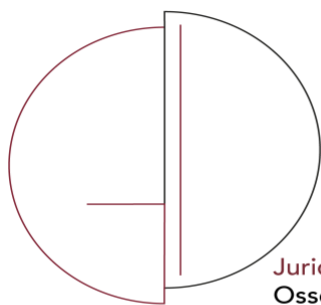




Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

Questa rubrica di aggiornamento è curata dal Prof. Salvatore Orlando e dal Dott. Mario Mauro nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia dell'Impresa dell'Università di Roma "La Sapienza" (<https://dei.web.uniroma1.it/it/ogid> - jodi.deap@uniroma1.it).

SOMMARIO

2025/4(1)SO Gli ultimi due ordini esecutivi del presidente degli Stati Uniti d'America Donald J. Trump in materia di intelligenza artificiale: "Launching the Genesis Mission" del 24.11.2025, e "Ensuring a National Policy Framework for Artificial Intelligence" dell'11.12.2025 – **Salvatore Orlando**

2025/4(2)SO Il "National Security Program" americano del novembre 2025 e il comunicato del Segretario di Stato Rubio del 23.12.2025 sulle azioni intraprese dal Dipartimento di Stato nei confronti di cinque persone tra cui l'ex Commissario UE Thierry Breton per contrastare il "complesso industriale di censura globale" – **Salvatore Orlando**

2025/4(3)PGI La "Dichiarazione per la sovranità digitale europea" del 18.11.2025: verso un modello europeo di autonomia digitale – **Paola Giacalone**

2025/4(4)CF La comunicazione della Commissione europea sulla nuova strategia dell'Unione per i dati "Unlocking Data for AI" COM(2025) 835 final del 19.11.2025 – **Carla Failla**

2025/4(5)EST Il pacchetto "Digital Omnibus": la proposta della Commissione "Digital Omnibus" COM(2025) 837 final del 19.11.2025 di modifica del GDPR, del Data Act, del regolamento sullo sportello unico digitale e delle direttive e-privacy, NIS2 e CER, nonché di abrogazione della direttiva Open

* Contributo non sottoposto a referaggio ai sensi dell'art. 2.2, lett. c), del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 306 del 21.12.2023.



Data, del Data Governance Act, del regolamento P2B e del regolamento sulla libera circolazione dei dati non personali – **Elisabetta Stringhi**

2025/4(6)Est (*segue*) Il pacchetto “Digital Omnibus”: la proposta della Commissione “Digital Omnibus on AI” COM(2025) 836 final del 19.11.2025 di modifica dell’AI Act – **Elisabetta Stringhi**

2025/4(7)SO Approvato dalla Commissione europea il 1.8.2025 il primo codice di buone pratiche per i modelli di IA per finalità generali – **Salvatore Orlando**

2025/4(8)FPa La prima bozza del codice di buone pratiche sulla trasparenza dei contenuti generati dalla IA ai sensi dell’AI Act pubblicata il 17.12.2025 – **Federica Paolucci**

2025/4(9)LCo L’AI Act Whistleblower Tool annunciato il 24.11.2025 - **Lorenzo Corea**

2025/4(10)TDMCDV Lo studio sull’utilizzo della IA nel settore della sanità pubblicato dall’Ufficio per le pubblicazioni dell’Unione europea l’8.8.2025 – **Tommaso De Mari Casareto dal Verme**

2025/4(11)VF Il regolamento (UE) 2025/2518 del 26.11.2025 che stabilisce norme procedurali aggiuntive sull’applicazione del GDPR – **Virginia Fusco**

2025/4(12)VM La comunicazione della Commissione europea “DigitalJustice@2030” COM(2025) 802 final del 20.11.2025: la competitività dell’Unione Europea attraverso la modernizzazione dei sistemi giudiziari e la formazione degli operatori del diritto – **Vincenzo Mignano**

2025/4(13)AA L’Agenda dei consumatori 2030 adottata dalla Commissione europea il 19.11.2025 – **Andrea Amidei**

2025/4(14)BP Il primo report del 18.11.2025 del Comitato europeo per i servizi digitali (EBDS) in cooperazione con la Commissione europea sui più significativi e ricorrenti rischi sistemici e sulle relative misure di mitigazione ai sensi del Digital Services Act – **Beniamino Parenzo**

2025/4(15)BG Le Linee guida EDPS dell’11.11.2025 Guidance for risk management of AI systems – **Beatrice Gallucci**

