innovation framework truly functions as a cohesive national model.

3. Regulatory Sandbox in Singapore

Singapore's regulatory sandbox framework has become one of the most influential and widely cited models globally, embodying the city-state's proactive and strategic approach to financial and technological innovation.
The origins of Singapore's sandbox can be traced back to November 2016, when the Monetary Authority of Singapore launched its original FinTech Regulatory Sandbox initiative. This move was part of a broader national agenda to position Singapore as a global FinTech hub, articulated under the Smart Financial Centre vision.[30]
Unlike many early sandbox models focused narrowly on financial products, the Monetary Authority of Singapore's initiative was deliberately broad in both scope and participation. It permitted experimentation not only across financial sectors – such as payments, wealth management, insurance, and even RegTech – but also among a wide range of actors, including not just traditional financial institutions, but also FinTech start-ups and professional services firms partnering with them.

[30] Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines*, in *mas.gov.sg*, November 2016, defining the sandbox as a regulatory tool to support experimentation with innovative financial services in a live environment, while maintaining safeguards to contain failure. MAS outlines key objectives such as enhancing efficiency, managing risk, creating new opportunities, and improving lives through technology-driven financial innovation. MAS sets eligibility criteria – including the novelty of the solution, consumer benefit, readiness for market, and risk mitigation plans – and clarifies which regulatory requirements may be relaxed (e.g., capital adequacy, licensing fees), and which must remain in place (e.g., anti-money laundering, customer data confidentiality), reflecting MAS's strategic vision of building a Smart Financial Centre by fostering safe and agile FinTech development. Monetary Authority of Singapore, A Smart Financial Centre (Speech by Mr. Ravi Menon, Managing Director, MAS), MAS, 2015. In this foundational speech, Menon outlines Singapore's vision to become a global fintech hub by integrating innovation and technology into the financial system, emphasizing regulatory flexibility, experimentation, and collaboration as key enablers of a "Smart Financial Centre".

A distinctive feature of Singapore's first sandbox was its flexibility: regulatory requirements could be adjusted on a case-by-case basis, depending on the nature, risk profile, and maturity of the innovation being tested.[31] Nonetheless, the Monetary Authority of Singapore remained prudent in its allocation of sandbox approvals.[32]

As early as 2019, learning from practical experience, the Monetary Authority of Singapore introduced the Sandbox Express, a faster-track version of the original framework designed for lower-risk activities such as insurance brokering, and recognized market operators dealing with simple products.[33]

This initiative significantly reduced approval timeframes from months to

[31] Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines*, cit., as stated in para. 2.2, MAS invites not only licensed financial institutions but also other interested firms – including FinTech start-ups and technology service providers – to apply for sandbox entry, provided their activities fall under MAS's regulatory remit. In para. 6.2(a), MAS highlights that applications should involve genuinely novel financial services, either by introducing new technologies or by applying existing ones in an innovative way. In para. 5.5, MAS makes it clear that sandbox applications replicating existing services in Singapore will only be considered if applicants can demonstrate a distinct technological or operational differentiation. Furthermore, as in para. 5.5 (b), the firm must show evidence of due diligence, including prior testing in a controlled environment and understanding of relevant legal and regulatory obligations. MAS does not restrict the sandbox to specific sectors, as noted implicitly in para. 4.1; instead, it assesses applications across a broad spectrum, provided they aim to improve efficiency, manage risk, create new opportunities, or enhance consumer outcomes (para. 5.2). Para. 6.2 (c - g) outline the operational evaluation criteria, such as the firm's ability and intent to scale the service in Singapore post-sandbox, the definition of test scenarios and success indicators, the articulation of boundary conditions (including limits on time, customers, and transactions), and the presence of robust risk mitigation and exit strategies. Importantly, para. 2.3 and Annex A emphasize MAS's case-by-case approach to regulatory relief: certain requirements (e.g., capital adequacy, license fees) may be temporarily relaxed, while core obligations related to customer protection and financial integrity (e.g., AML/CFT compliance, data confidentiality) must remain in force. As indicated in para. 7.3 - 7.5, successful completion of the sandbox requires the firm to either transition to full compliance for broader market deployment or exit the sandbox in a manner that ensures all customer obligations are fulfilled.

[32] See C. C. Chen, *Regulatory Sandboxes in the UK and Singapore: A Preliminary Survey*, in *papers.ssrn.com*, 2020, which highlighted that MAS had only awarded six sandboxes by the end of 2018, showed that half of these (three out of six) were related to the insurance sector, namely, PolicyPal, Inzsure, and MetLife. The remaining sandboxes focused on other areas: one in digital advisory services (Krystal Advisors), one in money changing (Thin Margin), and one in cross-border remittance (TransferFriend).

[33] Monetary Authority of Singapore, *Sandbox Express Guidelines*, in *mas.gov.sg*, 2019 (updated January 2022), 3, aiming to streamline the testing of innovative financial products by offering standardized constructs for lower-risk services, significantly reducing the time and resources required for market entry.

as little as 21 days, thereby enhancing Singapore's appeal to innovators seeking rapid market testing. By streamlining the regulatory process, the Monetary Authority of Singapore fostered a conducive environment for fintech growth, contributing to the establishment of over 1.000 fintech firms in Singapore by 2022.[34]

Blockchain technology soon became a key area of focus within Singapore's broader regulatory innovation framework. Notably, Project Ubin – a collaborative initiative led by the Monetary Authority of Singapore and major financial institutions to explore blockchain-based clearing and settlement – reflected the Monetary Authority of Singapore's commitment to fostering experimentation with distributed ledger technology under controlled, collaborative settings akin to sandbox principles.[35]

Building on these foundations, the Monetary Authority of Singapore welcomed applications from blockchain startups into its regulatory sandbox, facilitating experimentation in areas such as tokenization, decentralized finance, and cross-border payment solutions.[36]

Furthermore, the city-state demonstrated exceptional foresight with the enactment of the Payment Services Act 2019, which introduced a modular licensing framework for digital payment services – including crypto and blockchain firms – informed in part by the regulatory insights gained through earlier sandbox trials.[37]

With regard to artificial intelligence, Singapore has taken a similarly syste-

---

[34] Singapore Fintech Association – PwC, *FinTech's state of play: Taking stock of Singapore's FinTech landscape*, in *pwc.com*, 2022, 9. This growth reflects Singapore's strong regulatory support and its attractiveness as a regional base for innovation and expansion into ASEAN markets. At the same time, Singapore's fintech sector is maturing, moving from a start-up phase to a scale-up phase, offering a fertile environment for both local and international players.

[35] See.: Monetary Authority of Singapore, *Project Ubin: Central Bank Digital Money using Distributed Ledger Technology*, in *mas.gov.sg*, 2024. Project Ubin, launched by the Monetary Authority of Singapore in 2016, was a multi-phase collaborative initiative exploring the use of blockchain (distributed ledger technology) for clearing and settlement of payments and securities. While not part of the formal MAS regulatory sandbox, Project Ubin served as a parallel innovation initiative allowing real-world experimentation in a controlled environment. Its design echoed sandbox principles by enabling public-private sector collaboration and live testing of blockchain use cases without full-scale deployment risks. The project informed both MAS's approach to financial infrastructure innovation and its broader regulatory stance on digital assets and decentralized technologies.

[36] Singapore's regulatory sandbox has supported several blockchain-focused startups aligned with MAS's innovation agenda. For example, ADDX (formerly iSTOX) became the first platform to graduate from the sandbox in 2020, going on to operate under a Recognised Market Operator (RMO) license to enable tokenization and fractional trading of private market securities.

[37] *Singapore Parliament, Payment Services Act 2019 (No. 2 of 2019). Enacted on 14 January 2019*.

matic and forward-looking approach. The National Artificial Intelligence Strategy, launched in 2019, emphasized the importance of "AI model governance" and regulatory experimentation to support safe AI deployment.[38]

The Monetary Authority of Singapore has supported this development through the regulatory sandbox, in collaboration with AI-driven fintech firms working in areas such as credit scoring, fraud detection, and robo-advisory services, where regulatory clarity and consumer impact warrant controlled testing.[39]

In parallel, the Monetary Authority of Singapore launched the Veritas initiative to develop frameworks and open-source tools for implementing ethical AI in finance, aligned with the FEAT principles (Fairness, Ethics, Accountability, and Transparency). These tools may be adopted by firms testing AI solutions, including in sandbox environments, before wider deployment.[40]

A notable example is Kristal.AI, a digital wealth management platform that participated in the Monetary Authority of Singapore's FinTech Regulatory Sandbox to test its AI-driven robo-advisory services. Utilizing machine learning algorithms, Kristal.AI offered personalized portfolio recommendations and streamlined investor onboarding processes.

This participation demonstrated how AI-powered financial solutions

[38] See Smart Nation – Digital Government Office, *National Artificial Intelligence Strategy*, in *file.go.gov.sg*, 2019, 64 ff., setting out a whole-of-nation approach to AI deployment, including ethical model governance, public-private collaboration, and regulatory support for test-bedding AI systems. The strategy emphasizes responsible innovation and the need to adapt regulatory structures in tandem with technological advances; and B. Do – S. Gray, *Balancing Innovation and Oversight: Regulatory Sandboxes as a Tool for AI Governance*, in *Future of Privacy Forum*, 2025, which stress that regulatory sandboxes can stimulate AI development, enhance consumer protections, and help regulators develop more effective policies, as evidenced by Singapore's proactive AI governance testing efforts through the Infocomm Media Development Authority and AI Verify Foundation.

[39] See K. Lee, *Singapore Expands Its AI Governance Approach to Include Generative AI*, in *Lawflash*, 2024, that highlight the expansion of Singapore's AI governance framework with the introduction of the Model AI Governance Framework for Generative AI in 2024, which builds on earlier principles to address evolving AI risks, including bias, misuse, and lack of explainability.

[40] Smart Nation – Digital Government Office, *National Artificial Intelligence Strategy*, cit., 67. While the Veritas initiative is not part of the MAS regulatory sandbox itself, it plays a complementary role by addressing a major barrier to the responsible scaling of AI technologies – translating ethical principles into practical, testable standards. In the context of regulatory sandboxes, Veritas offers participating firms a structured way to evaluate and validate AI models during the experimentation phase. This alignment strengthens the sandbox's value not just as a testing ground for innovation, but as a mechanism for embedding governance and trust into AI-driven financial services from the outset.

could be responsibly trialed within a controlled regulatory environment, underscoring the importance of aligning innovative technologies with regulatory expectations and consumer protection standards[41].

Complementing these regulatory efforts, the Monetary Authority of Singapore also initiated Project Orchid, which explores the technical infrastructure for a potential digital Singapore dollar.

A key innovation under this initiative is Purpose Bound Money, which allows conditions to be embedded within digital currency, enabling targeted disbursements like government vouchers or subsidies. Purpose Bound Money has been tested in sandbox settings, offering regulators and innovators a safe environment to explore programmable digital money while preserving financial integrity and user protection.[42]

Singapore's sandbox ecosystem did not remain static. In 2021, the Mo-

[41] See L. Lin, *Regulating FinTech: The Case of Singapore*, in *SSRN Electronic Journal*, 2019, 94 ff., stressing that the sandbox model exemplifies Singapore's "innovator-centered" regulatory approach, where experimental financial services are trialed under relaxed requirements to evaluate regulatory fit while maintaining consumer safeguards and policy oversight. Kristal.AI's successful graduation from the sandbox illustrates how this framework facilitates FinTech development while ensuring regulatory integrity.

[42] Monetary Authority of Singapore, *Project Orchid: Programmable Digital SGD*, in *mas.gov.sg*, November 2022 and Monetary Authority of Singapore, *Purpose Bound Money (PBM): Technical Whitepaper*, in *mas.gov.sg*, June 2023. The Report served as a forward-looking exploration into the viability of a programmable digital Singapore dollar, with a specific emphasis on the concept of Purpose-Bound Money. This initiative did not set out to launch a retail central bank digital currency (CBDC) immediately but aimed instead to establish the foundational infrastructure and technical competencies required should the need for such a currency arise in the future. Project Orchid marked an extension of earlier experimentation by MAS into the retail space, having previously focused on wholesale digital currency solutions through initiatives such as Project Ubin. The 2022 report laid out a vision deeply aligned with Singapore's broader digital innovation goals, responsible financial governance, and inclusion. It emphasized that while Singapore's electronic payment systems were already advanced, the dynamic nature of the global digital asset landscape necessitated proactive research and preparedness. At the heart of Project Orchid was the idea of Purpose-Bound Money, a digital protocol that enabled money to be encoded with specific rules governing its use. This concept merged the strengths of programmable payment systems and programmable money, offering the ability to not only automate payments based on predefined conditions but also bind the money itself to its intended purpose. Such technology presented compelling opportunities across various domains, including government assistance programs, corporate incentives, charitable donations, and pre-paid consumer services. A notable aspect of the initiative was its inclusive approach to digital currencies. Rather than relying solely on a future CBDC, Purpose-Bound Money was designed to work with various digital instruments including securely backed stablecoins and tokenised bank deposits. This made the framework flexible and adaptable to different future scenarios. MAS clearly communicated that it did not yet see an urgent need for a retail CBDC, but the knowledge gained through Project Orchid would ensure that Singapore was prepared to move decisively if such a need emerged.

netary Authority of Singapore introduced the Sandbox Plus framework, enhancing support for early-stage Fintech startups. This initiative offers funding grants, regulatory guidance, and partnership opportunities through the Monetary Authority of Singapore Innovation Lab. Notably, Sandbox Plus introduced tiered levels of regulatory support, distinguishing between firms with lower regulatory risks and those requiring customized regulatory guidance.

This graduated approach underscores Singapore's progression from a sandbox pioneer to a sophisticated regulatory innovator, adept at tailoring interventions across a diverse technological landscape.[43]

Today, Singapore's regulatory sandbox infrastructure continues to serve as a global exemplar of progressive financial regulation. The Monetary Authority of Singapore operates the enhanced Sandbox Plus framework, which provides tailored support to startups innovating in fintech, blockchain, AI, and digital assets.

Complementary initiatives such as Project Guardian – a live industry pilot exploring asset tokenization and institutional DeFi – create sandbox-like environments for real-world experimentation involving regulated financial institutions.[44]

Furthermore, Singapore's leadership in cross-border regulatory cooperation, exemplified by its role in the Global Financial Innovation Network, enables firms to trial their solutions across multiple jurisdictions simultaneously, significantly lowering barriers to international market entry.

Thus, Singapore's approach has evolved beyond mere regulatory tolerance for innovation: it has become a dynamic ecosystem combining proactive regulation, public-private collaboration, and international interoperability. The city-state's continued success in sandbox regulation can be attributed to its unwavering commitment to maintaining a delicate balance between enabling technological breakthroughs and ensuring systemic resilience, consumer protection, and market integrity.

---

[43] Monetary Authority of Singapore, *MAS Enhances FinTech Regulatory Sandbox with Sandbox Plus*, in *mas.gov.sg*, 2021, reflecting MAS's recognition of the need for a more flexible, scalable regulatory environment as fintech innovation matures. By offering differentiated support based on firms' risk profiles and readiness levels, Sandbox Plus not only fosters experimentation but also aligns regulatory efforts with national priorities in digital finance, such as cross-border payments, green finance, and financial inclusion.

[44] Monetary Authority of Singapore – BIS, *Project Guardian: Enabling Open and Interoperable Networks*, in *mas.gov.sg*, 2023, initiative in collaboration with regulated financial institutions and international partners, designed to explore asset tokenization, open interoperable networks, and institutional DeFi protocols through live industry pilots. While not formally a regulatory sandbox, it facilitates real-world experimentation under supervisory conditions.

4. Approaches and Future Perspectives: a Comparative Framework

The comparative analysis of regulatory sandbox frameworks in the United Arab Emirates and Singapore reveals two distinct yet complementary models of innovation governance, each reflective of their unique legal, institutional, and geopolitical contexts. The UAE's polycentric approach, characterized by federal-emirate synergies and sector-specific sandboxes in domains such as finance, ICT, and TradeTech, leverages the country's federal structure to create a dynamic and adaptive regulatory ecosystem. Here, regulatory experimentation occurs across multiple jurisdictional levels, reflecting a regulatory pluralism that allows for sectoral specialization and localized innovation while maintaining alignment with national priorities, such as those articulated in the UAE National Artificial Intelligence Strategy 2031, and the Emirates Blockchain Strategy 2021, or at the emirate-level, the Dubai Economic Agenda D33.

This model resonates with Teubner's theory of legal pluralism, wherein multiple normative orders coexist and interact, fostering a regulatory environment that is both flexible and responsive to technological disruption.[45] Its evolution, from the 2016 FinTech Sandbox to Sandbox Plus and Project Guardian, illustrates a transition from reactive regulatory accommodation to proactive ecosystem design.

This trajectory aligns with Sabel and Zeitlin's "experimentalist governance", where iterative learning, feedback loops, and decentralized implementation inform adaptive regulatory policymaking.[46]

Both jurisdictions aim to balance innovation and systemic stability, but diverge in methodology.

The UAE leverages regulatory sandboxes to support geostrategic diversification, positioning itself as a global hub for emerging technologies such

[45] See G. Teubner, *Global Bukowina: Legal Pluralism in the World-Society*, in G. Teubner (ed.), *Global Law Without a State*, Darthmouth, 1996, 3 ff., that develops the notion of transnational legal pluralism, highlighting how autonomous regulatory subsystems, such as the lex mercatoria, interact with formal legal orders while maintaining its own internal logic; and A. Stazi, Smart Contracts and Comparative Law: A Western Perspective, cit., emphasizing how the automatic execution of smart contracts, with the relative trend towards a reduced use of the legal system, is in line with the general phenomenon of the increase in rules and private institutions which is giving rise to a gradual loss of relevance of state law.

[46] C. F. Sabel – J. Zeitlin, *Experimentalist Governance*, in D. Levi-Faur (ed.), *The Oxford Handbook of Governance*, Oxford, 2012, 169 ff., describing a model of governance in which central authorities set broad policy goals, while decentralized actors experiment with implementation. These practices are subject to iterative review and revision, a dynamic particularly relevant to Singapore's sandbox evolution from rule-based accommodation to adaptive regulatory design.

as blockchain, AI, and virtual assets, in line with its broader economic transformation agendas.[47]

Singapore, differently, adopts a standards-based and risk-calibrated approach, advancing regulatory exportability and ethical governance, as evidenced by the "Fairness, Ethics, Accountability, and Transparency" principles for AI and its leadership in the Global Financial Innovation Network.

Remarkably, while the UAE's multi-regulator model enables sectoral specialization, it risks fragmentation without strong inter-agency coordination, a challenge mitigated through federal oversight bodies like the Central Bank.

Singapore's regulatory approach, centered around the Monetary Authority of Singapore, effectively ensures regulatory coherence across the financial sector. However, the system must maintain flexibility to prevent this centralization from inadvertently stifling niche innovations (smaller, specialized, or unconventional financial technologies) that might not neatly fit established frameworks.

The comparative analysis underscores a key insight: while legal tradition, whether civil law, common law, or a hybrid system, provides the foundational context for regulatory design, it is the institutional configuration – polycentric versus monocentric – and the regulatory philosophy – sectoral pluralism versus unified governance – that most directly shape the sandbox's effectiveness as a governance tool.

The UAE's decentralized model fosters sectoral innovation and localized responsiveness but requires strong coordination to avoid regulatory fragmentation.

Singapore's centralized framework ensures coherence and regulatory clarity, but it must guard against rigidity that could stifle niche or frontier innovations.

Thus, regulatory sandboxes are not merely technical instruments for market experimentation, but they serve as strategic platforms for legal and policy learning, enabling jurisdictions to manage the complex interplay

[47] UAE, *We the UAE 2031*, in *u.ae*, 2022. This national strategy articulates the UAE's developmental trajectory for the next decade, with the ultimate aim of positioning the country as a global leader by its centennial in 2071. We the UAE 2031 outlines four strategic pillars, Forward Society, Forward Economy, Forward Diplomacy, and Forward Ecosystem, that encompass a wide range of priorities, including social empowerment, digital infrastructure, environmental sustainability, and international influence. Central to its economic vision is a highly diversified, innovation-driven economy that leverages cutting-edge technologies such as artificial intelligence, blockchain, and digital assets. The plan envisions a competitive private sector, a strong R&D ecosystem, and legislative agility that supports future industries. Regulatory sandboxes and innovation-friendly governance are explicitly framed as mechanisms for enabling this transformation. It is within this framework that the UAE uses its policy tools to achieve geostrategic diversification and economic resilience while maintaining systemic stability.

between innovation, risk, and regulation in a globalized technological landscape.

By juxtaposing the UAE's multi-level, sectoral model with Singapore's unified, standards-driven approach, this research provides valuable elements for other jurisdictions.

The comparison between the United Arab Emirates and Singapore reveals that institutional architecture, rather than legal tradition alone, determines the regulatory system's capacity to manage technological innovation.

The UAE's polycentric experimentation, rooted in the interaction between federal and emirate-level authorities, produces regulatory diversity and sectoral responsiveness but requires sophisticated coordination mechanisms to prevent fragmentation.

Singapore's monocentric experimentalism, by contrast, consolidates regulatory authority within the Monetary Authority of Singapore, ensuring coherence, predictability, and international interoperability, though at the risk of limiting unconventional or niche innovation.

Rather than representing opposing poles, the two systems illustrate complementary pathways of regulatory learning: UAE exemplifies adaptive pluralism, where innovation is driven through distributed experimentation; Singapore embodies coherent agility, where innovation is guided through unified governance and iterative refinement.

Together, they demonstrate that effective sandbox governance does not lie in a universal blueprint, but in a jurisdiction's ability to calibrate coherence and flexibility, centralization and diversity, in accordance with its institutional capacities and strategic ambitions.

In this sense, the comparative analysis of the UAE and Singapore highlights two distinct yet mutually informative models of regulatory innovation, each offering valuable lessons for jurisdictions seeking to reconcile experimentation with stability in the digital economy.

Abstract

Regulatory sandboxes have emerged as pivotal instruments for reconciling technological innovation with legal stability, particularly in sectors characterized by high regulatory density, such as finance, artificial intelligence, and blockchain. This comparative analysis examines the regulatory sandbox frameworks of the United Arab Emirates and Singapore, two jurisdictions that exemplify distinct institutional responses to the challenges of innovation governance and have been methodologically selected due to their shared ambition to position themselves as global hubs for digital transformation, while representing structurally divergent legal systems and regulatory philosophies. The UAE adopts a polycentric and sectoral model rooted in regulatory pluralism, where emirate-specific initiatives operate within a broader federal strategy. This structure enables localized experimentation while aligning with national objectives in digital transformation and geostrategic positioning. Singapore's unified approach, anchored in the Monetary Authority of Singapore, reflects a model of experimentalist governance characterized by regulatory coherence, iterative learning, and transnational interoperability. Despite their structural peculiarities, decentralized versus centralized, both models converge in their strategic function: enabling adaptive regulation, fostering innovation ecosystems, and safeguarding systemic integrity. The analysis underscores how legal design, institutional configuration, and normative priorities shape the deployment and evolution of regulatory sandboxes as tools of comparative regulatory innovation.

Keywords

Regulatory Sandbox – FinTech – Blockchain – Artificial Intelligence – Comparative Law

Riflessioni sull'evoluzione e sulla rilevanza del concetto di trasparenza algoritmica, dal GDPR all'Artificial Intelligence Act*

Alessandro Oldani

Sommario

1. La trasparenza algoritmica nel Regolamento generale sulla protezione dei dati (UE) 2016/679. - 2. Big Data, trasparenza algoritmica e i rischi per l'autodeterminazione dell'individuo. - 3. L'avvento dell'intelligenza artificiale generativa, l'evoluzione delle modalità di trattamento dei dati personali e la risposta della Commissione europea. - 4. La tutela dei diritti fondamentali nell'AI Act. Introduzione alla classificazione in base al rischio dei sistemi di intelligenza artificiale. - 4.1. Una breve panoramica sui sistemi "ad alto rischio". - 5. La tutela sostanziale dell'AI Act. Il ruolo dei *providers* e dei *deployers*. - 6. Il primo livello di trasparenza. - 7. La tutela degli "interessati", il secondo livello di trasparenza e gli obblighi dei *providers* e dei *deployers* nei confronti degli utenti finali. - 8. Interpretabilità e spiegabilità come presupposti della trasparenza algoritmica. - 9. Conclusioni.