2025/4(16)AG Gli orientamenti del 14.7.2025 della Commissione europea sulle misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online ai sensi dell’art. 28(4) del DSA (Comunicazione C/2025/5519) – **Antonio Gorgoni**

2025/4(17)BCo Le attività conoscitive avviate dalla Commissione europea nell’ottobre 2025 nei confronti di Snapchat, YouTube, Apple e Google sulle

misure di salvaguardia dei minori ai sensi del Digital Services Act - **Bruno Concas**

[2025/4\(18\)RR](#) La seconda versione dell'age verification blueprint della Commissione europea del 10.10.2025 – **Rachele Ranieri**

| 1015

[2025/4\(19\)RMo](#) La bozza di raccomandazione delle clausole contrattuali tipo non vincolanti relative all'accesso ai dati e al relativo utilizzo e delle clausole contrattuali standard non vincolanti per i contratti di cloud computing elaborate dalla Commissione europea ai sensi dell'art. 41 del Data Act (Comunicazione C(2025) 7750 final del 19.11.2025) – **Roberta Montinaro**

[2025/4\(20\)MVT](#) La sanzione di 120 milioni di euro comminata della Commissione europea a X il 5.12.2025 per violazione del Digital Services Act – **Maria Vittoria Trinchera**

[2025/4\(21\)GV](#) I preliminary findings della Commissione europea del 24.10.2025 sulla violazione dei doveri di trasparenza ai sensi del Digital Services Act da parte di TikTok e Meta e l'accettazione da parte della Commissione europea in data 5.12.2025 degli impegni assunti da TikTok in materia di trasparenza della pubblicità ai sensi del medesimo regolamento – **Giuseppe Versaci**

[2025/4\(22\)VH](#) L'istruttoria annunciata il 4.12.2025 della Commissione europea per abuso di posizione dominante e il provvedimento cautelare dell'AGCM n. 31775 del 22.12.2025 aventi entrambi ad oggetto la nuova policy contrattuale di limitazione di accesso a WhatsApp applicata da Meta ai fornitori di IA – **Victor Hartl**

[2025/4\(23\)AB](#) La sentenza della Corte di giustizia prima sezione nella causa C-413/23 P del 4 settembre 2025 sulla nozione di dati personali e di pseudonomizzazione (caso SRB (o CRU)) – **Alessandro Bernes**

[2025/4\(24\)EG](#) La sentenza della Corte di giustizia del 2.12.2025 nella causa C-492/23 (caso Russmedia) sul principio di responsabilizzazione del GDPR e il rapporto con la direttiva e-commerce a proposito del trattamento dei dati personali contenuti in annunci pubblicati sulla piattaforma di un mercato online - **Elisa Grossi**

[2025/4\(25\)ST](#) Il primo report dell'Appeals Centre Europe: potenzialità e ostacoli della risoluzione extragiudiziale delle controversie sulle decisioni delle piattaforme – **Sara Tommasi**

[2025/4\(26\)RA](#) La sentenza del 19.11.2025 del Tribunale dell'Unione europea di rigetto del ricorso di Amazon per l'annullamento della decisione della Commissione europea di designazione di Amazon Store come VLOP ai sensi del Digital Services Act e le inerenti statuizioni di conformità del DSA alla CDFUE – **Riccardo Alfonsi**



[2025/4\(27\)GD](#) I rimedi comportamentali e strutturali imposti a Google con sentenza del 2.9.2025 a proposito della proprietà di Chrome, dei dati di ricerca e dei contratti in esclusiva nella causa Stati Uniti d'America c. Google LLC, 2024 WL 3647498 – **Giorgia Diotallevi**

[2025/4\(28\)FF](#) La sanzione di 255,7 milioni di euro irrogata dall'AGCM a Ryanair il 19.12.2025 per abuso di posizione dominante nei confronti delle agenzie di viaggio fisiche e *online* (OTA) per i servizi aerei nazionali ed europei da e/o verso l'Italia - **Francesca Ferretti**

[2025/4\(29\)GG](#) Il Codice di condotta per gli influencer e le modifiche alle Linee guida per gli influencer approvati dall'AGCOM con delibera n. 197/25/CONS del 23.7.2025 – **Giorgio Giuliano**