1. La trasparenza algoritmica nel Regolamento generale sulla protezione dei dati (UE) 2016/679

Nel contesto del regolamento (UE) 2016/679 (GDPR), la trasparenza algoritmica può essere intesa come il diritto, riconosciuto agli interessati, di ottenere informazioni chiare e comprensibili sia sulle logiche alla base dei trattamenti automatizzati finalizzati a supportare o automatizzare decisioni, sia sulle motivazioni che giustificano l'esito finale di tali decisioni. Specularmente, ciò comporta anche l'obbligo - gravante sui soggetti chiamati a prendere le decisioni - di fornire ai diretti interessati (*data subjects),* le suddette informazioni[1]. La base giuridica di tale diritto è l'art. 22 GDPR, applicabile nei casi in cui l'individuo sia sottoposto a una decisione basata

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

unicamente sul trattamento automatizzato, compresa la profilazione, che «produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[2]. Il concetto di trasparenza algoritmica integra la tutela accordata dal GDPR al soggetto interessato, specificando – oltre al menzionato divieto di sottoporre individui a decisioni interamente automatizzate – il diritto riconosciuto a quest'ultimo ad essere informato, in termini comprensibili, circa le modalità logico/operative dell'algoritmo utilizzato, nonché la misura in cui l'*output* dello stesso abbia inciso sulla decisione finale. Al par. 2 del medesimo articolo sono altresì previste alcune eccezioni[3]. Di particolare interesse per le tematiche trattate in questa sede è la possibilità di instaurare procedimenti decisionali interamente automatizzati previo consenso dell'interessato, in cui emerge un'applicazione pratica del concetto di trasparenza algoritmica. La capacità del consenso – inteso come base giuridica legittimante il trattamento dei dati personali - di garantire un'adeguata protezione dell'individuo nei procedimenti decisionali automatizzati, infatti, è subordinata alla corretta formazione dello stesso, possibile soltanto – nel caso di specie – attraverso opportune informazioni trasmesse in termini chiari e comprensibili circa le modalità logico/operative dell'algoritmo.

Sul piano teorico, la proibizione generale del trattamento automatizzato senza intervento umano riflette la concezione giuridica europea delle nuove tecnologie e delle relative applicazioni, secondo cui l'intelligenza artificiale deve servire da strumento per l'attività umana, piuttosto che sostituirsi integralmente ad essa. Tale visione è stata definitivamente formalizzata nel c.d. AI Act, regolamento europeo sull'intelligenza artificiale, la cui proposta è stata avanzata dalla Commissione nel 2021 e il cui testo definitivo è stato approvato dal Parlamento europeo il 14 marzo 2024[4], del quale si tratterà più diffusamente in seguito, con particolare attenzione ai principi di proporzionalità, trasparenza e responsabilità che ne costituiscono l'impianto assiologico e operativo. Un accenno, seppur indiretto, al concetto di trasparenza algoritmica è infatti riscontrabile nell'art. 15, par. 1, lett. h) GDPR, in cui è sancito il diritto dell'interessato ad ottenere dal titolare del trattamento informazioni relative all'esistenza di un processo decisionale automatizzato, unitamente ad informazioni significative in merito allo stesso procedimento. La natura di tali informazioni significative è meglio

anonimo.

[1] P. Zuddas, *Brevi note sulla trasparenza algoritmica*, in *Amministrazione in Cammino*, 2, 2020, 1 ss.

[2] Regolamento (UE) 2016/679 (GDPR), art. 22.

[3] S. Borghi, *Decisioni automatizzate e profilazione: le indicazioni dei Garanti europei*, in *privacy.it*, 2 novembre 2017.

[4] Parlamento europeo, Risoluzione legislativa del 13 marzo 2024 sulla proposta di regolamento sull'intelligenza artificiale (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).

specificata negli artt. 13, par. 2, lett. f) e 14, par. 2, lett. g), GDPR[5], nei quali - oltre all'obbligo in capo al titolare del trattamento di rendere sempre edotto il soggetto interessato qualora vi fosse un trattamento decisionale automatizzato nei suoi confronti – viene specificato che tali informazioni vertono «sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

2. Big Data, trasparenza algoritmica e i rischi per l'autodeterminazione dell'individuo

Il tema della trasparenza algoritmica ha acquisito particolare rilevanza nell'utilizzo dei Big Data in ambito politico-elettorale[6]. L'utilizzo di algoritmi sempre più "opachi", in grado di "modellare" la personalità e le preferenze di un individuo – e, attraverso le c.d. *echo chambers*[7], indirizzarne le opinioni politiche – si pone in evidente contrasto con il diritto alla spiegabilità e alla conoscenza dei processi automatizzati.
Il considerando 63 GDPR è chiaro nel sottolineare il diritto dell'individuo di comprendere le modalità con le quali vengono prese le decisioni basate sui dati personali e sulla profilazione, ed in particolar modo a "comprenderne la logica". Questo non significa divulgare lo pseudocodice[8] o

[5] S. Stefanelli, *La trasparenza dell'algoritmo base della società del futuro: ecco perché è così importante*, in *agendadigitale.eu*, 3 maggio 2023.

[6] Per una più chiara comprensione della rilevanza economica, strategica e politica connessa all'acquisizione dei dati, cfr. G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma*, in *Rivista Italiana di Informatica e Diritto. Periodico Internazionale del CNR – IGSG*, 1, 2022 e S. Piva, *Forze politiche e garanzie giuridiche: spunti di riflessione sulla pronuncia del Garante dei dati personali in tema di piattaforma Rousseau*, in *dirittifondamentali.it*, 3, 2021, 447 ss.

[7] L'essere umano tende fisiologicamente a sviluppare *bias* cognitivi di conferma, ossia la propensione a ricercare informazioni che avvalorino convinzioni già maturate, evitando invece opinioni o dati contrari suscettibili di confutarle. Una volta profilato, l'algoritmo sotteso ai social network può proporre all'individuo contenuti coerenti con le preferenze politiche e valoriali manifestate in precedenza, riducendo così lo spazio per interpretazioni alternative della realtà. Tale dinamica, combinata ai preesistenti *bias* cognitivi della mente umana, rischia di favorire processi di radicalizzazione o, come emblematicamente evidenziato dal caso *Cambridge Analytica*, di consentire a determinati attori politici di orientare le tendenze individuali e di modellare conseguentemente la linea politica. Sul punto, M. Petrocelli, *Incoscienza digitale. La risposta alla rivoluzione digitale tra innovazione, sorveglianza e postdemocrazia*, Roma, 2022.

[8] "Pseudocode is a description of what a computer does, expressed in natural language instead of programming language». E. Ekohariadi - Y. Anistyasari - R. Putra - I. Kurniawan, Assessing Computational Thinking Using Pseudocode Programming Instrument, in Proceedings of the 4th National Seminar on Applied Technology, Science, and Arts (APTEKINDO 2018), 2018, 134 ss.

la *flowchart*[9] alla base degli algoritmi – i quali risulterebbero comunque incomprensibili per la maggior parte degli utenti - bensì mettere l'utente medio nelle condizioni di svolgere le proprie attività online avendo il più possibile contezza del valore commerciale e politico derivante dalla sua profilazione, affinché possa prestarvi o meno un autonomo ed indipendente consenso. La Cassazione si è recentemente espressa circa la corretta formazione del consenso dell'utente nel caso sia profilato o sottoposto a procedimento decisionale automatizzato. Ad integrare i presupposti del libero e specifico consenso, infatti:

«è richiesto che l'aspirante associato sia in grado di conoscere l'algoritmo, inteso come procedimento affidabile per ottenere un certo risultato o risolvere un certo problema, che venga descritto all'utente in modo non ambiguo ed in maniera dettagliata, come capace di condurre al risultato in un tempo finito. Che, poi, il procedimento, come spiegato con i termini della lingua comune, sia altresì idoneo ad essere tradotto in linguaggio matematico è tanto necessario e certo, quanto irrilevante: ed invero, non è richiesto né che tale linguaggio matematico sia esteso agli utenti, né, tanto meno, che essi lo comprendano»[10].

3. L'avvento dell'intelligenza artificiale generativa, l'evoluzione delle modalità di trattamento dei dati personali e la risposta della Commissione europea

Nel febbraio 2020 la Commissione europea ha rilasciato una comunicazione inerente alla propria Data Strategy[11],congiuntamente al White Paper on Artificial Intelligence[12]. Si edificavano così le fondamenta per una regolazione comunitaria dei servizi digitali e delle nuove tecnologie. In seguito a tali iniziative, nel 2022 è stato adottato il Digital Services Act (DSA)[13],

[9] Un *flowchart* è definito come una metodologia grafica per presentare algoritmi, utilizzando simboli standardizzati per rappresentare operazioni, decisioni e flussi di controllo. Viene utilizzato per visualizzare la sequenza logica di un algoritmo, facilitando la comprensione e la comunicazione tra programmatori e analisti. Per un approfondimento, si veda N. Ensmenger, *The Multiple Meanings of a Flowchart*, in *Information & Culture*, 3, 2016, 321 ss.

[10] Cass. civ., sez. I, 10 ottobre 2023, n. 28358, Rv. 669166-01.

[11] Commissione europea, Comunicazione *A European strategy for data*, COM(2020) 66 final, 2020.

[12] Commissione europea, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final, 19 febbraio 2020.

[13] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico per i servizi digitali (Digital Services Act), in *GUUE*, L 277, 27 ottobre 2022.

il quale stabilisce regole specifiche per i servizi digitali e le piattaforme online, con l'obiettivo di regolamentare la responsabilità degli intermediari online, la trasparenza e la moderazione dei contenuti, nonché la protezione dei consumatori e la concorrenza equa nel mercato digitale. Nel medesimo periodo, il 21 aprile 2021, la Commissione europea ha presentato la proposta dell'Artificial Intelligence Act ("AI Act", già menzionato nel par. 1, che mira a regolamentare l'uso e lo sviluppo dell'IA nell'Unione europea. L'AI Act stabilisce norme specifiche per garantire la sicurezza, la trasparenza e l'etica nell'uso dell'IA, con la finalità di creare un quadro normativo completo per il mercato digitale e l'uso responsabile delle tecnologie digitali nell'Unione[14]. In risposta a queste sfide emergenti, l'AI Act rappresenta un passo fondamentale per anticipare e indirizzare le implicazioni legali e sociali di tali tecnologie, cercando di colmare il divario tra progresso tecnologico e regolamentazione attuale. L'evoluzione tecnologica, infatti, spesso supera la capacità del diritto di tenerne il passo, come dimostra l'avvento dell'intelligenza artificiale generativa e l'evoluzione del *machine learning*. Le reti neurali generative sono un tipo di reti neurali artificiali utilizzate per generare nuovi dati realistici, come immagini, suoni e testi: si tratta quindi di una tecnologia che ha applicazioni nell'arte generativa, nella grafica computerizzata, nella sintesi vocale e nella creazione di contenuti multimediali. La precisione di questi modelli è ormai migliorata al punto tale da costituire – nel caso di uso scorretto e in mala fede – un serio pericolo per la libertà, la riservatezza e la dignità dell'individuo[15].

---

[14] Come si evince dal considerando 1 del Regolamento, «*The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework, in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety and fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union («the Charter»), including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free cross-border movement of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation*»; regolamento (UE) 2024/1689 (AI Act), considerando 1.

[15] Il caso probabilmente più noto è rappresentato dai *deepfakes*, contenuti multimediali manipolati in modo intelligente per apparire autentici, pur essendo generati artificialmente. Tali tecniche, basate su reti neurali generative (*Generative Adversarial Networks* – GANs), consentono di creare immagini, video o tracce audio in cui un soggetto sembra dire o fare qualcosa che in realtà non ha mai detto o fatto. La tecnologia dei *deepfakes* presenta applicazioni potenzialmente legittime, ad esempio nei settori cinematografico e pubblicitario, ma comporta altresì gravi rischi di manipolazione, frode, diffamazione e disinformazione, incidendo sulla fiducia pubblica nelle fonti digitali e sull'integrità dell'informazione. Per un approfondimento sul fenomeno dei *deepfakes* e sulle sue implicazioni etiche, economiche e regolatorie, si veda J. Kietzmann - L. W. Lee - I. P. McCarthy - T. C. Kietzmann, *Deepfakes: Trick or Treat?*, in *Business Horizons*, 2, 2020, 135 ss. e Furizal -

Le potenzialità e gli ambiti applicativi sono stati compresi solo a posteriori, e ciò ha reso difficile per il legislatore europeo prevedere le conseguenze di tali tecnologie sulle piattaforme online. In effetti, l'applicabilità del Digital Services Act stesso a determinate fattispecie è messa in discussione dalle potenzialità di queste tecnologie[16].

Tralasciando la tempistica e la relativa adeguatezza della produzione normativa nella regolamentazione di tali fenomeni in costante e rapida evoluzione, nell'AI Act il legislatore europeo ha adottato un approccio "basato sul rischio", il medesimo già utilizzato per il GDPR, seppur con le dovute peculiarità e differenze. Il GDPR mostra una particolare responsabilizzazione del titolare del trattamento, il quale – considerando anche le importanti sanzioni previste - è sensibilizzato e indotto a considerare i reali rischi nel trattare dati personali. Il principio della *privacy by design* - consistente nell'approccio alla progettazione di sistemi e processi che incorpora la privacy e la protezione dei dati personali fin dalla progettazione - implica infatti una certa proattività da parte del titolare nel trattamento nella predisposizione di misure tecniche ed organizzative che contemperino le dovute garanzie e nel rispetto dei principi fondamentali nel trattamento dei dati personali di cui all'art. 5 GDPR[17]. Ciò implica un processo continuo di valutazione e monitoraggio del rischio per ogni attività di trattamento; solo quando ricorrono le condizioni che comportano un rischio elevato per i diritti e le libertà degli interessati si attiva la procedura prevista dall'art. 35 GDPR, che richiede la redazione di una valutazione d'impatto sulla protezione dei dati personali (DPIA)[18]. Il fulcro del principio di responsabiliz-

A. Ma'arif - H. Maghfiroh - I. Suwarno - D. Prayogi - Kariyamin - S. Lonang - A.-N. Sharkawy, *Social, legal, and ethical implications of AI-Generated deepfake pornography on digital platforms: A systematic literature review*, in *Social Sciences & Humanities Open*, 2025, 101882.
Un esempio di come un tale fenomeno possa avere impatti diretti e riflessi significativi sui diritti fondamentali e sul funzionamento della giustizia penale è offerto dallo studio sistematico condotto da M. Sandoval - M. De Almeida Vau - J. Solaas - L. Rodrigues, *Threat of Deepfakes to the Criminal Justice System: A Systematic Review*, in *Crime Science*, 2024. Gli autori evidenziano come i *deepfakes* possano compromettere la genuinità delle prove digitali, minare l'affidabilità dei processi decisionali e incidere sulla corretta amministrazione della giustizia, sollevando questioni cruciali in materia di veridicità probatoria e tutela delle garanzie processuali.

[16] M. Bassini, *Intelligenza artificiale generativa: alcune questioni problematiche*, in questa *Rivista*, 2, 2023, 391 ss.

[17] Si fa riferimento ai seguenti principi: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; regolamento (UE) 2016/679 *(General Data Protection Regulation),* art. 5.

[18] La valutazione d'impatto riveste un ruolo cruciale con riferimento ai *Big Data*: nel merito, cfr. S. Gobbato, *«Big Data» e «tutele convergenti» tra concorrenza, GDPR (General Data Protection Regulation – Regolamento generale sulla protezione dei dati) e Codice del consumo*, in questa *Rivista*, 3, 2019, 148 ss., e C. Coniglione, *L'utilizzo dei «Big Data» in ambito politico-elettorale e il loro impatto*

zazione risiede infatti nell'obbligo del titolare della corretta identificazione del rischio e delle conseguenti azioni per "mitigare" gli effetti compromettenti la *privacy* dell'individuo. La responsabilizzazione salvaguarda di fatto la produzione normativa da una precoce obsolescenza, in quanto pone a carico del titolare del trattamento l'attenta valutazione di ogni ipotetica situazione di rischio, la quale non può prescindere da un'analisi includente le modalità tecniche di processamento e conservazione dei dati, con annesse misure di sicurezza.
È quindi agevole rintracciare questo impianto giuridico nell'Artificial Intelligence Act, che attribuisce la responsabilità in prima battuta al fornitore dei sistemi di intelligenza artificiale. Il Regolamento prevede infatti una specifica classificazione dei sistemi in relazione al livello di rischio. Ciò significa che, per i c.d. "Sistemi ad Alto Rischio", il fornitore è tenuto all'adempimento di specifici obblighi, tra i quali la redazione di una documentazione di tipo tecnico completa ed informata, in grado di dimostrare il rispetto della normativa, unita ad implementazioni di sistemi che consentano una realistica valutazione del rischio derivanti dall'impiego dell'intelligenza artificiale. Si evince da ciò una prima e vera "istituzionalizzazione" del principio di trasparenza algoritmica, sulla cui traduzione legislativa ci si concentrerà nelle pagine che seguono.

4. La tutela dei diritti fondamentali nell'AI Act. Introduzione alla classificazione in base al rischio dei sistemi di intelligenza artificiale

Nel contesto dell'AI Act, l'approccio basato sul rischio - oltre alla responsabilizzazione del fornitore – include la classificazione dei sistemi di intelligenza artificiale in relazione alla potenzialità lesiva dei diritti fondamentali, tenendo in considerazione sia l'eventualità in cui il rischio abbia origine da un malfunzionamento del sistema – come nel caso dei sistemi utilizzati come componenti di sicurezza – oppure dall'uso in mala fede degli stessi, come ad esempio il furto dell'identità digitale di un individuo mediante il campionamento e la sintesi realistica della sua voce. Diversi sono pertanto gli obblighi e le garanzie del fornitore e degli utenti all'aumentare o diminuire del livello di rischio. Il Regolamento classifica i sistemi di AI in quattro fasce di rischio — inaccettabile, alto, limitato e minimo — attribuendo obblighi progressivamente più stringenti al crescere del pericolo. In particolare, il legislatore vieta gli impieghi reputati "inaccettabili", sottopone i sistemi "ad alto rischio" a un rigoroso regime di conformità, impone semplici obblighi di trasparenza per i casi di "rischio limitato" e non prevede

sulla democrazia rappresentativa, in *Nomos*, 1, 2023, 15 ss.

vincoli per le applicazioni a "rischio minimo". Sebbene il Regolamento sia già entrato in vigore, la maggior parte delle sue disposizioni si applicherà a tappe tra il 2025 e il 2026. La Commissione ha deciso di concedere un periodo relativamente lungo per permettere alle imprese e agli altri soggetti interessati di adeguarsi ai nuovi obblighi. Le normative riguardanti i sistemi AI proibiti saranno applicate dopo 6 mesi; le regole relative alle GPAI (*General Purpose AI* o intelligenza artificiale generale)[19] entreranno in vigore dopo 12 mesi, eccetto per i modelli di GPAI già disponibili sul mercato prima di tale scadenza, per i quali il termine è di 24 mesi; le disposizioni per i sistemi AI considerati ad alto rischio saranno effettive dopo 36 mesi[20]. Infine, i sistemi AI ad alto rischio già utilizzati dalle autorità pubbliche al momento dell'entrata in vigore dell'AI Act beneficeranno di un periodo di tolleranza di 48 mesi.

Passando al merito, va innanzitutto ribadito che l'inaccettabilità di alcuni sistemi implica il divieto assoluto di commercializzazione ed implementazione nella società. Dal punto di vista giuridico-costituzionale sorge dunque un primo spunto di ragionamento, circa la precisa identificazione del discrimine – talvolta sottile e delicato – in base al quale un sistema di AI viene inserito nel rischio inaccettabile piuttosto che nei sistemi ad alto rischio. Pur essendo la questione regolata nel Titolo II del Regolamento, già nella relazione introduttiva della proposta si sottolineava che l'elenco delle pratiche vietate comprende tutti i sistemi di IA il cui uso è considerato inaccettabile in quanto contrario ai valori dell'Unione[21]. Questo approccio è finalizzato a proibire pratiche contrastanti i suddetti valori, relativi al rispetto della dignità umana, della libertà, dell'uguaglianza, della democrazia e dello Stato di diritto e dei diritti fondamentali dell'Unione, compresi il

[19] Per *GPAI* si intendono quei sistemi di intelligenza artificiale aventi finalità e scopi di tipo generale, progettati per l'esecuzione di una vasta gamma di compiti anziché essere limitati a scopi specifici. Gran parte dei modelli di intelligenza artificiale generativa usufruibili dagli utenti sul web rientrano in questa categoria. Per interessanti considerazioni sulla definizione di *General Purpose Artificial Intelligence Systems* (*GPAI*), si veda General Purpose Artificial Intelligence Systems (GPAI), si veda C. I. Gutierrez - A. Aguirre - R. Uuk et al., *A Proposal for a Definition of General Purpose Artificial Intelligence Systems*, in *Digital Society*, 2, 2023, 36.

[20] Parlamento europeo, *Il Parlamento europeo approva la legge sull'intelligenza artificiale*, comunicato stampa, 13 marzo 2024, disponibile su europarl.europa.eu.

[21] Nei considerando del testo definitivo approvato dal Parlamento europeo si trovano riferimenti espliciti e dettagliati ai sistemi di intelligenza artificiale vietati dall'Unione. In particolare, il considerando 26 recita: «Per introdurre un insieme proporzionato ed efficace di norme vincolanti per i sistemi di IA, si dovrebbe seguire un approccio chiaramente definito basato sul rischio. Tale approccio dovrebbe adattare il tipo e il contenuto di tali norme all'intensità e alla portata dei rischi che i sistemi di IA possono generare. È quindi necessario vietare alcune pratiche di IA inaccettabili, stabilendo requisiti per i sistemi di IA ad alto rischio e obblighi per i relativi operatori, e stabilire obblighi di trasparenza per alcuni sistemi di IA»; regolamento (UE) 2024/1689 (AI Act), considerando 26.

diritto alla non discriminazione[22], alla protezione dei dati[23] e della vita privata e i diritti dei minori[24].

Alla base è dunque riscontrabile un'analisi "costi-benefici", un'attenta valutazione analitica del progetto, dove il "costo" è rappresentato dal rischio delle ipotetiche situazioni lesive dei diritti fondamentali che la commercializzazione e l'uso di un determinato sistema di intelligenza artificiale può comportare. Non a caso, nella relazione della proposta, − Sezione 1.1, Motivi e obiettivi della proposta − l'intelligenza artificiale è definita come «una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali»; immediatamente dopo segue il passaggio chiave giustificante l'approccio basato sui livelli di rischio: «[t]uttavia gli stessi elementi e le stesse tecniche che alimentano i benefici socio-economici dell'IA possono altresì comportare nuovi rischi o conseguenze negative per le persone fisiche o la società». La definizione e le considerazioni in merito all'intelligenza artificiale sono state poi approfondite nei considerando 4 e 5 del testo definitivo, approvato dal Parlamento europeo il 14 marzo del 2024. L'IA è infatti considerata come un importantissimo vantaggio competitivo per le imprese, nell'ottimizzazione dei processi e nell'allocazione delle risorse. Allo stesso tempo, a seconda delle circostan-

[22] Si pensi ai potenziali rischi derivanti da eventuali *bias* algoritmici dei sistemi di intelligenza artificiale implementati nel sistema giudiziario. Sebbene l'automatizzazione di determinati procedimenti possa agevolare lo svolgimento del processo, resta comunque fondamentale un'attenta analisi dell'impatto che tali implementazioni possono avere sul giusto processo e sui diritti delle parti. Sul tema, cfr. P. R. Borges Fortes, *Paths to Digital Justice: Judicial Robots, Algorithmic Decision-Making, and Due Process*, in *Asian Journal of Law and Society*, 3, 2020, 453 ss. e A. Lorusso, *Algoritmo, provvedimento amministrativo e autotutela*, in questa *Rivista*, 1, 2023, 326 ss. È altresì evidente — considerando le attuali tecnologie — l'impossibilità di concepire un sistema di intelligenza artificiale operante in un'ottica integralmente sostitutiva della figura del giudice. Tuttavia, le nuove tecnologie potrebbero incidere profondamente su alcuni aspetti del diritto, sia sostanziale sia processuale, tra cui la determinazione dell'elemento soggettivo del reato, della prova scientifica, degli *standard* probatori e del rischio di recidiva. Quest'ultimo aspetto è approfondito in G. Tuzet, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in questa *Rivista*, 1, 2020, 45 ss.

[23] Già nel 2018 la Norwegian Data Protection Authority analizzava, nel proprio report *Artificial Intelligence and Privacy*, i rischi connessi all'applicazione dell'intelligenza artificiale al trattamento e all'acquisizione di dati personali, anticipando molte delle preoccupazioni oggi affrontate dall'Artificial Intelligence Act. Per ulteriori approfondimenti, cfr. Norwegian Data Protection Authority, *Artificial Intelligence and Privacy*, in *datatilsynet.no*, 22 giugno 2018.

[24] Si tratta di una categoria particolarmente vulnerabile sul web e sui social network. L'intelligenza artificiale rappresenta, tuttavia, una grande opportunità per automatizzare la moderazione dei contenuti sulle piattaforme online. Per approfondire l'argomento e i rischi implicati, cfr. P. Dunn, *Moderazione automatizzata e discriminazione algoritmica: il caso dell'hate speech*, in *Rivista italiana di informatica e diritto*, 1, 2022, 133 ss.

ze relative alla sua specifica applicazione, sono presi seriamente in considerazione i potenziali pericoli concernenti gli interessi pubblici e i diritti fondamentali tutelati dall'Unione, includendo danni materiali, immateriali, fisici, psicologici, sociali ed economici.
A scanso di equivoci, va subito segnalato che la stragrande maggioranza degli attuali sistemi di intelligenza artificiale è riconducibile alle categorie del rischio limitato e nel rischio moderato. Per questi ultimi è previsto solamente un regime minimo "di trasparenza": ad esempio, applicazioni come *Chatbot*[25] dovrebbero riconoscere all'utente la possibilità di prendere delle decisioni informate. Fatta questa doverosa premessa e prima di trattare nel merito il tema della trasparenza algoritmica, è necessario fornire un contesto sul fulcro della tutela normativa in oggetto, ovvero la regolamentazione dei c.d. sistemi "ad alto rischio".

4.1 Una breve panoramica sui sistemi "ad alto rischio"

A differenza dei sistemi a "rischio inaccettabile", i sistemi di intelligenza artificiale ad alto rischio possono essere immessi sul mercato o messi in servizio, purché rispettino i requisiti obbligatori specificati nel Regolamento. Il fornitore è soggetto a specifici adempimenti, inerenti ad obblighi di documentazione, tracciabilità e di trasparenza, nonché ad ulteriori criteri riguardanti l'interfaccia e la sorveglianza umana, la precisione e la "robustezza" o sicurezza del sistema[26].

[25] «Sono macchine. O meglio, *chatbot*: programmi per computer in grado di "apprendere" e sviluppare una propria intelligenza, mentre dialogano con gli esseri umani. Riuscendo, almeno per qualche minuto, a spacciarsi per gente in carne e ossa. Memorizzano, cioè, parole e frasi di ogni conversazione per farne uso nelle conversazioni successive, verificandone l'effetto e affinandone di passo in passo la correttezza. Imparando dagli errori. Sono i prototipi dei personaggi virtuali che presto ci faranno da ciceroni in musei e grandi magazzini, serviranno da alter ego alle celebrità o terranno compagnia a chi è troppo solo.» P. Accolla, *La Repubblica, Affari & Finanza*, 25 settembre 2006, 25.

[26] In un'ottica di confronto, l'art. 32 del regolamento (UE) 2016/679 (*General Data Protection Regulation – GDPR*) stabilisce gli obblighi di sicurezza che i titolari e i responsabili del trattamento devono rispettare per garantire un livello di protezione adeguato al rischio connesso ai dati personali trattati. Tali obblighi comprendono la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la possibilità di ripristinare tempestivamente l'accesso ai dati in caso di incidente fisico o tecnico, nonché l'implementazione di un processo di verifica e valutazione periodica dell'efficacia delle misure adottate. Inoltre, il titolare e il responsabile del trattamento devono tener conto della natura, dell'ambito, del contesto e delle finalità del trattamento (regolamento (UE) 2016/679, art. 32). Sul tema, cfr. J. S. Vanegas, *La violazione dei requisiti di sicurezza informatica di cui all'art. 32 del GDPR*, in *Rivista italiana di informatica e diritto*, 2, 2020, 5 ss. Nel regolamento (UE) 2024/1689 (AI Act), l'art. 15 introduce una prospettiva complementare, definendo

Per stabilire con esattezza quando un sistema di intelligenza artificiale debba essere classificato "ad alto rischio" ai sensi dell'AI Act occorre partire dall'art. 6, par. 2, che subordina tale qualifica alla compresenza di due elementi: da un lato il sistema deve costituire o integrare un "componente di sicurezza" di un prodotto — oppure presentarsi esso stesso come prodotto — disciplinato da una delle normative di armonizzazione dell'Unione richiamate nell'Allegato I; dall'altro lo stesso prodotto, o la IA venduta come prodotto autonomo, deve superare una valutazione di conformità svolta da un organismo terzo prima della sua immissione sul mercato o messa in servizio. Ne sono esempio i sensori in grado di rilevare la presenza umana o i pulsanti di arresto d'emergenza governati da logiche di IA. La nozione di "componente di sicurezza" è definita dall'art. 2, par. 3, della direttiva 2006/42/CE come quell'elemento commercializzato separatamente, destinato a una funzione protettiva, il cui guasto può compromettere la sicurezza delle persone e che non è essenziale al funzionamento primario della macchina, potendo essere sostituito da componenti equivalenti. A questi criteri l'art. 6 affianca il rinvio all'Allegato III, che individua otto ambiti di utilizzo particolarmente sensibili — biometria e identificazione, infrastrutture critiche, istruzione e formazione, occupazione e gestione delle risorse umane, accesso a servizi essenziali, applicazione della legge, migrazione e controllo delle frontiere, giustizia e processi democratici — all'interno dei quali un sistema di IA è qualificato "ad alto rischio" a prescindere dal collegamento con un prodotto fisico, salvo prova dell'assenza di un rischio significativo per la salute, la sicurezza o i diritti fondamentali. Più nel dettaglio, rientrano tra le categorie di cui all'Allegato III i sistemi di categorizzazione e identificazione biometrica delle persone fisiche; i sistemi utilizzati come componenti di sicurezza nella gestione del traffico stradale e nella fornitura di servizi essenziali; quelli impiegati per determinare l'accesso o l'assegnazione a istituti scolastici o percorsi di formazione e per valutare le prestazioni degli studenti; le soluzioni adottate nei processi di assunzione o selezione del personale; i sistemi utilizzati da autorità pubbliche per valutare l'ammissibilità a prestazioni o servizi di assistenza; nonché quelli impiegati nella gestione della migrazione, dell'asilo e del controllo delle frontiere. Analizzando tale classificazione, molto spesso si identifica un elevato livello di rischio in sistemi aventi funzionalità valutative degli in-

requisiti di *cybersecurity* e di robustezza per i sistemi di intelligenza artificiale, in particolare quelli ad alto rischio. Il legislatore europeo sottolinea che «la robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di *backup* o *fail-safe*» (regolamento (UE) 2024/1689 (AI Act), art. 15). Si delinea, dunque, un duplice livello di garanzia: da un lato, la tutela della sicurezza dei dati personali, che costituisce il fulcro dell'art. 32 GDPR; dall'altro, la sicurezza intrinseca e la resilienza operativa dei sistemi di intelligenza artificiale, vero e proprio pilastro tecnico-normativo dell'*AI Act*.

dividui[27] riguardo a temi più o meno sensibili[28]. L'oggetto della valutazione è infatti correlato ai diritti fondamentali dell'uomo – prima fra tutti la dignità umana, sancita dall'art. 1 della Carta dei Diritti Fondamentali dell'Unione europea – ed ogni restrizione imposta dalla normativa è a garanzia degli stessi. Rispetto alla proposta, il testo definitivo del Regolamento - all'art. 6, par. 3 - specifica che un sistema di IA non può essere considerato ad alto rischio se non presenta un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali delle persone fisiche, anche non influenzando materialmente l'esito del processo decisionale.
Approfondendo opportunamente le considerazioni di cui sopra, se il sistema di IA è progettato per svolgere compiti procedurali molto limitati[29], non viene classificato come ad alto rischio. Questo tipo di IA ha scopi ben definiti e non è destinato a eseguire valutazioni ampie o critiche. Un altro caso in cui un sistema di IA non è visto come ad alto rischio riguarda il suo uso per rilevare modelli decisionali o deviazioni da questi[30]. Tali sistemi

[27] Così come esistono i *bias* cognitivi propri dell'essere umano, per implicazione logica si pone anche il problema del *bias* algoritmico, poiché gli algoritmi vengono addestrati su dati che riflettono l'interpretazione umana della realtà. Per un maggiore approfondimento sull'elevato rischio di discriminazione, cfr. S. Tommasi, *Algoritmi e nuove forme di discriminazione: uno sguardo al diritto europeo*, in *Revista de Direito Brasileira*, 10, 2020, 112 ss.

[28] Basti pensare al potenziale impatto dei sistemi di riconoscimento facciale basati su intelligenza artificiale utilizzati dalle autorità pubbliche. Sul tema si è già espressa l'Alta Corte di giustizia nel caso *R (Bridges) v. The Chief Constable of South Wales Police*. Per un'analisi ampia e approfondita del caso, cfr. A. Pin, *There Is No «Silver Bullet»: The Artificial Face Recognition's First Judicial Scrutiny*, in *DPCE Online,* 4, 2019, 3075 ss.

[29] Si pensi, ad esempio, a un sistema di intelligenza artificiale utilizzato da un museo per fornire suggerimenti personalizzati ai visitatori in base alle opere già visualizzate o ai percorsi scelti all'interno dell'edificio. In tal caso, il sistema elabora informazioni di carattere contestuale, ma non adotta decisioni autonome né produce effetti giuridici o significativi sulla persona. Tale applicazione, avente finalità puramente informative e di supporto all'esperienza utente, non rientra tra i sistemi ad alto rischio ai sensi dell'art. 6 dell'*AI Act*, poiché non incide sui diritti fondamentali né comporta rischi di discriminazione o danni materiali. È tuttavia opportuno evidenziare che la valutazione del rischio varia in funzione del contesto e dell'utilizzo concreto del sistema di intelligenza artificiale, potendo mutare al variare delle finalità, del tipo di dati trattati o del grado di autonomia decisionale. Sulla gestione e valutazione del rischio nel quadro dell'*AI Act*, si veda J. Schuett, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2, 2023, 367 ss.

[30] Un esempio di tale sistema è uno strumento di IA che, dato un certo modello di valutazione (*grading pattern*) di un insegnante, può essere utilizzato per verificare *ex post* se l'insegnante possa aver deviato da tale modello, segnalando potenziali incongruenze o anomalie. In questo caso, il sistema agisce come un meccanismo di *flagging* che non prende la decisione finale, ma fornisce *input* per una successiva revisione umana. Un'interessante prospettiva sull'utilizzo dell'intelligenza artificiale nel contesto educativo è offerta da C. Kooli e N. Yusuf, i quali analizzano come i *Large Language Models* (*LLM*), e in particolare *ChatGPT*, possano contribuire a trasformare le modalità di valutazione scolastica, migliorandone l'efficienza, la coerenza

analizzano le decisioni passate per identificare consistenze o discrepanze, ma non sostituiscono il giudizio umano. Sono strumenti di supporto che necessitano di una revisione umana per garantire che le valutazioni siano corrette e appropriate. Questi sistemi preparano il materiale informativo necessario per decisioni importanti, agendo come un passaggio preliminare nel processo decisionale più ampio.

Rispetto alla proposta è intercorsa dunque una notevole evoluzione circa le modalità di classificazione dei sistemi: l'alto rischio non dipende soltanto dall'ambito di applicazione del sistema, bensì dalla funzione decisiva dell'intelligenza artificiale nel processo decisionale e nella sua potenziale capacità di causare danni significativi autonomamente.

L'obiettivo del Regolamento rimane comunque la responsabilizzazione dei fornitori, ponendo a loro carico precisi obblighi e procedure nello sviluppo e nella commercializzazione di intelligenze artificiali. Va tuttavia rilevato che l'individuazione di ipotesi per le quali un fornitore possa essere ritenuto responsabile degli effettivi risultati ottenuti dall'IA è operazione indubbiamente complessa; ciò in quanto il medesimo fornitore può non avere contezza dello scopo effettivo dell'utilizzo, né essere in grado di fornire un ragionevole e provato riscontro degli effetti a lungo termine al momento dell'immissione[31]. Sul tema risulta cruciale la figura del *deployer,* che verrà debitamente approfondita nel paragrafo seguente.

Esposte – seppur sommariamente – le ragioni e i criteri alla base delle suddette classificazioni, è agevole comprendere che la previsione di "requisiti obbligatori" in capo ai fornitori[32] o *providers* nella fase di progettazione e sviluppo, uniti ad una stringente valutazione di conformità - da effettuare *ex ante,* prima della commercializzazione - rappresentano la tutela sostanziale del Regolamento.

---

e la trasparenza. Gli autori mostrano come l'IA possa essere impiegata per supportare la correzione automatica e l'analisi qualitativa delle prove, mantenendo un ruolo complementare rispetto al giudizio umano e promuovendo una didattica più equa e personalizzata. Per un approfondimento, si veda C. Kooli - N. Yusuf, *Transforming Educational Assessment: Insights into the Use of ChatGPT and Large Language Models in Grading*, in *International Journal of Human-Computer Interaction*, 2024, 3388 ss.

[31] M. R. Carbone, *AI Act. Come procede il regolamento UE sull'intelligenza artificiale: il nuovo testo*, in *agendadigitale.eu*, 2 settembre 2022.

[32] Nel contesto dell'*Artificial Intelligence Act*, il «fornitore» (*provider*) è definito come la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che sviluppa un sistema di intelligenza artificiale — o ne fa sviluppare uno — e lo immette sul mercato o lo mette in servizio sotto il proprio nome o marchio, sia a titolo oneroso sia gratuito (regolamento (UE) 2024/1689 (AI Act), art. 3, punto 3). Tale definizione non comprende automaticamente l'importatore né il distributore, individuati separatamente ai punti 6 e 7 dello stesso articolo, sebbene tali soggetti possano, in determinate circostanze, assumere alcuni obblighi propri del fornitore.

5. La tutela sostanziale dell'AI Act. Il ruolo dei *providers* e dei *deployers*

Prima di approfondire la rilevanza del concetto di trasparenza algoritmica nella compliance all'Artificial Intelligence Act, è opportuno fare chiarezza sui soggetti definiti dal Regolamento. Analogamente ai soggetti definiti dal GDPR, come ad esempio il "titolare del trattamento" ed il "responsabile del trattamento", è necessario evidenziare la differenza tra il *provider*, ossia il fornitore, e il *deployer*. Per fornitore – ai sensi dell'art. 3, par. 3 del Titolo I del Regolamento – si intende quell'entità che progetta, sviluppa o produce sistemi di AI per uso diretto o per distribuzione sul mercato europeo, a titolo gratuito o a pagamento. Il *deployer* è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza il sistema di IA sotto la propria autorità, ad eccezione del caso in cui il sistema venga utilizzato nel corso di un'attività personale non professionale. Il regolamento pone a carico del *deployer* specifiche responsabilità, che completano e specificano quelle dei fornitori. Già il considerando 91 dell'AI Act chiarisce che, per i sistemi di intelligenza artificiale classificati "ad alto rischio", la conformità deve estendersi oltre la fase di progettazione e includere l'adozione di misure tecniche e organizzative capaci, da un lato, di assicurare l'uso del sistema in linea con le istruzioni del fornitore e, dall'altro, di consentire un monitoraggio costante delle prestazioni lungo l'intero ciclo di vita. Questa esigenza si traduce, all'art. 12, nell'obbligo di registrare in modo automatico e sistematico i c.d. *log*, vale a dire i dati di tracciamento degli eventi rilevanti, i quali devono essere accurati, affidabili e prontamente disponibili a fini di *audit* e di indagine *post-market*. La continuità di tale tracciabilità garantisce che eventuali anomalie o incidenti possano essere identificati e gestiti anche dopo l'immissione del prodotto sul mercato, inserendosi nel più ampio sistema di gestione del rischio delineato dall'art. 9.

A ciò si affianca l'art. 26, che impone ai *deployer* di assicurare che il personale incaricato della supervisione e dell'utilizzo del sistema disponga di un adeguato livello di alfabetizzazione in materia di IA, nonché della formazione e dell'autorità necessarie per intervenire ove occorra. L'efficacia di tutte queste cautele risulterebbe, tuttavia, compromessa se il fornitore non rispettasse i doveri di trasparenza sanciti dall'art. 13: istruzioni d'uso chiare, complete e comprensibili rappresentano infatti la condizione imprescindibile affinché i log siano interpretati correttamente, il monitoraggio sia significativo e le competenze degli operatori possano dispiegarsi in modo effettivo. In sintesi, il Regolamento costruisce un circuito virtuoso tra tracciabilità tecnica, controllo umano informato e trasparenza documentale, destinato a preservare la sicurezza e l'affidabilità dei sistemi di IA ad alto rischio per tutta la loro vita operativa.

L'art. 27 dell'AI Act attribuisce ai *deployer* di sistemi di IA ad alto rischio l'obbligo di redigere, prima della messa in uso, una Fundamental Rights Impact Assessment (FRIA) volta a valutare le ripercussioni che l'impiego del sistema può produrre sui diritti fondamentali delle persone coinvolte. Tale valutazione deve descrivere in modo puntuale: i processi operativi in cui il sistema sarà impiegato, il periodo e la frequenza di utilizzo, le categorie di individui potenzialmente interessate, i rischi specifici connessi all'applicazione concreta, le misure di supervisione umana previste nonché le azioni da intraprendere qualora tali rischi dovessero materializzarsi. L'obbligo riguarda i soggetti di diritto pubblico e le entità private che erogano servizi di pubblico interesse, nonché i *deployer* dei sistemi rientranti nei punti 5-b e 5-c dell'Allegato III, con la sola esclusione dei sistemi destinati alle infrastrutture critiche di cui al punto 2 dello stesso allegato. Il legislatore prevede che i risultati della FRIA siano notificati all'autorità di sorveglianza del mercato utilizzando il modello standardizzato che sarà messo a disposizione dall'AI Office. Inoltre, qualora una parte delle analisi sia già coperta da una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 GDPR, la FRIA deve integrarla, evitando duplicazioni e garantendo coerenza metodologica. Questa previsione, perfettamente in linea con il principio di accountability mutuato dal GDPR, responsabilizza il *deployer* sin dalle prime fasi di progetto, imponendogli di prevenire e mitigare in modo ragionevole i potenziali pregiudizi[33] per la salute, la sicurezza e le libertà fondamentali connessi all'impiego del sistema di IA

I fornitori sono infatti tenuti a redigere una documentazione di tipo tecnico "completa ed informata", in grado di dimostrare il rispetto della normativa, unita ad implementazioni di sistemi che consentano la predisposizione di una realistica valutazione del rischio derivanti dall'impiego dell'intelligenza artificiale. Sono inoltre previsti obblighi di tracciabilità delle decisioni dei sistemi ad alto rischio, provvedendo a creare sistemi di registrazione automatica dei log, cioè una sorta di "scatola nera" funzionale alla ricostruzione accurata degli eventi caratterizzanti un determinato procedimento decisionale.

6. Il primo livello di trasparenza

Tali imposizioni sono strettamente collegate al principio di trasparenza, che vincola il fornitore a predisporre informazioni chiare, precise e com-

[33] Parallelismo altresì approfondito in A. Alaimo, *Il regolamento sull'intelligenza artificiale, dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico*, in *federalismi.it*, 25, 2023, 136 ss.

prensibili[34]. Nonostante l'assonanza semantica, va precisato che si tratta qui di un principio diverso da quello sancito dal GDPR in merito alla trasparenza del trattamento dei dati personali[35] , dato che nella normativa in esame si fa riferimento ad un concetto avanzato di trasparenza algoritmica, strettamente funzionale all'autonomia e al controllo sulle modalità operative dei sistemi di AI. Ciò non significa la divulgazione del codice sorgente, bensì «la riduzione/eliminazione dell'asimmetria informativa finalizzata ad acquisire la capacità di descrivere, ispezionare e riprodurre correttamente i meccanismi attraverso cui i sistemi di intelligenza artificiale assumono decisioni ed imparano ad adattarsi ai loro ambienti»[36]. Comprendere a fondo la logica decisionale che governa l'algoritmo—nonché le modalità con cui il flusso di dati viene raccolto, preprocessato e alimentato nel modello—è condizione indispensabile per individuare l'origine di eventuali malfunzionamenti, ricostruirne la ratio causale e interrompere il rischio di reiterazione dell'errore. In questa prospettiva, l'art. 13 dell'AI Act impone al fornitore un livello di trasparenza tale da mettere il *deployer* in grado di decodificare le dinamiche interne del sistema, interpretarne correttamente gli output e applicare le necessarie misure correttive; solo così l'utilizzatore può monitorare il funzionamento dell'IA in modo informato, prevenendo derive sistemiche e garantendo che l'impiego del modello resti coerente con i requisiti di affidabilità e tutela dei diritti fondamentali che permeano l'intero impianto regolatorio. Fondamentale risulta il par. 3 di tale art., contenente un'accurata descrizione del contenuto delle istruzioni per l'uso che il fornitore deve fornire al *deployer*. In primo luogo, è necessario includere l'identità e i dati di contatto del fornitore e, se presente, del suo rappresentante autorizzato. Le istruzioni devono poi descrivere in modo accurato le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA. Il contenuto delle istruzioni deve chiarire lo scopo specifico del sistema, il livello di accuratezza atteso e i requisiti di robustezza e sicurezza informatica previsti dall'art. 15. Devono inoltre essere richiamate tutte le condizioni note in grado di incidere su tali parametri, nonché gli scenari di uso improprio ragionevolmente prevedibili che potrebbero generare rischi. Laddove pertinente, occorre spiegare la capacità del modello di fornire spiegazioni comprensibili dei propri output e precisare le prestazioni rilevate in relazione ai gruppi di destinatari. Risulta quindi necessario

[34] Si fa riferimento a un linguaggio rivolto all'utente medio che si interfaccia e utilizza il sistema di intelligenza artificiale, evitando il più possibile il linguaggio tecnico o strettamente comprensibile solo da esperti del settore.

[35] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, 27 aprile 2016 (GDPR), art. 12.

[36] M. Bonafè - C. Trevisi, *Intelligenza artificiale, l'algoritmo trasparente: un rebus ancora da sciogliere*, in *agendadigitale.eu*, 15 luglio 2019.

descrivere in dettaglio le caratteristiche dei dati di input nonché dei set di addestramento, validazione e test impiegati, sempre in rapporto alla finalità funzionale dell'IA.
Le istruzioni devono poi menzionare ogni modifica predeterminata delle prestazioni impostata dal fornitore in sede di valutazione di conformità, a garanzia di trasparenza e per consentire agli utenti di comprendere le basi dell'approvazione del sistema. Nel medesimo documento vanno illustrate le misure di supervisione umana previste dall'art. 14 e le soluzioni tecniche predisposte per facilitare una corretta interpretazione dei risultati. Non meno rilevante è l'indicazione delle risorse computazionali e hardware necessarie, della durata di vita prevista e degli interventi di manutenzione (inclusi gli aggiornamenti software) necessari al regolare funzionamento. Infine, qualora applicabile, occorre descrivere i meccanismi interni che consentono ai *deployer* di raccogliere, archiviare e interpretare correttamente i log ai sensi dell'art. 12, affinché tutte le operazioni siano tracciabili e sottoposte a verifiche di sicurezza e conformità.
Quanto appena descritto - per mera categorizzazione di tipo dottrinale - può intendersi come il primo livello di trasparenza, ovvero la trasparenza garantita dal *provider* affinché il *deployer* possa agire in conformità con il Regolamento, in accordo con quanto ampiamente descritto dal considerando 71[37]. Rimane ora da analizzare il secondo livello, ossia la trasparenza

[37] Il considerando 71 del regolamento (UE) 2024/1689 (AI Act) richiama l'attenzione su uno dei principi cardine della disciplina: la trasparenza, quale condizione preliminare per l'immissione sul mercato dei sistemi di intelligenza artificiale ad alto rischio. Il legislatore europeo riconosce che la complessità e l'opacità tecnologica possono ostacolare la comprensione effettiva del funzionamento di tali sistemi da parte dei loro utilizzatori — i cosiddetti *deployer* — e, di conseguenza, compromettere un uso consapevole e responsabile degli stessi. Per mitigare tale rischio, il Regolamento impone ai fornitori di progettare sistemi di intelligenza artificiale che risultino effettivamente intellegibili: chi li utilizza deve poter comprendere, in termini pratici, le modalità di elaborazione dei dati da parte dell'algoritmo, i risultati attesi e i limiti prestazionali entro cui il sistema opera. Questa esigenza di comprensione si traduce in un articolato obbligo informativo. Ogni sistema ad alto rischio deve essere accompagnato da istruzioni d'uso complete, redatte in una lingua comprensibile per il pubblico di riferimento, contenenti la descrizione delle caratteristiche tecniche, delle capacità e dei limiti del sistema, nonché degli scenari di utilizzo previsti e di quelli espressamente vietati. Devono inoltre essere indicate le condizioni — note o ragionevolmente prevedibili — in cui il comportamento del sistema può variare, in particolare quando un intervento del *deployer* possa incidere sulle prestazioni. Le istruzioni devono altresì specificare eventuali modifiche di *performance* già valutate in sede di procedura di conformità e le misure di supervisione umana necessarie per interpretare correttamente gli *output*. A fini di effettiva fruibilità, il considerando invita a integrare tali informazioni con esempi illustrativi: casi d'uso, limiti operativi e contesti nei quali il sistema di intelligenza artificiale non dovrebbe essere applicato. L'obiettivo è duplice: da un lato, agevolare il *deployer* nella selezione e nell'impiego del sistema più idoneo alle proprie esigenze e, dall'altro, assicurare un utilizzo conforme ai principi di sicurezza, tutela della salute e rispetto dei diritti fondamentali. In ultima

accordata all'utente finale interessato, ultimo beneficiario dell'operatività delle intelligenze artificiali.