[2025/4\(30\)RMa-MCG](#) Le “Linee guida per l’implementazione dell’Intelligenza Artificiale nel mondo del lavoro” adottate con decreto del Ministro del lavoro e delle politiche sociali n. 180 del 17.12.2025 – **Riccardo Maraga/Maria Chiara Garofalo**

[2025/4\(31\)FDA](#) La sentenza del TAR Lombardia del 21.10.2025 sulla segnalazione al Consiglio dell’Ordine dell’avvocato che si avvale dell’attività di collaboratori o di applicazioni di intelligenza artificiale senza verificare l’esito delle ricerche – **Filippo D’Angelo**

[2025/4\(32\)DI](#) Pubblicato lo studio dell’agenzia ministeriale francese ANSES sugli effetti dell'uso dei social network sulla salute degli adolescenti – **Daniele Imbruglia**

[2025/4\(33\)CI](#) La sanzione di oltre 98 milioni di euro irrogata dall'AGCM ad Apple il 16.12.2025 per abuso di posizione dominante in relazione alla policy App Tracking Transparency – **Cecilia Isola**

[2025/4\(34\)FZ](#) Il primo provvedimento AGCOM del 6.11.2025 di diffida ai sensi del regolamento UE Platform-to-business (caso Refurbed) – **Francesca Zampone**

[2025/4\(35\)ES](#) Pubblicato il d.lgs. n. 212 del 31.12.2025 di recepimento della direttiva (UE) 2023/2225 del relativa ai contratti di credito ai consumatori – **Emanuele Stabile**

[2025/4\(36\)TB](#) La nuova versione dello standard ISO/IEC 27701:2025 per la privacy – **Timoteo Bucci**

[2025/4\(37\)LC](#) Il provvedimento del Garante privacy italiano del 1.10.2025 di limitazione provvisoria del trattamento di dati personali relativi al servizio di IA generativa “Clothoff” – **Lucio Casalini**

[2025/4\(38\)SR](#) Il provvedimento del Garante privacy italiano del 10.7.2025 sul trattamento di dati personali di bambini da parte di un asilo nido. Alcune riflessioni sulla tutela della dignità dei minori e la tenuta del consenso genitoriale nell'era digitale - **Samuele Francesco Rosa**

[2025/4\(39\)EF](#) La sentenza della Corte di Cassazione n. 28772/2025 del 31.10.2025 confermativa dell'orientamento sulla etero-organizzazione dei riders – **Emanuela Fiata**

[2025/4\(40\)MC](#) La sentenza della Corte suprema svedese del 1 luglio 2025 di annullamento di un contratto di gioco per sfruttamento della compulsività del contraente giocatore desumibile dai dati del suo comportamento online – **Michele Ciancimino**

[2025/4\(41\)AF](#) Il GENIUS Act del 18.7.2025: confronto con il MiCAR – **Alice Filippetta**

[2025/4\(42\)AF](#) Verso il CLARITY Act: l'incertezza regolamentare per gli *asset* digitali – **Alice Filippetta**

[2025/4\(43\)FG](#) La sentenza del Landesgericht di Monaco dell'11.11.2025 nel caso GEMA (collecting tedesca) contro Open AI in materia di tutela del diritto d'autore, addestramento di modelli di IA generativa e ruolo dei "pesi" – **Francesco Grossi**

[2025/4\(44\)FR](#) La sentenza della High Court of England and Wales del 4.11.2025 nel caso Getty Images contro Stability AI in materia di tutela del diritto d'autore, addestramento di modelli di IA generativa e ruolo dei "pesi" – **Francesca Rotolo**

[2025/4\(45\)FZ](#) Il provvedimento interlocutorio del Giudice Donato del 6.11.2025 nel caso *Fortnite*: l'accordo transattivo Epic Games–Google tra rimedi antitrust e regolazione privata del mercato delle app – **Francesca Zampone**

[2025/4\(46\)RP](#) La legge dello Stato di New York "The Responsible Artificial Intelligence Safety and Education (RAISE) Act" sui modelli di intelligenza artificiale "di frontiera". Il comunicato stampa della Governatrice del 19.12.2025 e la nuova proposta legislativa dell'8.01.2026 – **Rosalba Potenzano**

[2025/4\(47\)FF](#) La legge dell'Illinois del 1.8.2025 che proibisce di affidare decisioni terapeutiche a sistemi di IA (il Wellness and Oversight for Psychological Resources Act) - **Francesca Ferretti**