7. La tutela degli "interessati", il secondo livello di trasparenza e gli obblighi dei *providers* e dei *deployers* nei confronti degli utenti finali

Sebbene nell'art. 3 del Titolo I del Regolamento non vi sia alcun riferimento ai soggetti interessati, intesi come "beneficiari" dei servizi offerti con l'ausilio o il supporto di intelligenze artificiali, possiamo inquadrare delle particolari categorie di interessati analizzando i considerando del Regolamento. Il considerando 51 analizza l'uso dell'IA nei delicati processi che regolano l'accesso a prestazioni essenziali, pubbliche o private. Gli interessati sono i cittadini che ne fanno richiesta; se un algoritmo decide in merito alla concessione, riduzione o revoca di tali prestazioni, si applica l'art. 22 GDPR. L'interessato deve essere dunque informato dal soggetto erogante il servizio dell'eventuale decisione basata su procedimento decisionale automatizzato, affinché sia possibile l'esercizio di tutti i diritti riconosciuti, inclusa la richiesta di informazioni aggiuntive. Ulteriori obblighi in capo ai «fornitori» - questa volta da intendersi come l'insieme di *providers* e *deployers* - nei confronti delle persone fisiche, sono sanciti nel Titolo IV del Regolamento «*Transparency obligations for providers and deployers of certain AI Systems*» all'art. 50. Il primo paragrafo sancisce un preciso obbligo per i fornitori che sviluppano sistemi di AI destinati all'interazione diretta con persone fisiche. Tali sistemi devono essere progettati e sviluppati in modo tale che le persone siano informate dell'interazione con un sistema di AI, a meno che ciò non sia ovvio data la situazione e il contesto di utilizzo[38]. L'obbligo di maggiore rilevanza – a tutela della libertà di espressione e di informazione sancita dall'art. 11 della Carta dei diritti fondamentali dell'Unione europea– è relativo alla necessità di informazione nel caso di generazione di contenuti *deep fakes* con sistemi di intelligenza artificiale. I *deployers* che generano o manipolano contenuti visivi o audio raffiguranti individui o situazioni, avendo come risultato un prodotto difficilmente distinguibile dalla realtà, devono rivelare che il contenuto è stato generato o manipolato

analisi, la trasparenza richiesta dal considerando 71 non si riduce a un mero adempimento documentale, ma rappresenta uno strumento funzionale alla più ampia *accountability* che permea l'intero impianto regolatorio dell'*Artificial Intelligence Act* (considerando 71).

[38] A titolo di esempio, supponiamo che un'azienda stia sviluppando un assistente virtuale basato su intelligenza artificiale per l'assistenza clienti in un sito web di e-commerce. L'azienda fornitrice avrà l'obbligo di progettare e sviluppare questo sistema in modo che i clienti siano informati dell'interazione con un sistema di AI, a meno che ciò non risulti ovvio data la situazione e il contesto di utilizzo.

artificialmente. Lo stesso obbligo circa l'informazione di un contenuto generato artificialmente si applica a chi genera e pubblica testi – aventi rilevanza di pubblico interesse, come ad esempio un articolo di cronaca – a meno che il testo non sia stato sottoposto a revisione umana. Inoltre - nel caso in cui servissero ulteriori approfondimenti circa la natura artificiale o meno di un contenuto, come ad esempio in contesti giudiziari – il Regolamento pone a carico dei fornitori l'obbligo di garantire che qualsiasi contenuto generato da sistemi di intelligenza artificiale abbia un formato *machine-readable*[39] e di conseguenza identificabile inequivocabilmente come artificiale. Infine, il considerando 91 attribuisce ai *deployers* il ruolo fondamentale di informare le «persone fisiche soggette all'uso del sistema di IA ad alto rischio», rendendole opportunamente edotte circa lo scopo previsto, il tipo di decisioni prese e il diritto a ricevere tutte le informazioni necessarie ai sensi del Regolamento.

8. Interpretabilità e spiegabilità come presupposti della trasparenza algoritmica[40]

Per garantire un'efficace trasparenza algoritmica, è fondamentale distinguere e integrare due concetti chiave: l'interpretabilità e la spiegabilità. L'interpretabilità[41] si riferisce alla capacità di un esperto di comprendere il funzionamento interno di un sistema algoritmico, analizzando come i dati vengono elaborati e come le decisioni vengono generate. Questo aspetto è cruciale per i tecnici e gli sviluppatori, che devono poter «aprire la black box»[42] per verificare la correttezza logica e funzionale del sistema, ad esempio tramite l'analisi dei pesi dei modelli o la visualizzazione delle attivazioni delle reti

[39] Un formato *machine-readable* (leggibile dalle macchine) si riferisce a qualsiasi formato di dati che può essere facilmente elaborato da un computer. D. Amadi - S. Kiwuwa-Muyingo - T. Bhattacharjee - A. Taylor - A. Kiragga - M. Ochola - C. Kanjala - A. Gregory - K. Tomlin - J. Todd - J. Greenfield, *Making Metadata Machine-Readable as the First Step to Providing Findable, Accessible, Interoperable, and Reusable Population Health Data:Framework Development and Implementation Study*, in *Online Journal of Public Health Informatics*, 2024, e56237., costituisce un ottimo esempio applicativo del concetto di *machine-readable*, poiché dimostra come la strutturazione e standardizzazione dei metadati nel contesto sanitario possano rendere i dati realmente *Findable, Accessible, Interoperable and Reusable* (*FAIR*), migliorandone la qualità, l'integrazione e la riusabilità nei sistemi di salute pubblica.

[40] Si ringrazia il Dott. Giorgio Presepio per la collaborazione nella redazione e revisione del presente paragrafo.

[41] F. Doshi-Velez - B. Kim, *Towards a Rigorous Science of Interpretable Machine Learning*, in *arXiv*, 2017, 1702.08608.

[42] F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (MA), 2015.

neurali per comprendere quali caratteristiche sono considerate rilevanti. La spiegabilità[43], d'altro canto, riguarda la possibilità per un utente non esperto – come un cittadino, un giudice o un consumatore – di comprendere le ragioni alla base di una specifica decisione prodotta da un algoritmo. La spiegabilità si concentra sul "perché" una decisione è stata presa, rendendola intelligibile a un pubblico non tecnico, ad esempio spiegando che "la tua richiesta di prestito è stata rifiutata perché il tuo reddito è inferiore alla soglia X e il tuo rapporto debito/reddito supera Y".

Questa distinzione evidenzia un doppio livello di comprensibilità necessario per la piena realizzazione della trasparenza. A un livello tecnico, la comprensione è rivolta a sviluppatori, responsabili della protezione dei dati (DPO) e revisori (audit), che necessitano di una visione approfondita del modello per assicurarne la correttezza, l'affidabilità e la conformità normativa. Questo si traduce nella necessità di strumenti e tecniche che permettano di analizzare la logica interna del sistema e i suoi *bias* intrinseci. A un livello sociale, la comprensione è destinata a coloro che sono direttamente influenzati dalle decisioni algoritmiche, i quali devono poter capire il perché di una determinata decisione per poter esercitare i propri diritti e per mantenere la fiducia nel sistema. Come sottolineato in letteratura, la fiducia pubblica nell'IA dipende dalla sua capacità di essere spiegata in modo significativo agli utenti finali.

Esiste una chiara connessione normativa tra questi concetti e il quadro giuridico europeo. L'art. 13 dell'AI Act, ad esempio, impone al fornitore di un sistema di intelligenza artificiale di fornire al *deployer* le istruzioni necessarie affinché quest'ultimo possa comprendere e utilizzare correttamente il sistema. Questo requisito mira a garantire un'adeguata interpretabilità a livello tecnico, permettendo al *deployer* di adempiere ai propri obblighi di supervisione e monitoraggio, inclusa una valutazione d'impatto sui diritti fondamentali (FRIA) efficace.

Parallelamente, l'art. 22 GDPR, applicabile alle decisioni basate unicamente sul trattamento automatizzato, inclusa la profilazione, che producano effetti giuridici significativi per l'individuo, impone l'obbligo di fornire «informazioni significative in merito alla logica utilizzata». Questo requisito si traduce nell'esigenza pratica della spiegabilità, poiché le informazioni devono essere presentate in termini comprensibili all'interessato.

Il quadro normativo europeo, pertanto, riconosce implicitamente l'importanza di interpretabilità e spiegabilità. Tali obblighi, già trattati nei paragrafi precedenti, trovano qui conferma nella necessità di garantire autonomia e consapevolezza all'utente. Il considerando 71 dell'AI Act rafforza

[43] M. Ribeiro - S. Singh - C. Guestrin, *Nothing Else Matters: Model-Agnostic Explanations by Identifying Prediction Invariance*, in *arXiv*, 2016, 1611.05817.

ulteriormente questa necessità, richiamando esplicitamente l'importanza di fornire una spiegazione comprensibile degli *output* dei sistemi di intelligenza artificiale agli utenti finali. In particolare, per i sistemi ad alto rischio, l'obbligo di rendere intellegibile la logica del processo decisionale è essenziale per consentire agli individui di comprendere come vengono prese le decisioni che li riguardano e di esercitare i propri diritti, come il diritto di ottenere un intervento umano o di contestare la decisione. La capacità di comprendere la "logica utilizzata" è dunque un requisito fondamentale per la validità del consenso e per l'esercizio dell'autodeterminazione, specialmente in contesti che possono influenzare diritti fondamentali. Garantire interpretabilità e spiegabilità non è solo un obbligo legale, ma anche un imperativo etico per costruire sistemi di IA che siano equi, responsabili e affidabili.

Nonostante i progressi normativi, i modelli attuali di intelligenza artificiale presentano dei limiti intrinseci. Molti algoritmi, in particolare le reti neurali profonde e i modelli generativi, operano come "scatole nere" (*black-box*), rendendo difficile una spiegazione diretta e trasparente del loro funzionamento interno. Questa opacità, ampiamente discussa nella letteratura scientifica[44], deriva dalla loro complessità e dal modo in cui apprendono da grandi quantità di dati. Spesso, esiste un trade-off tra l'accuratezza di un modello e la sua interpretabilità: un sistema altamente preciso potrebbe essere intrinsecamente meno comprensibile, e viceversa. Questo *trade-off* rappresenta una delle sfide più significative nello sviluppo di sistemi XAI[45]. Questa sfida tecnica ha significative implicazioni giuridiche. La spiegabilità diventa una vera e propria condizione di legittimità per l'automazione decisionale. In assenza di una spiegazione intelligibile, diviene estremamente difficile per gli individui esercitare pienamente i loro diritti, come il dirit-

[44] Per una rassegna sistematica sullo stato dell'arte dell'*Explainable Artificial Intelligence* (*XAI*) (v. nota n. 43), con particolare attenzione ai metodi di interpretazione dei modelli *black-box*, alle sfide di trasparenza e ai risvolti etico-normativi in ambiti critici come sanità, finanza e trasporti autonomi, si veda V. Hassija - V. Chamola - A. Mahapatra - A. Singal - D. Goel - K. Huang - S. Scardapane - I. Spinelli - M. Mahmud - A. Hussain, *Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence*, in *Cognitive Computation*, 1, 2023, 45 ss. Questo problema è particolarmente evidente in ambito sanitario; per una panoramica completa, si veda Z. Salahuddin-H. C. Woodruff-A. Chatterjee-P. Lambin, *Transparency of Deep Neural Networks for Medical Image Analysis: A Review of Interpretability Methods*, in *Computers in Biology and Medicine*, 2022, 105919.

[45] Un sistema *XAI* è un sistema di intelligenza artificiale capace di fornire spiegazioni sulle proprie decisioni o previsioni, offrendo agli utenti una comprensione del comportamento del modello e delle influenze che portano a un certo *output*. Si veda in merito A. Barredo Arrieta - N. Díaz-Rodríguez - J. Del Ser - A. Bennetot - S. Tabik - A. Barbado - S. Garcia - S. Gil-Lopez - D. Molina - R. Benjamins - R. Chatila - F. Herrera, *Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI*, in *Information Fusion*, 2020, 82 ss.

to di accesso ai dati personali, il diritto di opposizione a un trattamento automatizzato o il diritto di presentare un reclamo. L'introduzione di un sistema di "scatola nera" (questa volta intesa come un sistema di registrazione automatica dei *log*) funzionale alla ricostruzione accurata degli eventi, come previsto dall'art. 12 dell'AI Act per i sistemi ad alto rischio, mira proprio a colmare questa lacuna di tracciabilità e spiegabilità.
Le prospettive future in questo campo sono strettamente legate allo sviluppo della cosiddetta "XAI" (*Explainable AI*)[46], un'area di ricerca che si propone di sviluppare tecniche e metodologie per rendere i sistemi di intelligenza artificiale più trasparenti e comprensibili. La *XAI* rappresenta non solo una sfida tecnica, ma anche giuridica, poiché le soluzioni sviluppate dovranno essere in grado di soddisfare i requisiti normativi di trasparenza e spiegabilità imposti dal GDPR e dall'AI Act. Le soluzioni *XAI* non mirano solo a spiegare il «perché» di una decisione, ma anche a fornire controfattuali (cosa sarebbe dovuto cambiare perché la decisione fosse diversa) o a identificare i fattori più influenti in una decisione, offrendo così maggiore controllo e comprensione all'utente. A tal riguardo, la standardizzazione internazionale, come quella definita dalla norma ISO/IEC TR 24028[47] (*Trustworthiness in AI*), identifica la spiegabilità come una componente chiave dell'affidabilità dei sistemi di intelligenza artificiale, riconoscendone l'importanza per la fiducia del pubblico e la conformità legale. L'evoluzione del concetto di trasparenza algoritmica, dal GDPR all'AI Act, riflette la crescente consapevolezza dell'importanza di garantire agli individui non solo la protezione dei loro dati, ma anche la capacità di comprendere e controllare le decisioni automatizzate che li riguardano, salvaguardando così la loro autodeterminazione e i diritti fondamentali.

9. Conclusioni

Il significato sostanziale della trasparenza algoritmica si è progressivamente ampliato in parallelo all'evoluzione tecnologica e alla crescente incidenza che quest'ultima esercita sull'effettività e sulla tutela dei diritti fondamentali della persona. Già nell'era della profilazione tradizionale la piena consapevolezza delle conseguenze dei processi decisionali automatizzati costituiva un requisito imprescindibile per la tutela della privacy e, soprattutto, dell'autodeterminazione individuale. Nel 2016 il giornalista Steve

[46] A. Adadi - M. Berrada, *Peeking Inside the Black Box: A Survey on Explainable Artificial Intelligence (XAI)*, in *IEEE Access*, 2018, 52138 ss.

[47] ISO/IEC, *Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence*, ISO/IEC TR 24028:2020, 2020.

Lohr introdusse il termine «dataismo»[48] per descrivere una potenziale "dittatura digitale" in cui l'autonomia umana rischia di soccombere al peso degli algoritmi. Con i sistemi di intelligenza artificiale di nuova generazione, la posta in gioco è divenuta ancor più alta: l'ambito applicativo di tali tecnologie travalica l'analisi dei dati, interessando l'erogazione di servizi pubblici, la gestione del traffico, le componenti di sicurezza dei macchinari industriali, i veicoli a guida autonoma e, attraverso l'IA generativa, la produzione di contenuti testuali, visivi e sonori difficilmente distinguibili da quelli reali. La protezione non riguarda più soltanto la riservatezza delle informazioni e la libertà di scelta, ma si estende alla stessa integrità psico-fisica degli individui e alla tenuta dell'ecosistema informativo. In tale contesto il principio di *accountability* si dilata fino a investire direttamente i fornitori di sistemi di IA ad alto rischio, i quali devono assicurare un livello di trasparenza elevato lungo l'intero ciclo di vita del prodotto. Da un lato ciò implica mettere i *deployer* nella condizione di conoscere in modo esaustivo le caratteristiche tecniche, i limiti operativi e le condizioni di impiego sicuro, così da consentire un controllo effettivo del sistema anche dopo la commercializzazione; dall'altro, comporta fornire agli utenti finali informazioni chiare sui benefici e sui possibili pericoli derivanti da usi impropri o fraudolenti, affinché il rapporto con l'IA rimanga consapevole e bilanciato. Solo una trasparenza intesa in questa duplice accezione può consolidare la fiducia nella società dei dati e scongiurare il rischio che l'innovazione tecnologica si traduca in una nuova forma di eterodirezione digitale.

[48] S. Lohr, *Data-ism. Inside the Big Data Revolution*, Londra, 2016. Sul tema, cfr. I. Syllaidopoulos, *Dataism: The Rise of a Data-Driven World? A Guide for Data-Oriented Policy and Management*, in *International Journal of Multidisciplinary Research and Analysis*, 2023, 3580 ss.

Alessandro Oldani

Abstract

Il contributo esamina l'evoluzione del concetto di trasparenza algoritmica nel diritto europeo, ripercorrendone lo sviluppo dal GDPR fino all'AI Act. Dopo aver analizzato il fondamento giuridico nell'art. 22 GDPR, il lavoro si sofferma sulla classificazione dei sistemi di IA in base al rischio e sugli obblighi di trasparenza per fornitori e *deployer*. Vengono distinti i livelli di trasparenza tecnico-operativa e sostanziale, concludendo con una riflessione su interpretabilità e spiegabilità nel quadro della *Explainable AI* (XAI).

This article examines the evolution of algorithmic transparency in EU law, tracing its development from the GDPR to the AI Act. After analysing the legal basis under art. 22 GDPR, the paper addresses the AI Act's risk-based classification and the transparency obligations imposed on providers and deployers. Two distinct levels of transparency are identified: technical-operational and substantive, concluding with a reflection on interpretability and explainability within the framework of Explainable AI (XAI).

Keywords

algorithmic transparency – artificial intelligence – GDPR – AI Act – self-determination

Best interest of the child e cyberspazio: il fenomeno dello *sharenting* alla prova del diritto. Essere figli e genitori nell'epoca della sovraesposizione digitale*

Marco Ciuro

Sommario

1. Introduzione. – 2. Dall'*Offline* all'*Online*: l'evoluzione del *best interest of the child* nell'ecosistema digitale. – 3. La tutela dei minori nello spazio digitale: identità e autodeterminazione della persona minore d'età nella normativa sovranazionale e nazionale. – 4. Il figlio è mio e lo posto io...! Il "caso serio" dello *sharenting* tra *best interest of the child* ed esercizio della responsabilità genitoriale. – 5. Conclusioni.

1. Introduzione

Nell'era digitale in cui si trova a vivere, volente o nolente, il *parent technologicus*, l'immagine dell'infanzia si è trasferita, spesso con sciagurata inconsapevolezza, dagli album di famiglia ai *feed* dei social media. Si tratta di una fattualità che interpella plurimi sguardi, da quello del sociologo a quello dello psicologo, sino a bussare le porte delle stanze del giurista. L'incalzante tendenza alla "vetrinizzazione sociale" – per dirla con Codeluppi[1] - trova negli spazi pressoché sconfinati del *web* un palcoscenico catalizzante l'esibizione, sovente inconsapevole e financo rifiutata, di contenuti e protagonisti le cui intimità si scontrano appunto con le vetrine o, meglio, i vetri di *smartphone*, *pc* e *tablet*. A fronte di quello che potremmo chiamare un novello paradigma "digitale" delle relazioni familiari – e segnatamente,

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

[1] Il riferimento è a V. Codeluppi, *La vetrinizzazione sociale. Il processo di spettacolarizzazione degli individui e della società*, Torino, 2007.

quelle di filiazione - la genitorialità diviene *social*, si mette in vetrina e, di conseguenza, mette in vetrina anche l'infanzia[2]. I genitori di oggi sono infatti definiti "*media moms and digitals dad*"[3], e il *parenting* ha trovato una nuova e largheggiante declinazione nel c.d. "*sharenting*" termine nato dalla fusione dei verbi *to share* (condividere) e *parenting* (fare i genitori) e indicante la pubblicazione di foto e contenuti, da parte di genitori e/o *caregivers*, riguardanti i propri figli. L'equilibrio tra la volontà genitoriale di narrare pubblicamente la propria esperienza familiare e la tutela dei diritti fondamentali del minore – in particolare il diritto alla riservatezza, alla *privacy*, all'identità personale e allo sviluppo della propria personalità – rappresenta oggi una sfida ineludibile anche per il diritto minorile, il quale è chiamato a confrontarsi con tracciati nuovi di una responsabilità genitoriale pervasa dalla dimensione digitale, ove i confini tra doveri giuridici ben precisi connessi all'esercizio delle funzioni parentali (artt. 315 bis e 316, c.c.) e individualistici bisogni di pubblicizzare la vita propria e quella della propria prole, appaiono diafani e bisognosi di una precisa regolamentazione. In scenari in cui «la distinzione tra immagine pubblica e privata sembra perdere ogni rilevanza e lo stesso concetto di privacy, nel virtuale, appare profondamente mutato»[4], gli interrogativi che sovvengono sono diversi. Si tratta non solo di guardare al fenomeno dello *sharentin*g sulla base della normativa sovranazionale (comunitaria, soprattutto) e nazionale ma anche – e primariamente – verificare l'efficacia degli strumenti attualmente a disposizione del diritto per offrire una tutela effiace a quei soggetti – i minorenni, appunto – i quali abbisognano, in virtù della loro condizione, di una tutela rafforzata che non offra solamente garanzia di protezione nell'*hic et nunc*, ma si proietti al *post*, tenendo conto della dimensione prognostica di quei fatti che interessano il percorso evolutivo del minorenne e che potranno condizionarne la crescita e lo sviluppo. Nella fisiologia delle relazioni familiari i soggetti deputati alla cura e alla sorveglianza del percorso di crescita dei propri figli sono naturalmente i genitori o, comunque, i soggetti esercenti la responsabilità tutelare e/o *caregivers*: genitori e *caregiver*s, i quali sovente scontano un'asimmetria di nozioni informatiche rispetto ai figli e figlie, sono chiamati ad esercitare i doveri di sorveglianza su di un campo spaziale pressoché sconfinato com'è quello del *web*, con evidenti implicazioni, peraltro, in tema di responsabilità degli stessi per eventuali illeciti compiuti dai figli minori. Per un verso diametralmente opposto – ed è su questo che si concentrerà il presente contributo – si genera un'inversione

[2] Cfr. D. Cino, S. Demozzi, *Figli "in vetrina". Il fenomeno dello sharenting in un'indagine esplorativa*, in *Rivista Italiana di Educazione Familiare*, 2, 2017, 157.

[3] Si veda T.Y. Ulhs, *Media Moms, Digital Dads. A Fact Not Fear Approach to Parenting in the Digital Age*, Boston, 2015

[4] R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, in *Persona e Mercato*, 3, 2021, 512.

dei termini allorché la presenza in rete delle persone minori d'età non è un fatto scaturito da una mancata sorveglianza del genitore ma cagionata dalla precisa volontà dello stesso (o degli stessi) di gettare nel mondo virtuale i propri figli[5]. Detto diversamente, coloro che sono chiamati a garantire, tutelare e promuovere il superiore interesse del minore nel momento in cui quest'ultimo fa ingresso inconsapevole nel cyberspazio, invece che preservarne lo sviluppo dall'esposizione incontrollabile della rete, spesso arrivano ad esporre bambini anche molto piccoli ad intromissioni potenzialmente globali della di loro sfera personale, mettendo in discussione «*the strong presumption that the family always acts in the children's best interest [...] in fact, the implications of sharenting are reals for minors and have the potential to have long lasting effects on minor's lives*»[6]. Il tema in analisi, giocato tra equilibri delicati e bilanciamenti di interessi di adulti e minori, proprio nell'individuazione ermeneutica del superiore interesse del minore, (una sorta – potremmo dire – di "*best interest 2.0*"), sotto la cui egida vanno inquadrati i possibili conflitti di interessi tra genitori e figli, mette a fuoco un assetto familiare dai contorni problematici e affatto definiti; si tratta di fare i conti con un modello di organizzazione delle relazioni di filiazione a fronte del diritto della persona di minore età alla propria riservatezza nonché al controllo di quei dati personali che lo riguardano e gli appartengono ma che sovente nei casi di *sharenting* quest'ultimo non può fare valere per evidenti ragioni d'età[7]. In considerazione delle possibili violazioni dei diritti del minore ad opera dei *caregivers* di riferimento nel contesto digitale, nell'alveo di una riperimetrazione di limiti, autonomie e connesse responsabilità genitoriali nel contesto virtuale, la questione della preparazione del diritto e dei suoi sistemi rimediali a disciplinare ma anche a sanzionare il mancato rispetto di nuovi doveri di cura – perché di ciò si sta parlando – come sono quelli connessi alla protezione del minore da spazi sconfinati come sono quelli del *web,* non può essere elusa e va affrontata innegabilmente attingendo ad un approccio interdisciplinare. Si tratta infine – o primariamente – di interrogarsi sulla stessa adeguatezza del diritto di cogliere, prima di regolamentare, un assetto socio-culturale di egemonia della dimensione virtuale la cui forza è in grado di generare non solo nuovi interrogativi per le scienze ma anche di ridefinire i bisogni e financo generandone di nuovi, disegnando, di conseguenze, esigenze di tutela differenziate e rafforzate. Il fenomeno

[5] Su questo "corto circuito" esercizio della responsabilità genitoriale e "vigilanza digitale" si rinvia a B. Agostinelli, A*utonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, 427.

[6] S. Donovan, '*"Sharenting": The Forgotten Children of the GDPR*', in *Peace Human Rights Governance*, 4(1), 2020, 44.

[7] Cfr. C. Carmandi, *Minore e privacy nel contesto delle relazioni familiari*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, 2019, 121.

dello *sharenting* permette l'emersione di quanto sinteticamente tematizzato e consente riflessioni, *de iure condendo*, condotte alla luce del *best interest of the child,* diritto e principio anch'esso non immune alle modulazioni e fluttuazioni che l'ecosistema digitale può produrre.

2. Dall'*Offline* all'*Online*: l'evoluzione del *best interest of the child* nell'ecosistema digitale

Il ruolo di primaria importanza che il mondo digitale riveste per le persone minori d'età, le quali dall'avvento dei *social networks* hanno scelto questo canale quale privilegiata forma di interazione e comunicazione tra loro, esige una corrispondente edificazione di un sistema che sia in grado di bilanciare le istanze di circolazione dei dati con la garanzia di un'adeguata tutela dei soggetti più bisognosi di cautele – come sono, appunto, bambini/e e ragazzi/e - favorendo al contempo lo sviluppo della loro capacità di autodeterminazione[8]. L'ipercinesi che sconta lo sviluppo tecnologico, specie nel campo dell'informazione, impone innanzitutto un coerente e modulato approccio ermeneutico nonché una valutazione dell'efficacia degli strumenti giuridici a disposizione del giurista e, *a fortiori*, del legislatore per comprendere e regolamentare attraverso una lettura costituzionalmente orientata dei diritti e delle libertà che si incrociano nel fenomeno sociale dello sviluppo umano e tecnologico la rivoluzione che la c.d. infosfera[9], ha portato nella quotidianità. Gli echi di questa rivoluzione tutt'ora *in fieri*, sono sentiti – consapevolmente o meno – proprio dalle persone minori d'età, giacché principali utilizzattrici di tecnologie virtuali sempre più precocemente[10]. La frequentazione assidua del mondo virtuale e so-

[8] Cfr. I. Garaci, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in *NLCC,* 4, 2021, 812.

[9] Con quest'espressione s'intende il nuovo spazio che viviamo, ma non è il cyberspazio di una volta: è qualcosa di più, lo include. Sono proprio le tecnologie dell'informazione che hanno creato questa nuova realtà mutando lo spazio che fa coesistere online e offline. Il termine è stato introdotto da L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2014.

[10] Sul punto si può vedere la ricerca "*Alfabetizzazione mediatica e digitale a tutela dei minori: comportamenti*, *opportunità e paure dei navigatori under 16*", studio promosso dal *Ministero delle Imprese e del Made in Italy* e condotto dall'*Alta Scuola in Media, comunicazione e spettacolo dell'Università Cattolica di Milano*, pubblicato il 15 febbraio 2024. La ricerca è stata condotta su un campione costituito da 1.677 minori di età compresa fra gli 8 e i 16 anni. Dallo studio è emerso che il 94% degli intervistati utilizza regolarmente uno smartphone e fra questi il 68% ne possiede uno personale, ricevuto prima dei 10 anni nel 28% dei casi; il 70% dei ragazzi e il 50% dei bambini ha dischiarato di usare regolarmente social media; 4 intervistati su 10 hanno riferito esperienze negative; più della metà degli intervistati ha riferito di aver visto sui social contenuti non adatti alla propria età almeno una volta di

vente non accompagnata da una consapevolezza dello strumento manipolato e dei rischi ad esso connessi, impongono una riflessione particolarmente attenta che bilanci i bisogni di tutela rafforzata - garantiti da un approccio *child oriented* - l'autodeterminazione dei c.d. "grandi minori" nel contesto informatico, con i doveri che scaturiscono dall'esercizio della responsabilità genitoriale, e i limiti ad esso connessi *in subiecta materia*, sempre a garanzia dei diritti dei figli minori. Come noto, il principio ermeneutico e diritto fondamentale che permette di bilanciare diritti e interessi contrapposti, è il superiore (o preminente) interesse del minore, il c.d. "*best interest of the child*". L'espressione in parola, dall'ampio respiro innovativo, è in realtà – come ampiamente studiato – un concetto controverso e di non facile interpretazione, caratterizzato da un intrinseco dinamismo, rappresentante, a ben vedere, il maggiore potenziale e l'aspetto più vulnerabile del *best interest*. In tale sede non è possibile dare contezza di un tema tanto ampio e multiforme; appare utile – anche ai fini del presente contributo - rimarcarne l'aspetto pratico-applicativo più importante ossia che al concetto in parola non vada attribuita un'aprioristica e assoluta preminenza rispetto agli altri interessi ma si debba operare un ponderato bilanciamento con gli altri interessi in gioco e nel concreto si deve apprezzare in che modo l'interesse delle persone minori d'età possa essere integrato – pur dovendosi accordare a quest'ultimo una "netta prevalenza" - con gli altri interessi, potenzialmente confliggenti con esso[11]. Nella dimensione virtuale, gli scenari di conflitto con il principio del *best interest of the child* che possono profilarsi, come si dirà meglio nel successivo paragrafo, sono diversi; dal diritto alla *privacy*, passando per l'utilizzo delle immagini del minore, sino al complesso tema della profilazione dei dati di quest'ultimo. L'ambiente digitale, di converso, può indubbiamente concorrere alla realizzazione di molti diritti in capo alle persone minori d'età e giocare un significativo ruolo di inclusione e promozione personale[12]; si pensi, ad esempio, al diritto alla partecipazione del minore ai processi decisionali, sancito dall'art. 12 della Convenzione di New York del 1989. Lo strumen-

recente; i controlli dei genitori diminuiscono con l'aumentare dell'età dei figli: solo il 20% dei ragazzi (14-15 anni) ha ammesso di essere controllato dai genitori.

[11] Cfr. L. Lenti, *Note critiche in tema di interesse del minore*, in *Riv. dir. civ.*, 2016, 103. L'A., giustamente osserva che il concetto di "interesse del minore" non è scevro da ambiguità, polisemie ma anche utilizzi strumentali al fine di dirimere una questione in cui sono coinvolte le persone minori d'età. In nome, a volte, di un utilizzo "magico" del termine l'interesse del minore viene sottratto ad un bilanciamento con gli altri interessi in gioco. Si tratta invece, secondo il Lenti, di ricercare un punto di equilibrio pur nella salvaguardia delle cautele speciali che impone l'interesse di cui il minore è potatore.

[12] Cfr. L. Miglietti, *La sovraesposizione digitale dei minori ed i suoi effetti. Note comparative sul fenomeno del c.d. "sharenting" negli ordinamenti francese e italiano, in Rivista di Diritti Comparati*, 3, 2024, 211.

to digitale, caratterizzato dalla possibilità della globalità e viralità delle informazioni, può fungere da catalizzatore delle opinioni di bambini/e e ragazzi/e su larga scala. In questo scenario già di per sé intricato, come già accennato, si deve aggiungere il fatto che gli strumenti (soprattutto di natura privatistica) tutt'ora a disposizione del diritto non appaiono sufficientemente adeguati a rispondere ai nuovi bisogni generati (di continuo) dalle nuove tecnologie, con immediate ricadute sul piano della tutela; così, ad esempio, lo strumento del consenso appare poco idoneo «sia per la difficoltà tecnica di accertare l'età anagrafica degli utenti, sia perchè non garantisce di fatto una piena autodeterminazione informativa»[13]. Stessa sorte, come si avrà modo di argomentare, paiono scontare i profili rimediali più comuni che rispondo ad una logica affatto sovrapponibile agli interessi in gioco; difatti i rimedi offerti dal *General Data Protection Regulation* (da ora: GDPR) in materia di trattamento di dati personali si trovano inevitabilmente a presidiare tipologie diverse di interessi; personali quelli inerenti il diritto alla *privacy*, economici quelli inerenti alla circolazione dei dati. Spostandoci, invece, sul fronte giurisprudenziale interno, la criticità – innanzitutto di cultura giuridica – che pare emergere analizzando emblematicamente il "caso serio" dello *sharenting* (ma le riflessioni, *mutatis mutandis*, possono essere estese alle molteplici situazioni in cui si controverta in tema di immagine del minore nel *web*) riguarda proprio la piena comprensione degli interessi in gioco, spesso assorbiti dalle controversie familiari in cui, sotto il profilo rimediale, la tutela inibitoria largheggia nell'applicazione, glissando tuttavia sull'interesse preminente del minore al quale, come noto, deve essere attribuito un rango più elevato. Ancora una volta, si tratta di operare un bilanciamento evitando, però, che «il costo di questo difficile bilanciamento sia sopportato da chi ha inevitabilmente le spalle più deboli»[14]. Il riconoscimento in capo alla persona di minore età dell'effettiva titolarità di situazioni giuridiche esistenziali, come sono quelle che riguardano la sua presenza nel mondo digitale, rappresenta la più adeguata prospettiva di tutela e promozione del *best interest of the child*, nel contesto informatizzato. Il complesso intarsio di tematizzazioni e scienze coinvolte non può che richiedere un approccio interdisciplinare e transdisciplinare, al fine di tenere conto di tutte le implicazioni che s'irradiano ogni qualvolta la persona di minore età si trova a connettersi con il mondo virtuale; se da una parte appare poco lungimirante un approccio di tipo paternalistico e tabuizzante, volto a limitare l'accesso dei più giovani al mondo virtuale, dall'altra non si può negare, come emerge altresì dalla produzione giuridica

[13] Cfr. I. Garaci, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale,* cit., 803

[14] M. Bianca, *Il minore e i nuovi media, in* R. *Senigaglia (a cura di), Autodeterminazione e minore età*, cit., 68.

– perlopiù di *soft law* - soprattutto comunitaria, che proprio la condizione di riconosciuta vulnerabilità del minore e il correlato bisogno di maggiore attenzione, esigono una tutela rafforzata proprio al fine di garantirne il preminente interesse ad uno sviluppo identitario non influenzato e financo coartato, da ingerenze e costrizioni provenienti da i più disparati angoli del *web*, anche da parte di quei soggetti che dovrebbero esserne preposti – ed è il caso dello *sharenting* – alla cura e alla sorveglianza evolutiva[15]. È evidente, dunque, il delicato punto di equilibrio che si è chiamati a individuare: consentire ai minori di accedere alla rete al fine di esercitare i propri diritti costituzionalmente rilevanti, allo stesso tempo prestando adeguata attenzione perché la stessa non si riveli un'arma a doppio taglio in grado di ledere o minacciare il loro sviluppo e la loro formazione[16]. Gli stessi doveri connessi al *munus genitoriale*, così come richiamati dagli artt. 315 *bis* e 316 c.c., esigono un aggiornamento alla luce dei sopraggiunti bisogni suscitati dalla dimensione virtuale in cui si trovano a vivere bambini e ragazzi. Si tratta di ragionare rispetto all'accresciuta estensione del controllo genitoriale alla *digital life* dei propri figli, in particolare all'utilizzo dei *social networks* e dunque ai limiti di ingerenza di questi ultimi nella *privacy* degli stessi, giustificata proprio dai rischi connessi all'utilizzo di piattaforme telematiche e all'estrema difficoltà nel controllo e nel filtro dei contenuti in esse presenti[17]. Se non pare esserci dubbio che il dovere di sorveglianza dei genitori nei confronti dei figli si possa tradurre anche in un corrispondente potere di intrusione nella di loro vita privata – sempre al fine di evitare danni in capo ai medesimi e/o a terzi – è altrettanto vero che tali ingerenze incontrino un limite nel diritto del minore alla riservatezza. La questione è, ancora una volta, quella della confine, del limite non solo tra i dicotomici parametri giuridici del "lecito" ed "illecito" ma anche tra quelli educativi della fiducia e del controllo che permeano la relazione "genitori-figli" e che costituisce uno dei tratti più complessi ed identificativi della fenomenologia della c.d. "famiglia digitale"[18]. Allora, gli spazi di ingerenza del genitore potranno dirsi leciti sia sotto l'aspetto giuridico che sotto quello educativo, allorquando l'intromissione dell'esercente responsabilità genitoriale è funzionale e teleologicamente orientata alla protezione del

[15] Così, M. Orofino, *Minori e diritto alla protezione dei dati personali*, in M. Orofino - F. G. Pizzetti (a cura di), *Privacy, minori e cyberbullismo*, Torino, 2018, 13.

[16] Cfr. D. Pierantoni, *Minori su internet: profili di responsabilità*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, 405.

[17] Vedi diffusamente G. B. Reggiani, *Protezione dei minori dai contenuti nocivi circolanti sulle Video Sharing Platforms: un'ipotesi di (ir)ragionevolezza legislativa?*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, 375 ss.

[18] Il riferimento è a V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, Milano, 2021.

figlio stesso, verso sé stesso e verso altri. Proprio perché si tratta di comprimere un diritto di rango elevato (e per alcuni di rilievo costituzionale)[19] della persona minore d'età (il diritto, appunto, alla riservatezza), tale compressione è ragionevole che debba avvenire nei limiti di quanto necessario ai genitori per addivenire «alla soluzione del problema esistenziale del minore in ragione del quale l'accesso [ai suoi dati personali, n.d.r.] è stato motivato»[20] . Se si considera che le norme civilistiche nulla dicono sull' *an* e il *quomodo* di questo difficile equilibrio[21], ancora più importante si staglia il ruolo del *best interest of the child,* modulato alla luce delle specificità del contesto digitale. L'accentuata forza pervasiva della sfera personale e relazionale esercitata dalla tecnologia digitale non può allora che esigere dall'ordinamento giuridico risposte adeguate «sia in termini di interessi tutelati (emersione di nuovi diritti) sia di mezzi di protezione»[22]. Oltre a ciò, è d'uopo una riflessione preliminare: l'ordinamento giuridico ha preso atto della necessità dei limiti degli strumenti a propria disposizione per regolamentare un flusso in costante divenire? E ancora: c'è la consapevolezza del mutamento di paradigma in atto sia sul fronte dei doveri genitoriali e dei corrispondenti interessi dei minori generato proprio dall'affermarsi della digitalizzazione? Come si avrà modo di vedere nel paragrafo dedicato allo *sharenting*, il quadro che emerge desta non poche perplessità in ordine all'importanza attribuita alla fenomenologia della presenza virtuale della persona minore d'età, che pare rivestire un ruolo di parvenu all'interno dei conflitti familiari piuttosto che assurgere a questione preminente ai fini della predisposizione di un adeguato sistema di protezione ed, eventualmente, anche sanzionatorio. È evidente che senza un adeguata prioritarizzazione del tema in parola, il sistema di protezione e anche di promozione di diritti ed interessi della persona minore d'età in ambito informatico non potrà che essere strutturalmente deficitaria.

In un quadro siffatto, di complessità ed opportunità, anche per quel che concerne il tema della presenza dei minori sul web, *il best interest of the child*, è chiamato a svolgere il ruolo di principio-cardine, come ben attestato a livello comunitario. Il *General Comment n. 25* del 2021 *on children's rights in relation to the digital environment* è dedicato proprio alla posizione del minore nel contesto digitale. La *Committee on the Rights of the Child* , riconoscendo che «*The digital environment is becoming increasingly important across most aspects of*

[19] Così M. Orofino, *Minori e diritto alla protezione dei dati personali*, in M. Orofino - F.G. Pizzetti (a cura di), *Privacy, minori e cyberbullismo,* cit., 1 ss.

[20] C. Camardi, *Minore e privacy nel contesto delle relazioni familiari*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età*, cit., 136

[21] Così M. Foglia, *Sharenting e riservatezza del minore in rete*, in *Actualidad Juridica Iberoamericana*, 16 bis, 2022, 3560.

[22] R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, in *Persona e Mercato*, 3, 2021, 515

children's lives, including during times of crisis, as societal functions, including education, government services and commerce, progressively come to rely upon digital technologies» (I, 3), incarica gli Stati di «*implement the Convention in relation to the digital environment and provides guidance on relevant legislative, policy and other measures to ensure full compliance with their obligations under the Convention and the Optional Protocols thereto in the light of the opportunities, risks and challenges in promoting, respecting, protecting and fulfilling all children's rights in the digital environment*» (II, 7). Il punto appena citato può dirsi una summa efficace della postura digitale del minore negli spazi del web, ove si gioca la partita tra le più volte citate istanze partecipative e promotive e le istanze protettive provenienti dal mondo adulto. Nel General Comment n. 25 è ripreso altresì il ruolo del *best interest of the child* che proprio grazie alla sua duttilità è capace di adattarsi ad un contesto nuovo, quello dello sviluppo digitale il quale, si ammette con una certa laconicità «*was not originally designed for children, yet it plays a significant role in children's lives*» III, B, 12). La questione non è dunque altrimenti differibile da parte del legislatore e, in genere, del giurista, pena un vuoto normativo che si traduce irrefragabilmente in un vuoto di tutela. Tra gli strumenti atti a garantire una presenza quanto più sicura possibile delle persone minori d'età, si può mutuare la pratica suggerita nel General Comment 14 del 2013 *on the right of the child to have his or her best interests taken as primary consideration,* di attuare un costante lavoro di *child right impact assestment* , quale pratica fondamentale di *child safeguarding*; si tratterebbe, ad esempio, di potenziare i sistemi di *parental control* – come peraltro suggerito dal recente d.l. 123/2023, il c.d. "Decreto Caivano" - incrementare la responsabilità degli *Internet service provider*, visto il loro ruolo attoriale nel creare un ambiente quanto più sicuro possibile per i soggetti più vulnerabili ma anche più presenti. Si è consapevoli che tali proposte non sono di facile attuazione o, meglio, difficilmente possono stare dietro all'ipercinesi dello sviluppo digitale. Come si può leggere nel recente (febbraio 2025) documento dell'Unicef *Best Interests of the Child in Relation to the Digital Environment, vi* è un'intrinseca complessità che caratterizza la predisposizione di un adeguato sistema di protezione e promozione digitale rivolto e tarato sulle caratteristiche evolutive delle persone minori d'età. Così «*This is due to several factors, including rapid technological change, the difficulty of gathering accurate data about children's online presence and vulnerability to online risks, varying forms and levels of impact*»[23] (IV). È d'uopo rimarcare il fatto che lo spazio digitale non è solo un terreno sconnesso; è altresì una fucina di opportunità, di inclusione e di partecipazione per le persone minori d'età e innegabilmente costituisce un mezzo imprescindibile per garantire il rispetto e l'attuazione dell'art. 12 della CRC su differenti livelli; si pensi, ad esempio, alla possibilità di promuovere delle forme di consultazione da

[23] Il testo del documento è consultabile al sito *unicef.org*.

remoto, delle occasioni di "*question time*" e di dibattito anche su proposte legislative che poi, di fatto, si riverberano su ragazze e ragazzi, il cui ascolto potrebbe più agevolmente essere realizzato ricorrendo a delle piattaforme digitali. In sintesi, riprendendo ancora il documento dell'Unicef in parola, la questione è «*protecting children from potentially harmful online content needs to be balanced with respecting their right to access information and participate in online communities*» (V). La riconosciuta importanza del tema *de quo*, pare essere centrale nella strategia dell'Unione Europea, come si vedrà anche dall'apparato normativo comunitario. A riprova di ciò, il 23 febbraio 2022 il Comitato dei Ministri del Consiglio d'Europa ha adottato la nuova Strategia per i diritti dell'infanzia (2022-2027) "*Children's Rights in Action: from continuous implementation to joint innovation*"che guiderà il lavoro del Consiglio nei prossimi sei anni[24]. All'interno della *strategy* un passaggio importante riguarda proprio il diritto di bambini e ragazzi alla sicurezza digitale. Sulla base dei presupposti che «*Children are growing up in a digital world and come into contact with technologies in many different ways*» (2.3, 35) ma tale sviluppo non avviene in modo omogeno per tutti e infatti «*Many children in vulnerable situations, such as children belonging to national minorities or children with disabilities, and children having no or limited access to the Internet and other digital technologies, are not familiar with these and are left out of digital education*» (2.3, 36), l'obiettivo di una strategia di tutela dei diritti dell'infanzia non può prescindere dal garantire non solo la possibilità diffusa di accesso alle informazioni che la rete può offrire ma lavorando alacremente perché tale accesso sia il più sicuro possibile. Solo rispettando ambedue i criteri si potrà garantire la realizzazione del *best interest of the child* ad avere «*Equal opportunities and social inclusion for all children*» con l'attenzione costante a garantire il difficile equilibrio tra istanze di protezione e di promozione. Con le parole del documento «*There is a challenging balance to be struck between children's protection and privacy and their right to participate in the digital environment, whilst identifying innovative, childsensitive ways of using the digital technologies in the best interests of the child and society*» (2.3, 37). Vale la pena fare un accenno di completezza. La strategia del Consiglio d'Europa (2022-2027) va letta unitamente ad un'altra strategia, questa *ad hoc* sul tema. Si tratta della "Strategia europea per un internet migliore per i ragazzi" del maggio 2022, la c.d. "*Bik* +", la quale costituisce un aggiornamento della strategia "*Bik*" del 2012. La *Bik* +, in estrema sintesi, propone azioni basate su tre pilastri: garantire esperienze digitali sicure, realizzare un'emancipazione digitale e garantire una

[24] Il testo approvato costituisce la quarta edizione di una serie di strategie di successo volte a far progredire la protezione e la promozione dei diritti dei bambini in tutto il continente Europeo, nel quadro del programma "Costruire un'Europa per e con i bambini" in vigore dal 2006.

partecipazione attiva di ragazzi e ragazze[25].
Il nostro Paese non è stato insensibile al tema del superiore interesse del minore in ambito digitale. L'Autorità Garante per l'Infanzia e l'Adolescenza (AGIA) ha realizzato il *Manifesto dei bambini sui diritti in ambiente digitale*; non è causale che non si tratti di un manifesto dei diritti ma un manifesto dei bambini, a rimarcare la dimensione paidocentrica e partecipativa di ogni riflessione giuridica e metagiuridica sui diritti dell'infanzia e dell'adolescenza. Sotto l'egida del *best interest of the child* va dunque condotta la riflessione sulla complessità ortopratica che connota il mondo digitale e l'affermazione di una cittadinanza del minore in questo mondo, regolata – ed è questo il punto – da una normativa che sia rispondente alle nuove situazioni che l'*internet* è in grado di suscitare.

3. La tutela dei minori nello spazio digitale: identità e autodeterminazione della persona minore d'età nella normativa sovranazionale e nazionale

Il tema sovra enucleato del ruolo chiave del superiore interesse del minore nel mondo digitale e l'esigenza di una sua modulazione che tenga conto del *proprium* del contesto informatizzato affinché possa inverarsi e non rimanere un mero proclama, necessita di un quadro normativo di riferimento. Negli ultimi anni la normativa sovranazionale (*in primis*) ha dimostrato un'attenzione particolare per lo sviluppo digitale (*digital enviroment*), specialmente nelle ripercussioni sui minori, in quanto privilegiati utilizzatori delle nuove tecnologie.
Volendo individuare – anche per evidenti ragioni di brevità espositiva – i principali ambiti in cui l'intervento normativo interno e sovranazionale in materia di protezione del minore nell'ambiente digitale, si possono segnalare due macroaree, tra loro chiaramente interconnesse. La prima area riguarda la tutela dell'identità e della riservatezza del minore ed ha precipuamente a che fare con l'intrinseca vulnerabilità di quest'ultimo e le connesse peculiari esigenze di tutela, prefigurando possibili scenari in cui l'immagine del minore abbia una diffusione potenzialmente virale e di questa possano essere fatti gli usi più diversi e abietti. Il quadro normativo internazionale richiama innanzitutto l'art. 8 della Convenzione di New York del 1989 il quale impone agli Stati l'obbligo di tutelare e preservare l'identità personale del minore. Tale norma va letta in combinato disposto con l'art. 16 il quale, a sua volta, tutela la vita privata del minore, vietandone indebite interferenze nonché qualsivoglia tipo di pregiudizio alla sfera dell'onore, della reputazione e dell'immagine. La seconda macro-

[25] Il documento è consultabile al sito *eur-lex.europa.eu*.

area riguarda l'autodeterminazione del minore nel mondo digitale nonché la validità e le conseguenze del consenso da questi manifestato. Volendo continuare il parallelismo con la Convenzione di New York, il riferimento è il ben noto art. 12 il quale, pur non occupandosi direttamente del consenso, sancisce il diritto della persona minore d'età ad essere ascoltato, ad esprimere la propria opinione la quale dovrà essere presa in seria considerazione attribuendo al minore dotato di discernimento l'esercizio di una certa autonomia decisionale.