[2025/4\(48\)DI](#) Il "New York Algorithmic Pricing Disclosure Act" entrato in vigore il 10.11.2025 – **Daniele Imbruglia**



2025/4(49)LS La legge dello Stato della California sull'intelligenza artificiale "The Transparency in Frontier Artificial Intelligence Act" (SB53) del 29.9.2025 – **Ludovica Sposini**

| 1018

2025/4(50)GDM Le Linee guida dell'UNESCO del 2025 sull'uso dei sistemi di IA nei tribunali – **Gennaro Di Martino**

Una raccolta indicizzata dei numeri della rubrica degli anni 2020-2023 è disponibile sull'[Atlante storico del diritto dei dati 2020-2023](#). Tutti i numeri della rubrica (compresi i numeri del 2024 e quelli del 2025 non ancora raccolti nell'Atlante) sono facilmente consultabili nella sezione [OGID](#) del sito web della Rivista.

2025/4(1)SO

Gli ultimi due ordini esecutivi del presidente degli Stati Uniti d’America Donald J. Trump in materia di intelligenza artificiale: “Launching the Genesis Mission” del 24.11.2025, e “Ensuring a National Policy Framework for Artificial Intelligence” dell’11.12.2025

| 1019

Tra novembre e dicembre 2025, il Presidente degli Stati Uniti d’America Donald J. Trump (**POTUS**) ha emesso due ordini esecutivi in materia di intelligenza artificiale (IA):

- l’executive order del 24.11.2025 intitolato “[Launching the Genesis Mission](#)” (**Genesis Mission EO**);
- l’executive order dell’ 11.12.2025 intitolato “[Ensuring a National Policy Framework for Artificial Intelligence](#)” (**Policy Framework EO**)

Essi seguono altre significative iniziative già messe in campo nel corso del 2025 dal POTUS in materia di IA, di cui si è dato conto in questa Rubrica, ossia:

- l’executive order emesso dal POTUS il 23.1.2025 dal titolo «Rimuovere le barriere alla leadership americana nell’intelligenza artificiale» (**Removing Barriers EO**) per mezzo del quale il POTUS fissava i tre obiettivi generali della sua politica di «dominio globale dell’America sull’intelligenza artificiale» individuati nella promozione della «fioritura umana», nella competitività economica e nella sicurezza nazionale, disponendo la revoca di alcune precedenti politiche e direttive sull’IA in quanto considerate alla stregua di «barriere all’innovazione americana della intelligenza artificiale», ed in particolare disponendo in merito alla revoca dell’Executive Order n. 14110 del 30.10.2023 del suo predecessore Joe Biden, intitolato Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (v. *amplius* il contributo n.1 del [numero 2/2025](#) [2025/2(1)SO], in *PeM* 2025, p. 612);
- il piano di azione sull’intelligenza artificiale degli Stati Uniti d’America annunciato dal POTUS il 23 luglio 2025 (il **Piano di azione americano sulla IA**), contenente più di 90 raccomandazioni alle agenzie federali, su un’ampia gamma di argomenti, tra cui la riduzione della regolazione, la promozione della distribuzione di modelli di IA e set di dati open source, l’eliminazione di “bias ideologici” dai modelli di IA, la formazione dei lavoratori per l’uso dell’IA, lo sviluppo di infrastrutture per l’IA, l’incremento dell’esportazione, così individuando indirettamente altrettanti specifici obblighi per gli sviluppatori di IA in particolare per i fornitori del governo federale; e prevedendo in particolare che i sistemi di IA usati dal governo federale debbano essere «liberi da misinformation», a tal fine richiedendo, inter alia, al Dipartimento del Commercio di modificare il *National Institute of Standards and Technology AI Risk Management Framework* al fine di «eliminare riferimenti al



cambiamento climatico e ad iniziative DEI [Diversità Equità Inclusion]», ed istruendo le agenzie federali affinché esse si approvvigionino soltanto di large language models (LLMs) che siano «objective and free from topdown ideological bias» (v. *amplius* il contributo n. 2 nel [numero 3/2025](#) [2025/3(2)SO] in *PeM* 2025, p. 1020);

- l'executive order emesso dal POTUS il 23.7.2025 dal titolo «Preventing Woke AI in the Federal Government» (il **Bias EO**) coevo al Piano di azione americano sulla IA, che si diffonde sui requisiti ideologici dei sistemi di IA di cui al medesimo Piano, richiedendo alle agenzie federali di attenersi a due c.d. «Unbiased AI Principles» (la «ricerca della verità» e la «neutralità ideologica») in particolare vietando applicazioni IA che possano «manipolare le risposte favorendo dogmi ideologici come DEI», e che inoltre prevede una serie dettagliata di policy recommendations per snellire i procedimenti autorizzativi e facilitare lo sviluppo di data centers e altre infrastrutture e per «esportare la IA americana» a «partner e alleati degli Stati Uniti» (v. *amplius* il contributo n. 2 nel [numero 3/2025](#) [2025/3(2)SO] in *PeM* 2025, p. 1020).