Si deve precisare che autodeterminazione e identità non sono le uniche tematiche che emergono dalla normativa che regolamenta la tutela del minore in ambito digitale ma rappresentano le coordinate privilegiate sulle quali pare costruirsi su più livelli, una strategia che sia capace innanzitutto di comprendere la portata rivoluzionaria del periodo storico-giuridico in cui sussumere codeste tematiche. Un'ulteriore premessa metodologica prima di iniziare la panoramica. L'apparato normativo sul tema, anche qualora brillasse per esaustività, limpidezza e coordinamento – ma non è così – servirebbe a poco se non presumesse un'alleanza "con" la famiglia e "nella" famiglia; va da sé che se i genitori abiurano il loro mandato di cura e sorveglianza nei confronti dei figli e non condividono un modello educativo in cui il minore non va né lasciato in balia dei flutti del *web* (che di per sé non può tabuizzarsi), allora non potrà costruirsi alcunché di utile per la società giacché ad essere aggirato è primariamente un piano assiologico. Il richiamo è, dunque, non solo all'impegno da richiedere agli Stati ma anche al «dovere educativo che incombe in capo ai soggetti privati che presidiano le piattaforme frequentate dal minorenne e che intrattengono, per lo più in via esclusiva, il rapporto (tecnologico) con lui»[26].

Ciò premesso, si è avuto modo di cogliere già nel precedente paragrafo alcune espressioni di *soft law* che hanno il merito di contribuire ad implementare la normativa comunitaria sulla questione in analisi. Come anticipato, i temi principali attorno i quali è costruito il plesso normativo di tutela del minore nello spazio digitale, possono individuarsi nell'identità e nell'autodeterminazione.

Preliminarmente, va precisato che la nozione di identità a cui si fa riferimento in questa sede è la c.d. "nozione estrinseca", intesa come mezzo di identificazione del soggetto[27]. L'avvento e l'espansione informatica ha inciso profondamente su questo aspetto che riguarda, chiaramente, la collettività tutta ma che assume dei rilievi ulteriormente critici quando si ha

[26] R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, cit., 516.

[27] L'altra nozione di identità è quella "intrinseca". Quest'ultima è stata ricostruita in una prima frase come «diritto ad essere correttamente rappresentati» mentre in una fase successiva, dopo la sentenza della Corte Costituzionale n. 13 del 1994, la nozione è da intendersi come «diritto ad essere sé stessi».

a che fare con le persone minori d'età. Giustamente è stato osservato che «l'identità è diventata un concetto liquido. E il diritto alla identità un diritto connesso con una realtà fattuale fluttuante, fluida, quasi inafferrabile. Di questa identità si è impossessata l'informatica, e l'ha piegata strumentalmente ai suoi usi patrimoniali»[28]. In particolare il diritto all'identità personale quale «diritto a non veder travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale»[29], è un diritto che è stato concepito quale diritto alla verità della persona, nella sua essenza fisica e morale attuale[30]. Nella persona minore d'età quanto sin ora detto si carica di un ulteriore elemento, che rappresenta il *proprium* di quella tutela rafforzata che esige ogni riflessione minorilistica; si tratta della dimensione evolutiva, ossia l'essere in formazione di bambini e ragazzi, sicché ogni evento che li riguardi non va pensato limitatamente all'*hic et nunc* situazionale ma va proiettato prognosticamente nella tensione al futuro e alla crescita di ogni individuo in formazione. Pertanto, emerge inevitabilmente l'esigenza di proteggere l'immagine e, così, l'identità del minore da una continua condivisione di dati alla quale sono, peraltro, correlati molteplici ed insidiosi rischi, che possono, appunto, riverberarsi sullo sviluppo della di lui personalità: si pensi non solo al furto di dati o di identità on line ma anche a fenomeni con coefficiente disvaloriale maggiore quali il cyberbullismo, il *child-grooming* e la pedopornografia.

Il diritto comunitario, dal canto suo, pare essere consapevole di questi ed altri rischi[31]. Nel 2022 è stato approvato il *Digital Services Act* (DSA[32]) il quale impone alle piattaforme online l'obbligo di proteggere i minori, mirando a prevenire e contrastare l'esposizione a contenuti dannosi, cyberbullismo, interazioni indesiderato, comminando altresì sanzioni fino al 6% del fatturato in caso di violazioni. Il DSA contiene all'art. 28 un preciso riferimento alla protezione online dei minori ("*Online protection of minors*") e, al paragrafo secondo, esplicita: «*Providers of online platform shall not present advertisements on their interface based on profiling as defined in Article 4, point (4), of*

[28] G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e Impresa*, 3, 2017

[29] Così Cass. civ., sez. I, 22 giugno 1985, n. 3769.

[30] Così M. Bianca, *La filter bubble e il problema dell'identità digitale,* in questa *Rivista*, 2, 2019, 50.

[31] Si sono comunque già occupati specificatamente dei dati dei minori sia il Programma comunitario pluriennale per la protezione dei bambini che usano Internet e altre tecnologie di comunicazione (Decisione n. 1351/2008/CE del Parlamento e del Consiglio del 16 dicembre 2008), sia la Risoluzione del Parlamento europeo del 20 novembre 2012 sulla tutela dei minori nel mondo digitale.

[32] Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo ad un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE.

Regulation (EU) 2016/679 using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor». Vietando esplicitamente la profilazione dei minori per scopi di marketing e impedendo alle piattaforme online la raccolta, l'analisi e l'utilizzo di dati appartenenti a persone infradiciottenni per creare pubblicità mirate, nonché stabilendo che le interfaccia e i meccanismi devono essere progettati con un livello massimo di privacy e sicurezza per i minori, da attivare per impostazione predefinita (c.d. "*privacy by design*"), il legislatore europeo ha preso una netta posizione sul tema. Non solo. Così facendo ha altresì colmato (come vedremo, *infra*) anche «quel vuoto di tutela che sembrava lasciato al GDPR»[33]. Accanto all'art. 28, il tema della protezione dei minori spicca nel Considerando 71 e ss. È infatti proprio in questo che vengono definite sia le condizioni a cui deve sottostare una piattaforma digitale per potersi dire accessibile ai minori, ma anche gli standard a cui i provider devono adeguarsi e gli obiettivi che devono perseguire per allinearsi alla disciplina europea. Si legge:

«*The protection of minors is an important policy objective of the Union. An online platform can be considered to be accessible to minors when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes. Providers of online platforms used by minors should take appropriate and proportionate measures to protect minors, for example by designing their online interfaces or parts thereof with the highest level of privacy, safety and security for minors by default where appropriate or adopting standards for protection of minors, or participating in codes of conduct for protecting minors*»

Il tema della protezione dei minori è dunque centrale nel DSA, a ragione – lo si è detto – del fatto che questi ultimi sono assidui frequentatori di piattaforme digitali ma anche della di loro condizione di vulnerabilità (cfr. art. 34, DSA). Sebbene il *Digital Services Act* abbia il merito di aver attenzionato la priorità di assicurare un ambiente *on-line* più sicuro e trasparente, sottolineando l'importanza della «responsabilizzazione delle piattaforme on-line» [34], rimangono ancora dei punti insoluti, altri che, invece, meritano un approfondimento: per quanto il DSA richieda alle piattaforme digitali

[33] M. Martorana - R. Savella, *L'utilizzo degli strumenti digitali da parte dei minori tra opportunità e rischi,* in M. Martorana - G. Guadagnini (a cura di), *Tutela del minore nella società digitalizzata. Analisi giuridica, filosofica e psicologica delle questioni legate all'uso delle nuove tecnologie*, Milano, 2023, 64.

[34] I. Garaci, *L'autodeterminazione digitale del minore e i confini della responsabilità genitoriale*, in *Archivio Giuridico Sassarese*, XXIX, 2, 2024, 62.

la rimozione di contenuti illegali, ancora c'è da fare rispetto al filtraggio sistematico di contenuti inappropriati per bambini/e e ragazzi/e; più stringente, poi, potrebbe essere la limitazione alla profilazione pubblicitaria e alle procedure di verifica dell'età minima. Qualcosa in più, si potrebbe fare rispetto al tema del c.d. "*design* etico", ossia delle linee guida rispetto alla realizzazione di interfaccia, notifiche, contenuti ma anche algoritmi più "*child friendly*".

La predetta vulnerabilità digitale ha come elemento costitutivo il fatto che il contesto che la determina, appunto quello virtuale, è in costante mutamento e il rischio di obsolescenza degli strumenti giuridici atti a regolamentarne i confini, è quanto mai concreto con il risultato di trovarsi a dei vuoti di tutela. Nell'era digitale, i minori sono esposti quotidianamente a sistemi di intelligenza artificiale che possono influenzarne – direttamente o indirettamente – le scelte; che si tratti di *social networks*, utilizzo di ChatGPT, giochi *online* e financo *chatbot* educativi, la presenza dell'IA è oramai onnipervasiva e la sfida pedagogico-giuridica è stare al passo, costruendo un dialogo multidisciplinare[35]. Ad esemplificare questa corsa all'aggiornamento informatico-giuridico, si inserisce il Regolamento sull'Intelligenza Artificiale (*Artificial Intelligence Act – AI Act*) del 2024. L'attenzione specifica alle vulnerabilità è espressa in diversi punti, fra i quali spicca l'art. 5 il quale vieta anche

« *the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm* »(lett. a) nonché «*the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation*» (lett. b).

L'*AI Act*, è indubbiamente un passo fondamentale di presa di consapevolezza della portata rivoluzionaria di questa "terza fase" del rapporto tra diritto e tecnica, in cui, come dice Mirzia Bianca, si pone «il problema della esistenza di nuovi attori della vita reale che si affiancano all'uomo e si sostituiscono ad esso per lo svolgimento di varie attività e di singole funzioni»[36]. L'impatto che l'intelligenza artificiale puà avere sulle immagini del minore e l'immagine che quest'ultimo ha di sé è potenzialmente incontrol-

[35] Sul punto si rimanda a F. Agrusti, *Educazione e intelligenza artificiale*, Roma, 2023, 13 ss.

[36] M. Bianca, *La filter bubble e il problema dell'identità digitale,* cit., 43.

lato: dall'elaborazione di immagini virtuali a scopo pornografico, sino chat artificiali in cui si possono veicolare contenuti svalutanti (es. *body shaming*). Come il *Digital Services Act*, anche l'*Artificial Intelligence Act* presenta delle criticità: dall'applicazione che sarà indubbiamente lente e prevedibilmente disomogenea, passando per una certa indefinitezza terminologica, sino ad arrivare all'intrinseca e connaturata velocità evolutiva dei modelli generativi, dei sistemi predittivi e degli algoritmi che superano di misura i tempi di aggiornamento normativi. Dai succinti passi riportati dei due Regolamenti, pare potersi affermare una certa apprensione da parte del Legislatore europeo per i rischi connessi alle pratiche manipolative le cui implicazioni vanno ben oltre le ragioni commerciali[37], suscitando riflessioni più ampie relative al rapporto tra diritto e tecnica, incidendo, *de iure et de facto*, anche sul paradigma tradizionale dei diritti fondamentali, in particolare quelli legati all'immagine e all'identità personale. Tali riflessioni non possono essere ignorate, *a fortiori* se si sta discettando di minorenni, poiché è partendo da tali coordinate che possono scorgersi le implicazioni etiche, giuridiche e pedagogiche sulle quali tentare di edificare un sistema condiviso – com'è quello di matrice comunitaria - di protezione e promozione dei diritti del minore in ambito digitale.

Le ragioni di brevità espositiva non consentono di indugiare dettagliatamente ma un accenno è d'uopo farsi – prima di passare alla normativa interna – alla proposta del 2022 di Regolamento per contrastare gli abusi sessuali sui minori (*Child Sexual Abuse Material* - CSAM). In breve, L'11 maggio 2022 la Commissione europea ha pubblicato una proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori. La proposta imporrebbe ai prestatori di servizi di *hosting*, di servizi di comunicazione interpersonale e di altri servizi obblighi condizionati di rilevazione, segnalazione, rimozione e blocco di materiale pedopornografico online noto e nuovo e per l'adescamento di minori. La proposta prevede inoltre l'istituzione di una nuova agenzia decentrata dell'UE (il «Centro dell'UE») e di una rete di autorità nazionali coordinatrici per le questioni di abuso sessuale su minori, al fine di consentire l'attuazione del regolamento proposto. Sebbene l'abuso e lo sfruttamento sessuale dei minori e la diffusione di materiale pedopornografico costituiscano reato in tutta l'UE come stabilito dalla direttiva 2011/93/UE sulla lotta contro l'abuso sessuale e la pornografia minorile, la portata *online* del fenomeno rappresenta una sfida che richiede adeguata attenzione e un'azione specifica da parte dell'UE e dei suoi Stati membri[38].

[37] S. Orlando (a cura di), *Profili giuridici del neuromarketing. Annuario 2023-2024 OGID. Osservatorio Giuridico sull'Innovazione Digitale*, Roma, 2025, 148.

[38] Sul tema, si rimanda a F. Di Gianni, *Protezione dei minori vs tutela dei dati personali: profili*

Ciò detto, a livello nazionale come viene tutelata l'immagine e l'identità del minore nei meandri del web? Nel contesto italiano, il tema della protezione del minore dai rischi del *web* si è delineata prevalentemente lungo le direttrici del contrasto alla pedopornografia e del cyberbullismo. Rispetto al primo nucleo, il d.lgs. 208/2021, il c.d. "TUSMA", ha recepito la direttiva (UE) 2018/1808 (c.d. "Direttiva SMAV") la quale ha modificato la precedente direttiva (UE) 2010/13 sui servizi media audiovisivi. Il TUSMA risponde all'esigenza (anche) del diritto delle telecomunicazioni di dotarsi di una normativa quanto più possibile al passo col progresso tecnologico e con la crescita esponenziale di *devices*»[39]. L'art. 37 contiene, al punto primo, disposizioni a tutela dei minori nella programmazione audiovisiva, sancendo come regola generale il divieto di «trasmissioni televisive gravemente nocive allo sviluppo fisico, psichico o morale dei minori, e, in particolare, i programmi che presentano scene di violenza gratuita o insistita o efferata ovvero scene pornografiche». Tali contenuti non vengono vietati *in absoluto*, ma la loro accessibilità deve essere limitata attraverso sistemi di controllo parentale e comunque al di fuori di quelle che sono individuate come fasce protette (art. 37, p. 3). Nemmeno il TUSMA è immune dalle criticità – lo si può dire – endemiche di quegli interventi (siano essi di *soft law* o di *hard law*) che tentano di dare una disciplina ad una materia che, per definizione, soffre le maglie della perimetrazione e della definizione normativa. L'individuazione di fasce protette e i meccanismi di filtraggio dei contenuti possono essere facilmente elusi dall'utilizzo di servizi di *streaming* e di accessi *on demand*, così come, del resto, lo stesso *parental control*. Un discorso a parte, che può solo presentarsi, meriterebbe la nozione di "contenuto nocivo" il cui contenuto vago ed indefinito non può che prestare il fianco ad interpretazioni difformi e applicazioni disomogenee.

Il richiamo ai contenuti pornografici è ripreso anche dalla l. 238/2021, in vigore dal 17 gennaio 2022, recante "Disposizioni per l'adempimento degli obblighi derivanti dall'adesione dell'Italia all'Unione Europea - Legge Europea 2019-2020". Il provvedimento in parola ha contribuito ad ampliare la tutela della personalità individuale delle persone minori d'età, introducendo nuove fattispecie delittuose e circostanze aggravanti, in particolare per l'adescamento dei minori (il c.d. "*Child grooming*") a mezzo *internet* e simili. L'art. 20 di questa legge modifica alcune norme in tema di repressione degli abusi sessuali ai danni dei minori e contro la pedoporno-

critici della proposta di regolamento sulla prevenzione e la lotta contro l'abuso sessuale sui minori online, in *Ordine internazionale e dirtti umani*, 2023, 838 ss.

[39] Così V. Franceschelli, *Diritto delle comunicazioni. Studi e capitoli*, Milano, 2022, 258. Per uno sguardo più approfondito rispetto alla riforma del Testo Unico dei Servizi Media Audiovisivi in relazione alla protezione dei minorenni, si rinvia a L. Musselli, *Prospettive di tutela dei minori nella «Over-the-top television» dopo la riforma del T.U. Servizi Media Audiovisivi*, in *Il Diritto dell'Informazione e dell'Informatica*, 2012, 805 ss.

grafia, adeguando la legislazione italiana alla normativa CSAM. Una delle novità più rilevanti è senza dubbio la previsione del delitto di accesso a materiale pedopornografico introdotto nell'art. 600 *quater*, c. 2, c.p. Con tale aggiunta il legislatore italiano ha provveduto ad adeguare la risposta sanzionatoria– oltre ad evitare una procedura d'infrazione - alla previsione di cui all'art. 5, par. 3, della direttiva (UE) 2011/92 – unitamente al Considerando 18 della stessa - , la quale, nell'indicare i reati di pornografia minorile, dispone che gli Stati membri adottino le misure necessarie affinché sia punita, con una pena detentiva massima di almeno un anno, la condotta, intenzionale e non giustificata, di accesso consapevole, a mezzo di tecnologie dell'informazione e della comunicazione, a materiale pedopornografico. Inoltre, l'art. 20 della legge europea ha introdotto nel contesto normativo del Capo III, Titolo XII ulteriori circostanze aggravanti volte a dare attuazione all'art. 9 della direttiva[40].

L'ultimo provvedimento nazionale che va menzionato sulla tutela specifica dell'identità e dell'immagine del minore è il d.l.123/2023 ("Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile nonché per la sicurezza dei minori in ambito digitale") convertito in legge n. 159/2023, conosciuto come "Decreto Caivano". Tra le novità digitali vi sono l'obbligo per i fornitori di servizi di comunicazione di offrire strumenti di controllo parentale gratuiti, e la previsione che i nuovi dispositivi debbano pre-installare tali applicazioni. A questo proposito l'art. 13 chiarisce che tali strumenti debbano agevolare, appunto, il controllo parentale inteso come potere (e, diremmo noi, dovere) degli esercenti responsabilità genitoriale di limitare e financo vietare l'accesso ai contenuti *web* e/o alla rete *tour court*. Il decreto Caivano sottolinea altresì la responsabilità dei produttori di fornire dispositivi che consentano l'installazione di default di sistemi di *parental control*. La linea, dunque, pedagogico-giuridica che pare perseguire il provvedimento in parola è protesa a sensibilizzare sull'urgenza di un'alfabetizzazione digitale[41]. Senza entrare nel merito delle scelte di politica criminale del provvedimento in parola, lascia, invero, un po' perplessi che il dovere di sensibilizzare i fruitori – per la maggior parte, più giovani – di servizi digitali venga di fatto rimesso in capo agli stessi erogatori di tali di servizi.

Al fine di dare attuazione ai contenuti e alle finalità sulla protezione digitale delle persone minori d'età previste dal decreto Caivano, l'Autorità per le garanzie nelle comunicazioni (AGCOM) ha approvato, con la delibera

[40] Per una disamina più completa si rimanda a F. Costantini, *Le modifiche al codice penale introdotte dalla l. 238/2021 (c.d. Legge Europea) in materia di contrasto allo sfruttamento sessuale dei minori e della pedopornografia*, in *Sistema Penale*, 2024.

[41] Cfr. B. Agostinelli, *Autonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale*, cit., 425.

n. 96/25/CONS, le nuove modalità che le piattaforme di *video sharing* e i siti *web* devono adottare per verificare la maggiore età degli utenti. Il provvedimento definisce le modalità tecniche con le quali soggetti terzi ed indipendenti dovranno garantire una verifica affidabile della maggiore età (c.d. "*age verificatio*n") degli utenti che accedono a contenuti ritenuti potenzialmente inadeguati per i minori. Il coinvolgimento di soggetti terzi e verificati è motivato dalla procedura tecnica prevista per l'*age assurance* che prevede un inevitabile trattamento dei dati personali con i rischi di gestioni improprie da parte dei gestori delle piattaforme; invece, gli intermediari verificati a cui viene demandata la procedura di verifica dell'età, non hanno modo di conoscere l'identità della piattaforma a cui il soggetto sta accedendo. La delibera dell'AGCOM si concentra prevalentemente sui sistemi di *age verification* senza però occuparsi direttamente del c.d. "*parental control*", ossia di quei strumenti di "filtro" nella navigazione nel *web*, che consentono un monitoraggio dei contenuti visionabili nei dispositivi ad uso dei soggetti più esposti ai rischi dei suddetti, come sono le persone minori d'età. Va detto che per quanto riguarda la situazione nazionale, con la delibera AGCOM 9/23 CONS del 2023, dopo consultazione pubblica con i principali operatori ed associazioni di categoria, sono state emanate delle linee guida in materia di "protezione dei minori dai rischi del cyberspazio", dando così attuazione all'art. 7 *bis* del d.l. 28/2020 in base al quale «I contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice di cui al decreto legislativo 1° agosto 2003, n. 259, devono prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto» (c. 1). Come è stato notato, i sistemi di *parental control* non sono dei meri accorgimenti tecnici ma vanno visti più ampliamente come una «vera e propria "sottovoce" dell'educazione»[42], sicché un provvedimento di controllo dell'accesso del minore all'ambiente digitale non può disgiungere, pena una parziarietà regolamentativa e, dunque, di efficacia di tutela, i sistemi di verifica dell'età con una più diretta implementazione dei sistemi di *parental control*, quale binomio imprescindibile di alfabetizzazione ed educazione digitale.

Il quadro sin ora presentato, lungi dall'avere pretese di esaustività, ha in qualche modo tratteggiato il fronte normativo sovranazionale e nazionale in tema di protezione dell'identità e dell'immagine del minore nel contesto digitalizzato. L'altro fronte, lo si è anticipato, riguarda il modo in cui la normativa comunitaria e italiana regolamentano la questione cruciale dell'autodeterminazione delle persone di minore età all'interno dello spazio informatico.

Il quadro normativo di riferimento per il tema individuato è il Regola-

[42] Ivi, 424.

mento europeo per la protezione dei dati (Reg. UE 2016/679), meglio noto come GDPR. In particolare, per il tema de quo, il provvedimento in parola nell'occuparsi specificatamente della capacità del minore di prestare il proprio consenso, supera la lacuna normativa della precedente normativa, ossia l'abrogata direttiva (UE) 1995/46/CE, giacché il tema dell'autodeterminazione digitale delle persone minori d'età è un tema non più differibile né tanto meno eludibile. In via generale, il GDPR intende il consenso come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento» (art. 4). Chiaramente, la disciplina generale del consenso esige una declinazione minorilistica, atta a controbilanciare la possibilità riconosciuta alla persona minore d'età di prestare il proprio consenso e, dunque, di acconsentire a ciò che la manifestazione di volontà manifestata può comportare in termino di accesso ai propri dati, con le esigenze di tutela rafforzata propria dei minori. Di ciò, il *Recital* (Considerando) 38 pare averne contezza quando afferma *«Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data»*. L'esigenza di apprestare una specifica protezione ai minori è presente – prima di vedere il cuore del GDPR – anche al *Recital* 58 ove si legge «*Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand»*. Il tema della "*specific protection*", ritornante in entrambe i Considerando e basamento sulla quale il GDPR articola la disciplina minorilistica della protezione dei dati personali, delinea la persona minore d'età come un soggetto a cui l'ordinamento giuridico – in questo caso eurounitario – riconosce un protagonismo all'interno del contesto virtuale; proprio per ciò l'attribuita titolarità di diritti particolari esercitabili in una dimensione il cui controllo è, per le ragioni più volte menzionate, demandato a strumenti normativi che faticano non poco a stare al passo con il progresso informatico, sicché bambini e ragazzi, sono particolarmente protetti in ragione della loro vulnerbailità ma non per questo «aprioristicamente limitati nell'esercizio dei diritti medesimi, vale a dire nel potere di autodeterminazione, in ragione della minore età»[43]. *Au contraire*, il GDPR delinea il consenso digitale manifestabile dalle persone di minore età attraverso previsioni dal contenuto specifico che tratteggiano uno scenario di ampio respiro e, si può dire, di riconosciuta responsabilità al minore che frequenta l'ecosistema del *web*. Fra le novità più rimarchevoli apportate dal GDPR figura la previsione

[43] C. Camardi, *Minore e privacy nel contesto delle relazioni familiari,* in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, cit., 123.

della soglia di età minima fissata dal legislatore europeo per poter esercitare autonomamente il consenso al trattamento dei dati personali. In particolare, l'art. 8 prevede che «*in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years*». Sebbene in questa sede – deputata ad uno sguardo di sintesi sul tema – non sia possibile dare adeguatamente conto di una certa ambiguità dell'espressione "*information society services*" vale la pena fare un appunto, relativamente al citato Considerando 38. Quest'ultimo, riportando l'esigenza di apprestare una particolare protezione ai "*personal data*" dei minori, delinea, con un'espressione appunto ampia, un contesto di tutela ampio e generale; volendo tracciare un parallelismo con il *best interest of the child*, possiamo dire che nel GDPR il Considerando 38 non solo afferma un obiettivo e pone un limite all'attività delle piattaforme digitali, ma lascia intravedere un preciso criterio ermeneutico con il quale leggere le fattispecie che hanno ad oggetto il rapporto tra la persona minore d'età nello spazio digitiale, ogni qualvolta – e di fatto, in praticamente ogni situazione – vi sia il rischio di intrusione nella sfera dei dati personali di questi ultimi. Si tratta, dunque, di un "*favor minoris*"[44] che, vista la portata del GDPR, non pare circoscrivibile solo al suddetto documento ma possa estendersi alla normativa (sia essa di *soft* o *hard law*) *in subiecta materia*. L'art. 8 del GDPR, invece, riferendosi solamente all'offerta di servizi delle società d'informazioni, ha indubbiamente un ambito di applicazione più limitato. A ciò va aggiunto che esso riguarda solo l'ipotesi in cui il trattamento dei dati necessari per fornire od offrire il servizio si fondi unicamente sulla base della legittimazione fornita dal consenso dell'interessato (*ex* art. 6, par.1, lett. a). In ragione di ciò non si può che convenire con chi, tirando le somme a proposito dell'impianto previsto dall'art. 8, osserva che il suddetto «non garantisce affatto ai minori una maggiore tutela di portata in generale rispetto al trattamento dei dati personali che li riguardano o anche solo rispetto ai dati utilizzati ai fini di marketing o di profilazione dell'utente o della raccolta per qualunque tipo di "servizi offerti ai minori"»[45]. L'introduzione della possibilità per l'infrasedicenne di prestare il proprio consenso in forma digitale, abbassando, così, la soglia legale della maggiore età, depone per una visione del

[44] D. Cacioppo, *Sharenting e tutela dei dati personali del minore: profili giuridici di un fenomeno interdisciplinare,* cit., 390.

[45] Così e, in generale, più diffusamente sulle criticità di sistema dell'art. 8 del GDPR, F. Pizzetti (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021, 105 ss.

legislatore comunitario – come altresì visto nei documenti di *soft law* sovra esaminati – protesa verso la concessione a ragazzi e ragazze non solo di una maggiore autonomia ma anche, e primariamente, di riconoscere loro quella capacità di discernimento tale per cui essi sono in grado di autodeterminarsi in merito ad un aspetto così delicato com'è quello della *privacy*. Chiaramente, il riconosciuto valore del consenso prestato dall'ultrasedicenne non deve essere inteso aprioristicamente come una garanzia "magica" dell'acquisita capacità di ragazzi e ragazze di proteggersi dai rischi del *web* e nemmeno dalla contezza di poter esercitare in questa dimensione i propri diritti e quali siano, infine, i contenuti degli stessi. Infatti, come giustamente nota Senigaglia, la condizione di strutturale vulnerabilità del minore, si sostanzia proprio nella «non piena consapevolezza dei propri diritti e dei rischi, sovente subdoli, che li minacciano nelle vie del web»[46].
L'art. 8, si è visto, rimanda agli Stati membri la possibilità di fissare una soglia d'età minima per il consenso, inferiore agli anni 16 ma non inferiore agli anni 13. ll Legislatore nostrano ha scelto, con l'art. 2 *quinquies* del d.lgs. 196/2003 (il c.d. "Codice della *privacy*", come modificato dal d.lgs. 101/2018) di portare a 14 anni l'età minima per il consenso digitale e ha esplicitato l'accessibilità, la comprensibilità e la chiarezza che devono caratterizzare il linguaggio dell'informativa predisposta dal titolare dell'offerta del minore, dando così attuazione alla previsione del già richiamato Considerando 58 del GDPR. Per quanto riguarda l'infraquattordicenne, il consenso è lecito a condizione che sia prestato dall'esercente responsabilità genitoriale.
Al di là dell'abbassamento dell'età prevista dalla normativa interna, il tema è foriero di considerazioni le quali si debbono tracciare in un'ottica interdisciplinare, giacché solo l'attivazione delle altre scienze (dalla psicologia, alla pedagogia sino alla filosofia) rende ragione della complessità del tema e solo l'intarsio di riflessioni provenienti da plurimi campi, può fornire al giurista gli strumenti per disciplinare un quadro protettivo e promotivo i diritti del minore in ambito digitale. Se allo psicologo competono *in primis* le riflessioni circa la maturità del minore ad esprimere il consenso sulla base di elementi interni ed esterni a lui, il giurista è innanzitutto chiamato a chiedersi se, in ottica di protezione e valorizzazione del *best interest of the child*, il consenso sia effettivamente lo strumento più adatto a proteggere gli interessi del minore, stante la natura "bifronte", caratterizzata, cioè, da elementi patrimoniali e non patrimoniali, del diritto al trattamento dei dati personali[47]. Allargando la questione, limitatamente come rinvio, la riconosciuta capacità di prestare il consenso al trattamento dei dati personali

[46] R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, cit., 518.

[47] Sul tema, si veda M. Bianca, *Il minore e i nuovi media*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, cit., 156 ss.

mette in discussione la già attualmente critica nozione civilistica della capacità d'agire, rispetto alla quale la previsione del GDPR e, *a fortiori*, del Codice della *Privacy* che prevedono una soglia più bassa della maggiore età, spingono ulteriormente a rivedere un retaggio giuridico non più in linea non solo con l'accresciuta capacità delle persone minori d'età di comprendere il significato anche giuridico delle proprie azioni ma anche con le tendenze comunitaria che protendono per un centralismo del minore e della sua capacità di autodeterminarsi[48].

Sebbene non si tratti di un atto normativo, per la sua importanza va almeno richiamato in questa sede anche il Libro Bianco "Media e Minori", nella sua versione più recente, ossia la "2.0" del 2018, aggiornamento del Libro Bianco "Media e Minori" del 2013, a firma dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM). La necessità di rivedere a distanza di un tempo relativamente breve il Libro Bianco è sintomatica dell'ipercinesi del mondo digitale e dell'urgenza indifferibile di una sua regolamentazione, soprattutto per tutelare i più giovani. Il testo[49], nelle sue battute iniziali, parte dal condivisibile assunto che «Il minore da tutelare è un soggetto tecnologicamente esperto e dotato di uno strumentario tecnologico personale – cellulare, PC, webcam, smartphone, tablet - che autogestisce e utilizza nell'intero arco della giornata...». Molti sono i temi, le problematizzazioni e feconde le sfide che il Libro Bianco tratteggia nell'era dei nativi digitali. In questo percorso, si legge in più punti, il ruolo attoriale non possono che svolgerlo i genitori, in ragione del fatto che «l'ambiente domestico è comunque per i minori il principale spazio di accesso ad Internet, e ciò sottolinea l'importanza del ruolo delle figure genitoriali nella modulazione delle pratiche digitali dei figli»[50]. Indubbiamente senza un apparato giuridico di protezione, gli stessi adulti si trovano sguarniti di opportuni strumenti operativi per esercitare i doveri di cura e protezione (anche) in campo digitale.

Il quadro normativo, sovranazionale e nazionale, sinteticamente enucleato, delinea un'attenzione affannosa del legislatore nel tentativo di stare al passo col progresso tecnologico e coi possibili rischi, soprattutto in tema di *privacy* e di esposizione dell'immagine del minore la quale veleggia spesso incontrollata per i meandri del *web*, senza che, sovente, gli adulti di riferimento ne abbiano contezza. Cosa accade, però, quando sono proprio i genitori, coloro i quali sono deputati a proteggere i figli dai rischi del web, ad essere i responsabili (*rectius*: irresponsabili) dell'esposizione digitale di quest'ultimi? Èil caso dello *sharenting* il quale si staglia a "caso serio" per

[48] Cfr. R. Senigaglia, *The best interest of the child tra persona e contratto*, in M.. Bianca (a cura di), T*he best interest of the child,* Roma, 2021, 491 ss.

[49] Il testo è consultabile al sito *astrid-online.it*.

[50] Libro Bianco "Media e Minori" 2.0., 1.2.1.

il diritto minorile, giacché apre a più approfondite riflessioni in tema di responsabilità genitoriale ma si staglia altresì a paradigma sociologico di un'adultità fragile, per certi versi immatura rispetto ad un progresso tecnologico che pone sfide radicali alla competenza genitoriali, la cui elusione si rivelerebbe nociva proprio per i figli e per il loro *best interest*[51].

4. Il figlio è mio e lo posto io...! Il "caso serio" dello *sharenting* tra *best interest of the child* ed esercizio della responsabilità genitoriale

Le riflessioni sin qui condotte a partire dal "diritto-guida" del superiore interesse del minore permettono di condurre un'indagine più consapevole su di un tema strettamente collegato a quello che concerne il diritto delle persone di minore età alla tutela dei propri dati personali in relazione alla di loro diffusione all'interno del web. La questione è appunto quella dei limiti al diritto dei genitori di pubblicare immagini dei figli minori, *a fortiori* se si tratta di pubblicarle in spazi virtuali accessibili al grande pubblico, come sono i *social networks*[52]. Come già accennato, il fenomeno dello *sharenting* appare emblematico di un'evoluzione (o involuzione?) dello stesso esercizio della genitorialità, ridefinendo il paradigma del munus genitoriale, che si estrinseca nei doveri di cura e protezione (anche) della *privacy* dei propri figli. Allorché siano gli stessi genitori a postare le foto della prole, si assiste ad un rovesciamento in cui non solo la distinzione tra immagine pubblica e privata sembra scolorire ma lo stesso concetto di *privacy* «nel virtuale appare profondamente mutato, in primo luogo, grazie all'affermazione dei social network che sviluppano e consolidano l'abitudine di esporre le emozioni e i ricordi più intimi in cambio di visualizzazioni e like, alimentando un "narcisismo 2.0" che coinvolge anche i più piccoli...»[53]. Si tratta di interrogarsi radicalmente sulla capacità dei genitori di riflettere sul fatto che l'esercizio della responsabilità genitoriale va esteso anche al mondo virtuale e le cautele che esso impone non possono essere ignorate e qualora lo siano, si tratta altresì di indagare sotto il profilo rimediale quale sia la risposta più adatta. In queste situazioni l'adulto pare scordarsi di adottare le stesse accortezze che metterebbe in atto nel mondo fisico allorché, ad esempio, un perfetto sconosciuto chiedesse a mamma o papà

[51] Cfr. D. Cino - S. Demozzi, *Figli "in vetrina". Il fenomeno dello sharenting in un'indagine esplorativa,* cit.*,* 158

[52] Cfr. F. Scia, *Diritti dei minori e responsabilità dei genitori nell'era digitale*, Napoli, 2020, 52 ss.

[53] A. Maceratini, *Sharenting e tutela dei minori, riflessioni informatico-giuridiche tra diritto alla privacy e diritto all'immagine*, in *Tigor: rivista di scienze della comunicazione e di argomentazione giuridica*, A. XVI, 1, 2024, 122.

se può fare una foto alla di loro figlia o al di loro figlio. Se in tali occasioni si può azzardare a dire che alcun genitore acconsentirebbe ad una richiesta di tal guisa, è d'uopo un lavoro di alfabetizzazione digitale ma anche di "alfabetizzazione genitoriale 2.0" per far capire che i rischi della sovraesposizione dei minori in campo digitale è ancora maggiore[54]; considerando poi il fatto che le immagini circolano incontrollatamente e si depositano nel *web* (o nel *dark web*) si conviene con chi osserva che «*Parents post images of their children online with little comprehension or regard for the fact that they are crafting their children's online footprint and compromising their private identity along with interfering with the child's right to digital self-actualisation. Arguably, parents are sacrificing their children's privacy in return for their own positive online connectivity*»[55].
Lo scenario a cui il giurista deve prestare attenzione non è dunque dei più semplici sia per il fatto che è intrinsecamente in evoluzione, sia per il fatto che in Italia, sul piano normativo, non esiste ancora una specifica legge riguardante la condivisione *on-line* di materiali digitali dei figli minorenni, facendosi, infatti, rimando alle regole in materia di *privacy*, di tutela dell'immagine, ai doveri genitoriali di cura, protezione ed educazione della prole sino, nei casi più gravi, ai reati connessi alla pedopornografia. La giurisprudenza, dal canto proprio, si è trovata in diverse occasioni ad occuparsi di casi si *sharenting*, tuttavia, in maniera incidentale nell'affrontare altre questioni. Il punto non è da sottovalutare, come si avrà modo di sostenere.
Il Tribunale di Mantova con ordinanza del 17 settembre 2017 si è occupato dell'inserimento di foto di figli minori sui *social network* nonostante l'opposizione di un genitore, stabilendo che detto comportamento – in questo caso della madre la quale ha agito senza il consenso del padre della figlia minore - integra violazione della norma di cui all'art. 10 c.c. (concernente la tutela dell'immagine), del combinato disposto degli artt. 4,7,8 e 145 del d. lgs. 196/2003, nonché degli artt. 1 e 16 I co. della Convenzione di New York dell'89. Il contenuto dell'ordinanza del Tribunale di Mantova si fa più pregnante allorquando riconosce che «l'inserimento di foto di minori sui social network costituisce comportamento potenzialmente pregiudizievole per essi in quanto ciò determina la diffusione delle immagini fra un numero indeterminato di persone...» e, per i rischi a cui vengono esposti i minori, si deve concludere che «il pregiudizio per il minore è dunque insito nella diffusione della sua immagine sui social network»[56]. L'ordinanza

[54] Sul punto, A. Martorana - R. Savella, *L'utilizzo degli strumenti digitali da parte dei minori tra opportunità e rischi,* in A. Martorana - G. Guadagnini (a cura di), *Tutela del minore nella società digitalizzata,* cit., 25.

[55] S. Donovan, '*"Sharenting": The Forgotten Children of the GDPR,* cit., 42.

[56] In questo caso, il Tribunale di Mantova non solo ha ordinato la rimozione delle foto pubblicate senza consenso del padre della figlia minore, vietandone ulteriori pubblicazioni ma ha altresì disposto l'attivazione della Tutela Minori al fine di approfondire la situazione

porta in rilievo due questioni che paiono essere le due tipologie di lenti con le quali la giurisprudenza si è occupata del fenomeno dello *sharenting*. La prima questione riguarda la pubblicazione dell'immagine del figlio minore senza il consenso espresso di entrambi i genitori. In tempi recenti il Garante per la protezione dei dati personali con il provvedimento 13 novembre 2024, n. 681 ha chiarito che la pubblicazione di immagini e fotografie ritraenti soggetti minori di quattordici anni richiede necessariamente il preventivo ed esplicito consenso di entrambi i genitori, ai sensi dell'art. 320 c.c., in quanto il trattamento dei dati personali del figlio minorenne è atto di straordinaria amministrazione – avendo ad oggetto un diritto della persona annoverabile tra i c.d. diritti "limitatamente disponibili" - e pertanto necessita del comune accordo dei genitori[57]. La seconda questione riguarda più specificatamente il tema dello *sharenting* e i rischi ad esso connesso, che la citata ordinanza del Tribunale di Mantova menziona esplicitamente, specie nella sua forma più odiosa, ossia la circolazione di materiale pedopornografico. L'ordinanza è particolarmente preziosa proprio per l'attenzione che dedica a questo punto: enunciando come principio generale la necessità di proteggere i minori dai rischi del *web*, stigmatizzando il comportamento del genitore non solo nella parte in cui viola l'accordo di non pubblicazione ma proprio nei rischi della pubblicazione in sé, si sta affermando implicitamente che il *best interest of the child* è il diritto ad essere salvaguardato dalle ingerenze che la pubblicazione della sua immagine e/o altri dati personali nel *web* possono cagionare e tale diritto ha dei precisi riferimenti normativi sia sovranazionali che nazionali, sia di rango ordinario che di rango costituzionale.

L'ordinanza del Tribunale di Mantova non è un caso isolato. Il Tribunale di Rieti con sentenza del 7 marzo 2019, richiamandosi esplicitamente alla Convenzione di New York dell'89, rimarca la subordinazione della pubblicazione dell'immagine del minore al consenso espresso da entrambi gli esercenti responsabilità genitoriale[58]. Nel caso specifico il Tribunale ha condannato la nuova compagna del padre al pagamento di 50 euro per ogni giorno di ritardo nella rimozione delle immagini pubblicate o per ogni pubblicazione successiva non autorizzata, stabilendo quindi che il divieto di pubblicare sul *web* immagini dei figli minori vale anche nel caso in cui a postarle sia il/la nuovo/a compagno/a di uno dei due coniugi,

familiare, mediante valutazione delle capacità genitoriali dei genitori.

[57] *Funditus*, sulla questione della necessità o meno del consenso di entrambi i genitori per la pubblicazione delle foto dei figli minori si rimanda a G. Magliano, *Quando il minore deve essere social: il consenso alla pubblicazione di una foto di un minore su un social network da parte dei genitori*, in *Filodiritto*, 5 dicembre 2016.

[58] Cfr. A. Maceratini, *Sharenting e tutela dei minori, riflessioni informatico-giuridiche tra diritto alla privacy e diritto all'immagine,* cit., 126.

quando manca il consenso dell'altro soggetto che esercita la responsabilità genitoriale.
Sempre nel 2019 va menzionata la sentenza n. 1038/2019 del Tribunale di Ravenna che conferma il fatto che non è sufficiente il consenso di un solo genitore per autorizzare la pubblicazione sul *web* di foto dei figli minorenni, anche se si tratta di coniugi separati e se i figli sono in regime di affido condiviso. Il caso riguardava la partecipazione di una bambina di 3 anni ad un evento in cui compariva in costume da bagno a cui ha fatto seguito la pubblicazione delle foto della figlia su Facebook da parte della madre senza l'espresso consenso del padre.
Anche il Tribunale di Trani si è occupato di un caso di *sharenting*, rimarcando con ordinanza del 30 agosto 2021 la necessità del consenso di entrambi i genitori per pubblicare – in questo caso sul social *TikTok* – le foto della figlia minore, ordinando altresì la rimozione delle stesse. La pronuncia merita attenzione perché riprende testualmente quanto espresso dal Tribunale di Mantova nel 2017, proprio nella parte in cui mette in guardia dai rischi derivanti dalla diffusione di immagini di minori nel mare *magnum* del *web*.
Sempre il Tribunale di Rieti, con sentenza n. 443 del 15 ottobre 2022 ha ribadito che la pubblicazione non autorizzata di fotografie e video ritraenti minori sui *social network* costituisce fatto illecito ex art. 2043 c.c. e comporta il risarcimento del danno non patrimoniale ex art. 2059 c.c. qualora manchi il consenso espresso di entrambi i genitori esercenti la responsabilità genitoriale. Il diritto all'immagine del minore, rientrando tra i diritti inviolabili della persona tutelati dall'art. 2 Cost. e configurandosi come proiezione del diritto alla *privacy*, richiede per il suo trattamento il preventivo consenso di entrambi i genitori ai sensi dell'art. 320 c.c., trattandosi di atto eccedente l'ordinaria amministrazione avente ad oggetto dati personali sensibili. Anche in questo caso il giudice, dopo aver citato la normativa sovranazionale e nazionale in tema di protezione dei dati personali dei minori, accenna alla «diffusività della condotta lesiva» a ragione della «accessibilità alle foto da parte di una platea potenzialmente sterminata, quale è quella costituita dagli utenti di Facebook»; in questo caso, peraltro, il numero di foto era consistente (ben 52) e ritraevano altresì la minore in costume da bagno.
Sotto un diverso profilo, invece, il Tribunale di Roma con ordinanza del 23 dicembre 2017 (procedimento n. 39913/2015) ha accolto la richiesta pervenuta dal diretto interessato, un minorenne di anni 16, il quale ha chiesto l'immediata cessazione da parte della madre nei *social networks*, di immagini, notizie e altri dettagli relativi alla sua vita privata nonché ad una vicenda giudiziaria che lo coinvolgeva. Il Tribunale, oltre a ordinare la rimozione dei contenuti, disponeva d'ufficio nei confronti della madre, ai sensi dell'art.614 *bis* c.p.c, la corresponsione di una somma di denaro nei confronti del figlio in caso di mancata ottemperanza agli obblighi (c.d *astreintes* o penalità di mora). Il tribunale capitolino, richiamandosi alla legi-

slazione ma anche alla giurisprudenza di Cassazione in materia di ascolto, sottolinea che «in considerazione dell'età del minore (16 anni) deve essere evidenziata l'elevata rilevanza che assume la volontà dello stesso» e che tale volontà del minore depone per la rimozione di contenuti virtuali che possano in qualche modo danneggiarlo nel nuovo contesto di vita nonché per la futura cessazione degli stessi.

Quest'ultima pronuncia, proprio perché riguarda un ragazzo di 16 anni, menziona in più occasioni il diritto al superiore interesse del minore. Alla luce delle pronunce citate, è il momento di svolgere alcune considerazioni proprio alla luce del *best intereest of the child*. Come già anticipato, la maggior parte delle situazioni in cui emerge il tema dello *sharenting* originano in seno a controversie familiari Sebbene ci siano casi "virtuosi" come quello del Tribunale di Mantova o quello di Trani in cui il tema della pubblicazione di persone minori d'età sui *social networks* e/o altre piattaforme digitali a diffusione incontrollata emerge direttamente, come questione rilevante *in re ipsa*, in altre situazioni – e sono la maggior parte - il "caso serio" dello *sharenting* emerge subordinatamente alla questione del comportamento illecito del genitore che pubblica senza il consenso dell'altro; in tal modo il tema dei rischi connessi alla sovraesposizione digitale dei minori non emerge in sé ma con ruolo ancillare rispetto al tema del consenso. Si condivide pertanto l'acuta osservazione di chi mette in dubbio «la linearità dell'argomentazione più ricorrente, indicativa, infatti, di una certa sovrapposizione di piani: se il pregiudizio per il minore è insito nella diffusione della sua immagine sui social network […] il consenso di entrambi (e non già di uno solo) alla pubblicazione non potrebbe valere e bastare a scongiurarlo»[59]. A siffatta notazione ne va aggiunta un'altra. Il rischio che corre un certo *iter* argomentativo rinvenibile in casi giurisprudenziali in cui lo *sharenting* appaia in subordine rispetto alle violazioni delle regole del consenso è di assorbire una questione come quella della tutela dell'immagine del minore, avente fondamento e valore costituzionale, all'interno, appunto, della regolamentazione civilistica sul consenso sugli atti che riguardano i minori (art. 320 c.c.) e di abuso del diritto di immagine (art. 96 e 97, l. 633/1941).

Come adombrato, il tema dello *sharenting* è ontologicamente connesso con quello della genitorialità e del suo esercizio. Sotto la lente del giurista, quest'inversione del paradigma della cura e della protezione, sicché è colui il quale è deputato a proteggere ad essere l'autore della pericolosa esposizione, impone un ragionamento anche sotto il profilo sanzionatorio. La natura "fondamentale", infatti, dei diritti coinvolti esige l'applicazione di strumenti di tutela che trovino la loro giustificazione tanto nel rango

[59] Così osserva B. Agostinelli, *Autonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale*, cit., 427.

primario delle situazioni protette, quanto nella più volte osservata inadeguatezza dei rimedi civilistici ad offrire un'effettiva tutela al fenomeno dello *sharening*. Dalle pronunce sovra esaminate, gli strumenti rimediali e sanzionatori attivati sono quelli dell'azione inibitoria ex art. 10 c.c., volta ad ottenere un ordine giudiziale, anche in via cautelare (*ex* art. 700 c.p.c.) al fine di impedire o far cessare la condotta illecita; tale rimedio assicura una protezione di carattere preventivo e specifico anche «suscettibile di cumularsi con il rimedio della cancellazione dei dati personali (art.17 GDPR), allo scopo di reagire contro l'illecito impedendone la continuazione»[60]. Alla tutela offerta dall'azione inibitoria si affianca il ruolo offerto dal risarcimento del danno non patrimoniale per lesione del diritto d'immagine (art. 2059 c.c., art. 10 c.c.). Infine, un importante strumento processuale volto a far cessare la diffusione di immagini di minori sui *social* è costituito dal ricorso *ex* art. 473-*bis* 39 c.p.c. In caso di gravi inadempienze o comunque di atti che arrechino pregiudizio al minore, il giudice può modificare i provvedimenti in vigore e, oltre ad ammonire il genitore inadempiente, può anche condannarlo ad un risarcimento del danno in favore del minore o dell'altro genitore.

La pericolosità insita nella diffusione delle immagini di persone minori d'età da parte dei genitori ed esercenti responsabilità genitoriale suggerisce invero una lettura che conduca la questione all'interno dei doveri di cura, protezione ed educazione riconosciuti sui genitori ma anche gravanti sugli stessi. Non c'è dubbio che l'indiscriminato accesso ad immagini, foto e video di minorenni costituisca, come rilevato da un'attenta parte della giurisprudenza menzionata, un pericolo in sé sicché andranno seriamente valutati i confini dell'applicazione di provvedimenti incidenti sulla responsabilità genitoriale (*ex* art. 330 e ss.). Poiché non possono ignorarsi i rischi insiti nella diffusione incontrollata di tutto ciò che può essere direttamente ricondotto alla persona minorenne in termini di identificabilità, la questione non può essere decentrata o assorbita in altre, come, appunto, quella del consenso e difatti «che detto consenso […] integri una forma di esercizio di responsabilità genitoriale *ex* art. 316 c.c., è lecito dubitare, poiché non si tratta di agire nell'interesse del figlio ma, semmai, in quello (futile e) egoistico di rendere pubblici e visibili momenti di vita personale...»[61]. Si tratta invece, al fine di dare concreta attuazione al principio del *best interest of the child*, non solo di valutare caso per caso i conflitti generati – prevalentemente in senso a controversie familiari – dalla rappresentazione dell'immagine del minore nel mondo virtuale ma di trattare codeste situazioni separatamente dalle altre, con uno sguardo centrato sul soggetto di minore

[60] G. Carapezza Figlia, *Sharenting: nuovi conflitti familari e rimedi civili*, cit., 1107.

[61] Così B. Agostinelli, *Autonomia e controllo dei minori on line. I nuovi confini della responsabilità genitoriale,* cit., 428.

età e sui rischi che in cui concretamente può incorrere[62].
Già ad una lettura superficiale si colgono i limiti degli strumenti giuridici a disposizione del legislatore per dare una risposta che sia effettivamente tutelante al fenomeno dello *sharenting*. Il tema continua ad essere oggetto di dibattito – e a ciò non si può che plaudire e guardare con speranza – che ha portato tra il 2023 e il 2024 ad una serie di proposte di legge[63]. Tali proposte sono accomunate dall'obiettivo di consolidare un sistema complessivo di tutele sulla diffusione dell'immagine dei minori nonché sulla possibilità di quest'ultimi di esercitare il diritto alla cancellazione dei dati (c.d. "Diritto all'oblio") richiamandosi, peraltro, ai principi espressi anche dala Carta di Treviso. Tuttavia, ad ora, manca una precisa definizione normativa che regolamenti il fenomeno dello *sharentin*g da inquadrare, si ritiene, non nella prospettiva adultocentrica di porre un limite ai genitori di pubblicare foto dei figli sui *social* quanto nella prospettiva paidocentrica del diritto di bambini e bambine, ragazzi e ragazze a non vedere a propria insaputa o contro la propria volontà, le loro immagini diffuse nel *web*. Forse l'effettiva tutela del fenomeno dello *sharenting* parte proprio da questa rivoluzione copernicana, che fonda il proprio impianto regolamentativo sui diritti delle persone minori d'età e da qui muove e trae legittimazione per garantire il *best interest of the child*. Se si condivide l'approccio metodologico, si tratta di pensare – *de iure codendo* – a delle proposte che possano essere effettivamente tutelanti per le persone minori d'età., in linea con l'attuale normativa ed indirizzo sovranazionale e nazionale. In una delle proposte menzionate sopra (proposta di legge n. 1800/2024, "Modifiche all'articolo 37 del testo unico dei servizi di media audiovisivi, di cui al decreto legislativo 8 novembre 2021, n. 208, in materia di impiego dei minori nell'ambito delle piattaforme digitali per la condivisione di video, audio e immagini, e disposizioni concernenti il diritto del minorenne alla

[62] Vedi su questo punto G. Carapezza Figlia, *Sharenting: nuovi conflitti familari e rimedi civili*, cit., 1108.

[63] Proposta di legge n. 1771/2024, "Modifiche alla legge 17 ottobre 1967, n. 977, in materia di impiego dei minori nellpambito delle piattaforme digitali di condivisione di contenuti multimediali, nonché disposizioni sulla diffusione dell'immagine e di contenuti multimediali di minori"; proposta di legge n. 1800/2024, "Modifiche all'articolo 37 del testo unico dei servizi di media audiovisivi, di cui al decreto legislativo 8 novembre 2021, n. 208, in materia di impiego dei minori nell'ambito delle piattaforme digitali per la condivisione di video, audio e immagini, e disposizioni concernenti il diritto del minorenne alla rimozione dei dati e dei contenuti che lo riguardano dalla rete internet e dai motori di ricerca"; proposta di legge n. 1863/2024, "Disposizioni per la tutela dei bambini e degli adolescenti nell'utilizzo degli strumenti digitali"; proposta di legge n. 1217/2024, "Modifiche al codice in materia di protezione dei dati personali , di cui al decreto legislativo 30 giugno 2003, n. 196, in materia di verifica dell'età deigli utenti dei servizi di comunicazione elettronica, e altre disposizioni per la tutela dei minori nella fruizione di tali servizi".

rimozione dei dati e dei contenuti che lo riguardano dalla rete internet e dai motori di ricerca"), si ipotizza una dichiarazione scritta che i genitori (o comunque gli esercenti responsabilità genitoriale) devono firmare ed inviare all'AGCOM qualora vogliano mostrare il volto dei loro bambini sulla rete. Tale proposta non sembra, in realtà garantire un'effettiva protezione dalla sovraesposizione del minore nel mondo digitale. In linea con la fissazione dell'età per esprimere il consenso in ambito digitale (fissata, si è visto, ai 14 anni) non sembra eccessivamente severo ipotizzare che al di sotto di quest'età in cui il minore può esercitare tutta una serie di diritti rispetto all'utilizzo dei propri dati, il legislatore preveda un divieto di pubblicazione delle immagini del minore in contesti ad accesso libero, onde evitare una fruizione e financo un'appropriazione di codesti contenuti a soggetti sconosciuti. I genitori, dunque, non potrebbero disporre liberamente dell'immagine del figlio infraquattordicenne in maniera indiscriminata, ponendo dunque un limite al diritto di utilizzare l'immagine del figlio in piattaforme che non garantiscano un adeguato controllo negli accessi; al compimento degli anni 14, giacché l'ordinamenti italiano ha fissato in questa età la possibilità di prestare l'assenso al trattamento dei dati personali, la pubblicazione dovrebbe richiedere il preventivo consenso espresso del figlio minorenne alla pubblicazione. Argomentando in tal modo, pare potersi riconoscere una cittadinanza al *best interest of the child*: per l'infraquattordicenne, al quale la normativa nazionale (*ex* art. 2-*quinquies*, c. 1, d.lgs. 196/2003, modificato dal d.lgs. 101/2018) non consente di esprimere il proprio consenso al trattamento dei dati, ossia ne ammette l'immaturità in merito, alla persona minore d'età viene garantita una tutela dalla completa libertà dei genitori di pubblicare le di lui o di lei foto sui *social networks*, cosicché il diritto personalissimo e fondamentale del minore alla riservatezza dell'immagine prevalga rispetto alla possibilità di utilizzo dei genitori; per l'ultraquattordicenne l'espressa manifestazione del consenso al trattamento dei suoi dati personali dovrebbe essere altresì condizione necessaria per la pubblicazione da parte di altri delle proprie immagini, con la possibilità – questa già riconosciutagli – di agire per richiedere la cessazione della condotta a lui pregiudizievole e l'inibizione al postare ulteriori contenuti.

5. Conclusioni

Il progresso informatico sta ridefinendo molti paradigmi tra i quali quello della responsabilità genitoriale. All'atavica ricerca di un bilanciamento tra le istanze di autonomie dei figli e i doveri di protezione, cura ed educazione propri della funzione parentale, si aggiunge – con funzione disequilibrante – la spinta dei genitori a vetrinizzare la vita propria e quella della prole, con il rischio di generare un pernicioso corto circuito in chi dovrebbe saper

proteggere dai rischi dell'esterno, invece che esporre volontariamente[64]. Si tratta, dunque, di leggere lo *sharenting* come una sorta di "cartina al tornasole" di un'adultità troppo spesso auto-centrata, sovente dimentica che «*Sharenting includes a moral obligation to act with appropriate discretion and with full regard for the child's safety and well-being*»[65]. L'incalzante sviluppo tecnologico non può essere ignorato dal diritto ed urge una precisa regolamentazione dello *sharenting*, in linea con la normativa comunitaria e nazionale rispetto alla protezione dei dati personali della persona minore d'età e al consenso digitale che quest'ultimo è in grado di prestare. In sintesi, come rimarcato dal Presidente del Garante per la protezione dei dati personali, si tratta di partire dal fatto che le politiche dell'innovazione tecnologica «devono fondarsi dunque e prioritariamente su una e vera e propria pedagogia digitale, che renda anzitutto i ragazzi consci delle opportunità ma anche dei rischi cui li espone la rete, sfruttandone tutte le straordinarie risorse per essere più consapevoli, mai meno liberi»[66]. Le sfide che interpellano il giurista sono, *mutatis mutandis*, le sfide che scuotono la genitorialità nell'era digitale, chiamati entrambi ad essere attenti alle esigenze di bambini/e, ragazzi/e, alla continua ricerca di un equilibrio tra protezione e promozione, guardando sempre al *best interest of the child* quale faro guida di ogni politica normativa ma anche genitoriale. Il mondo adulto non può dunque esimersi da una prova di autoresponsabilità, quella di implementare l'alfabetizzazione digitale di grandi e piccoli, giacché la "cittadinanza digitale" è la prova che attende la famiglia in questo tempo: ai genitori il compito di stare al passo; al diritto il compito di predisporre un quadro normativo e delle politiche formative che garantiscano un consapevole e tutelante esercizio della funzione genitoriale 2.0. cosicché bambini e ragazzi esperiscano consapevolmente quanto la tecnologia avrà ogni giorno da offrire.

[64] Cfr. anche sul ruolo tecnologico nella vita genitoriale, M. Foglia, *Sharenting e riservatezza del minore in rete*, cit., 3562.

[65] S. B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, in *Emory L. J.*. 66, 839, 2017, 882.

[66] Audizione del Presidente del Garante per la protezione dei dati personali, 26 aprile 2023.

Abstract

Tra le sfide ineludibili a cui il diritto, e segnatamente quello minorile, non può sottrarsi, vi è indubbiamente la tutela del minore in ambito digitale. La sempre maggiore frequenza del mondo informatizzato da parte delle persone di minore età sta ridefinendo gli stessi paradigmi della responsabilità genitoriale, chiamata ad esercitare i doveri di cura, protezione ed educazione anche oltre il mondo fisico, appunto in quello virtuale. Nel momento in cui, però, sono gli stessi esercenti responsabilità genitoriale, ossia coloro che sono incaricati di vigilare sul comportamento e il benessere dei figli, ad esporre questi ultimi ai rischi connessi la pubblicazione di dati sensibili di soggetti più vulnerabili, si genera un corto circuito, a cui il diritto è chiamato a dare una risposta in termini di regolamentazione e tutela. È questo il "caso serio" dello *sharenting*.

Among the inescapable challenges that the law—particularly juvenile law—must confront is the protection of minors in the digital environment. The increasing presence of minors in the digital sphere is reshaping the very paradigms of parental responsibility, which is now required to fulfill its duties of care, protection, and education not only in the physical world but also in the virtual one. However, when it is the very holders of parental responsibility—those entrusted with overseeing the conduct and well-being of their children—who expose them to the risks associated with the dissemination of sensitive data concerning vulnerable individuals, a paradox arises. This normative short-circuit demands a legal response in terms of regulation and protection. This is the serious legal issue posed by the phenomenon of sharenting.

Keywords

sharenting – children's rights – best interests of the child – parental responsibility – children's digital protection

Recensioni

Recensione a V. Pezzella, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca delle fake news, degli hate speeches e dell'intelligenza artificiale*

Rebecca Bovatti

Il volume di V. Pezzella, *La diffamazione. Le nuove frontiere della responsabilità penale e civile e della tutela della privacy nell'epoca delle fake news, degli hate speeches e dell'intelligenza artificiale,* giunto alla sua terza edizione, si propone di offrire una ricostruzione sistematica e aggiornata del reato di diffamazione, con l'obbiettivo di restituirne la complessità teorica e applicativa alla luce delle più recenti evoluzioni tecnologiche e normative. Uno sforzo particolarmente apprezzabile agli occhi di chi abbia consapevolezza della natura intrinsecamente dinamica della materia, da sempre crocevia tra diritto penale, civile e costituzionale.

Pochi settori, infatti, impongono agli operatori del diritto e dell'informazione un confronto tanto articolato quanto quello relativo al bilanciamento tra diritto all'onore e alla reputazione e libertà di manifestazione del pensiero, nelle sue declinazioni del diritto di cronaca e di critica. Come ricordato dalla Corte costituzionale con ordinanza n. 132 del 2020, «il punto di equilibrio tra la libertà di "informare" e "formare" la pubblica opinione svolto dalla stampa e dai media, da un lato, e la tutela penale della reputazione individuale, dall'altro, non può essere pensato come fisso e immutabile, essendo soggetto a necessari assestamenti, tanto più alla luce della rapida evoluzione della tecnologia e dei mezzi di comunicazione verificatasi negli ultimi decenni»[1].

Il manuale si distingue per la capacità di coniugare l'analisi dei fondamenti

[1] Corte cost., ord. 9 giugno 2020 [26 giugno 2020], n. 32, par. 7.3.

tradizionali della materia con le trasformazioni indotte dalla rivoluzione digitale. Se le pronunce del 1984 sul c.d. "decalogo del giornalista" continuano a costituire un imprescindibile riferimento sistematico, esse si confrontano oggi con un contesto profondamente mutato, nel quale la carta stampata ha ceduto il passo a strumenti comunicativi caratterizzati da immediatezza e diffusività. Le statistiche giudiziarie registrano un incremento esponenziale dei casi di diffamazione mediante piattaforme digitali, da cui l'impellente necessità di dare conto dei più recenti orientamenti giurisprudenziali su quella che l'Autore definisce "diffamazione 2.0".

La prima parte del volume è così dedicata alla ricostruzione dogmatica della fattispecie, dalla forma semplice alle ipotesi aggravate. Con riferimento all'elemento oggettivo del reato, l'Autore dà conto di come l'evoluzione tecnologica abbia inciso sul concetto stesso di "presenza" della persona offesa – tradizionalmente rilevante quale elemento distintivo dall'ipotesi, oggi depenalizzata, dell'ingiuria – rispetto al quale si è progressivamente consolidata un'equiparazione tra presenza fisica e presenza virtuale, in linea con la diffusione nell'era post Covid di videoconferenze e *smartworking*.

La seconda parte offre una ricognizione puntuale delle scriminanti tipiche del diritto di cronaca, di critica e di satira, con uno sguardo attento alla giurisprudenza nazionale ed europea.

Di particolare rilievo è la terza parte, dedicata alle sfide poste dalla diffamazione online. Internet e i nuovi strumenti di comunicazione hanno moltiplicato le occasioni di lesione della reputazione, sollevando interrogativi inediti in ordine alla configurabilità del reato, all'individuazione del soggetto responsabile e alla prova dell'elemento soggettivo. Guardando ai casi portati all'attenzione dell'autorità giudiziaria, l'Autore affronta questioni di indubbia rilevanza pratica: cosa accade se si condivide su Facebook un post diffamatorio? Integra il reato di diffamazione mettere *like* a un *post* che lede l'altrui reputazione? Messaggi e *screenshot* hanno valenza probatoria? Quali sono i limiti del diritto di critica in piattaforme quali TripAdvisor?

Si tratta di un'evoluzione che investe l'intero apparato interpretativo. In tale prospettiva, l'Autore ricostruisce il dibattito dottrinale sviluppatosi attorno ai concetti di "lettore medio" e "lettore frettoloso", interrogandosi su quale tra questi possa assurgere a parametro più adeguato a valutare l'idoneità diffamatoria di una notizia diffusa in rete. Il confronto tra i due modelli riflette l'esigenza di calibrare il giudizio di offensività della comunicazione alla luce delle attuali modalità di fruizione dei contenuti digitali, caratterizzati da rapidità, sinteticità e consumo frammentato dell'informazione.

All'interno di questa terza parte, il capitolo XVI è dedicato all'Intelligenza Artificiale (*AI*) e alle più recenti iniziative legislative, tanto a livello nazionale quanto sovranazionale. In tale contesto si colloca la legge 10 otto-

bre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", adottata in attuazione del Regolamento (UE) 2024/1689 (*AI Act*) quanto ai profili rimessi alla competenza degli Stati membri. Come recita l'art. 1, lo scopo della legge è promuovere «un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale» volto a coglierne le opportunità e prevenirne i rischi.

In tale scenario si impone altresì un ripensamento del diritto all'oblio, laddove, con i motori di ricerca, si possono riportare in vita con un semplice clic notizie che in passato sarebbero rimaste sepolte negli archivi dei giornali o delle emittenti radiotelevisive.

L'ultima parte dell'opera è dedicata ai profili risarcitori specifici del danno da diffamazione, con un'analisi delle singole voci di pregiudizio e dei criteri di liquidazione, in un'ottica di coordinamento tra tutela penale e tutela civile.

Nel complesso, l'opera si segnala per rigore metodologico, aggiornamento normativo e costante attenzione alla casistica. Essa costituisce uno strumento di particolare utilità per studiosi e operatori del diritto e dell'informazione, offrendo una ricostruzione organica di una materia in continua evoluzione, nella quale la ricerca di un equilibrio tra libertà di espressione e tutela della dignità individuale si conferma, oggi più che mai, una sfida aperta.

La diffamazione
Vincenzo Pezzella

UTET Giuridica
Anno di edizione: 2026
ISBN: 9788859828570
Pagina: 1504

Ricordo di Angelo Marcello Cardani

Oreste Pollicino

Lo scorso 1° aprile si è spento Angelo Marcello Cardani, già presidente dall'Autorità per le garanzie nelle comunicazioni dal 2012 al 2020, professore di economia politica all'Università Bocconi e membro del gabinetto di Mario Monti durante i suoi mandati da commissario europeo dal 1995 al 2004. Componente del comitato scientifico della nostra rivista sin dalla sua fondazione, lo ricordiamo attraverso le parole di Oreste Pollicino.

Ricordare Angelo Cardani significa, per me, ricordare anzitutto una presenza. Non soltanto un economista raffinato, un uomo delle istituzioni, un protagonista della regolazione italiana ed europea delle comunicazioni. Tutto questo appartiene alla sua biografia pubblica e va ricordato: la Bocconi, la London School of Economics, l'insegnamento universitario, l'esperienza europea accanto a Mario Monti, la politica della concorrenza, la presidenza dell'Autorità per le garanzie nelle comunicazioni in anni decisivi per la trasformazione digitale del Paese. Ma chi ha avuto la fortuna di conoscerlo da vicino sa che in Angelo la dimensione istituzionale non cancellava mai quella umana. Semmai la rendeva più credibile.
Angelo è stato per me un vero amico. Una persona con cui si poteva parlare delle cose più serie senza mai sentirsi schiacciati dalla loro gravità. Aveva profondità, ma non pesantezza. Sapeva entrare nei problemi, anche nei più

complessi, senza compiacersi della complessità; e sapeva uscirne con una parola precisa, un sorriso, una battuta lieve, un'intuizione che spostava il punto di osservazione. Non banalizzava mai. Alleggeriva.

In Angelo Cardani la leggerezza non era mai il contrario della profondità. Era piuttosto il modo più elegante di abitarla. Calvino, nelle Lezioni americane, non oppone banalmente leggerezza e serietà: parla dell'opposizione tra leggerezza e peso, ma avverte che sostenere le ragioni della leggerezza non significa negare quelle del peso. È qui che mi pare di ritrovare Angelo. Egli conosceva benissimo il peso delle istituzioni, della regolazione, delle scelte pubbliche che incidono sui mercati, sui diritti, sulle persone. Ma non lasciava che quel peso diventasse pesantezza. Lo trasformava in misura, lucidità, ironia, ascolto. In una parola: autorevolezza.

La sua era una leggerezza adulta. Non fuga dalla realtà, non distacco aristocratico, non indifferenza. Era la leggerezza di chi ha attraversato davvero il peso delle cose e proprio per questo non ha bisogno di esibirlo. Come studioso e come regolatore, Angelo sapeva che le istituzioni vivono di competenza, ma anche di stile; di regole, ma anche di equilibrio; di decisioni, ma anche di responsabilità verso chi di quelle decisioni subisce gli effetti. Il suo modo di esercitare l'autorevolezza non era mai gridato. Non cercava il centro della scena. Eppure lo occupava naturalmente, perché la qualità del giudizio, quando è autentica, non ha bisogno di alzare la voce.

Negli anni della sua presidenza dell'AGCOM, il mondo delle comunicazioni stava cambiando natura. Non era più soltanto il mondo delle frequenze, della televisione, delle reti, del pluralismo informativo nel senso tradizionale. Era già l'ecosistema delle piattaforme digitali, della concentrazione del potere tecnologico, dei diritti degli utenti, della trasformazione del linguaggio pubblico. Angelo ha attraversato quel passaggio con la sobrietà di chi comprende che la regolazione non è mai pura tecnica, ma neppure pura politica. È un esercizio difficile di proporzione: tra mercato e diritti, tra innovazione e garanzie, tra libertà e responsabilità.

Eppure, al di là dei ruoli, ciò che resta con più forza è il modo in cui sapeva stare con le persone. Angelo ascoltava davvero. Non l'ascolto formale di chi attende il proprio turno per parlare, ma l'ascolto raro di chi prende sul serio l'interlocutore. Anche nel dissenso conservava una forma di gentilezza intellettuale. Non aveva bisogno di semplificare l'altro per affermare sé stesso. Questa è una qualità sempre più rara, nella vita pubblica come in quella accademica: la capacità di essere rigorosi senza essere duri, autorevoli senza essere distanti, ironici senza essere superficiali.

Forse è proprio qui che si incontrano l'uomo e il professionista. La competenza di Angelo non era mai separata dalla sua umanità. La sua intelligenza non diventava mai freddezza. La sua esperienza istituzionale non diventava mai posa. C'era in lui una combinazione preziosa di rigore e mitezza: il rigore dello studioso, abituato alla disciplina dell'argomento e

alla verifica delle conseguenze; la mitezza dell'uomo che non scambia la forza con l'aggressività, né l'autorevolezza con l'imposizione.

Per questo il suo ricordo non può essere soltanto il ricordo di una carriera importante. È, più profondamente, il ricordo di una qualità umana. Angelo apparteneva a quella categoria di persone che rendono le istituzioni meno fredde e l'intelligenza meno distante. Persone che non sottraggono peso alle cose perché non le prendono sul serio, ma perché sanno portarlo meglio. E forse questa è la forma più alta della leggerezza calviniana: non cancellare il peso del mondo, ma impedirgli di diventare opaco, immobile, insopportabile.

Ricordarlo oggi significa allora custodire una lezione di misura. La misura del pensiero, della parola, della relazione. La misura di chi sa che la profondità non ha bisogno di pesantezza e che la gentilezza non è mai debolezza. In Angelo questa misura era naturale. Era il suo modo di essere amico, maestro, interlocutore, uomo delle istituzioni.

E per questo, nel dolore del distacco, resta soprattutto la gratitudine. Gratitudine per ciò che ha dato alla vita pubblica del Paese. Gratitudine per ciò che ha rappresentato per chi gli è stato vicino. Gratitudine per quella sua capacità, così rara, di attraversare con profondità e leggerezza il peso delle cose.

Elenco autori

Stefania Ardito
dottoranda di ricerca in diritto della cybersicurezza, LUISS Guido Carli

Vittorio Bachelet
professore associato di diritto privato, Università Cattolica del Sacro Cuore

Rebecca Bovatti
dottoranda di ricerca in studi sulla criminalità organizzata, Università degli Studi di Milano

Omar Caramaschi
ricercatore di diritto costituzionale e pubblico, Università di Genova

Anna Chimenti
academic visitor, St Antony's College, University of Oxford

Sharmin N. Chogule
research associate, IRDi, University of Marburg

Marco Ciuro
docente a contratto, Università degli Studi di Padova

María Luisa Mena Durán
lecturer in private law, Universidad Cardenal Herrera-CEU/CEU Universities

Giulia Formici
ricercatrice di diritto pubblico comparato, Università degli studi di Parma

Federico Gravino
dottore di ricerca, Università degli Studi della Campania "Luigi Vanvitelli"

Riccardo Jovine
docente a contratto, Università San Raffaele – Roma

Elena Maioli Castriota Scanderbech
dottore di ricerca in diritto dell'Unione europea, Università degli Studi di Napoli "Federico II"

Carlo Melzi d'Eril
avvocato in Milano

Riccardo Merli
dottorando di ricerca in European studies for innovation, Università di Teramo

Marco Milani
avvocato in Milano

Alessandro Oldani
consulente in protezione dei dati personali e sicurezza informatica in Milano

Elenco autori

Federico Riboldi
avvocato in Milano

Andrea Stazi
professore ordinario di diritto privato comparato, Università San Raffaele – Roma

Raffaele Torino
professore ordinario di diritto privato comparato, Università degli Studi Roma Tre

Nico Tonti
ricercatore di diritto e religione, Università di Bologna

Anna Vasylchenko
dottoressa di ricerca, Università degli Studi di Bari "Aldo Moro"

Giulio Enea Vigevani
professore ordinario di diritto costituzionale e pubblico, Università di Milano - BicoccaEdoardo Salvatore

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.

mediaLAWS

ANNO 2026 - CODICE ISSN 2532-9146