Gli ultimi due ordini esecutivi del POTUS si ineriscono nella stessa linea di policy normativa.

Il **Genesis Mission EO** si divide in 7 sezioni.

La **I sezione** del Genesis Mission EO fissa lo scopo della «Genesis Mission» (la **Missione**) e cita il Progetto Manhattan per evocare un precedente storico ritenuto di importanza comparabile agli sforzi sostenuti dall'amministrazione del POTUS per vincere la «gara» nella «competizione globale sulla IA». Si definiscono dunque gli obiettivi della Missione nei seguenti termini: «the Genesis Mission **will bring together our Nation's research and development resources** — combining the efforts of brilliant American scientists, including those at our national **laboratories**, with pioneering American **businesses**; world-renowned **universities**; and existing **research infrastructure, data repositories, production plants, and national security sites** — to achieve dramatic acceleration in AI development and utilization».

Nella **II sezione** del Genesis Mission EO, si istituisce formalmente la Missione, definendola come «uno sforzo inteso ad **accelerare l'applicazione della IA per scoperte scientifiche trasformative focalizzate sulle pressanti sfide nazionali**» e si individuano i compiti del Secretary of Energy (**Secretary**) e dell'Assistant to the President for Science and Technology (**APST**).

Nella **III sezione** del Genesis Mission EO, si prevede che il Secretary debba istituire e rendere operativa l'*American Science and Security Platform* (la **Piattaforma**) in funzione di infrastruttura per la Missione, e si prevedono alcune caratteristiche della Piattaforma oltre che un cronoprogramma per il Secretary.

Nella **IV sezione** del Genesis Mission EO, si prevede che il Secretary debba entro un certo termine presentare una lista di almeno 20 «sfide» di interesse

nazionale da includere nella missione, in una serie di settori strategici, tra i quali:

- (i) manifattura avanzata;
- (ii) biotecnologia;
- (iii) materie prime critiche (*critical materials*);
- (iv) fissione nucleare ed energia da fusione;
- (v) scienza informatica quantistica;
- (vi) semiconduttori e microelettronica.

La **V sezione** del Genesis Mission EO individua compiti più specifici dell'APST in particolare relativamente ai suoi poteri di coinvolgimento di agenzie e di altri enti per il perseguimento dei fini della Missione.

Infine, la **VI** e la **VII sezione** del Genesis Mission EO contengono, rispettivamente, istruzioni sulla reportistica delle attività relative alla Missione da parte del Secretary e previsioni di carattere amministrativo.

Il successivo **Policy Framework EO** si prefigge di sviluppare ulteriormente la linea di policy del Removing Barriers EO, nel senso di abolire regole esistenti e future in quanto ritenute un freno allo sviluppo della IA americana, e si compone di 9 sezioni.

Nella **sezione I** del Policy Framework EO, si fissa il suo obiettivo generale di riduzione di limiti normativi allo sviluppo della IA e si dice che l'amministrazione del POTUS deve agire insieme al Congresso per assicurare la creazione di **uno standard normativo nazionale con un impatto minimo**, piuttosto che 50 standard normativi statali discordanti. Si aggiunge che dovranno assicurarsi due risultati:

- 1) **proibire leggi statali configgenti con la policy prevista dal medesimo Policy Framework EO;**
- 2) **perseguire come obiettivi la protezione dei bambini, il contrasto alla censura, la tutela del diritto d'autore, la salvaguardia delle comunità.**

Nella **sezione II** del Policy Framework EO, si ribadisce in breve che la policy degli Stati Uniti prevista dal medesimo executive order consiste nel **sostenere e aumentare il dominio globale della IA** americana attraverso una cornice normativa nazionale di governance della IA avente un impatto minimo.

Nella **sezione III** del Policy Framework EO, si prevede l'istituzione di una speciale task force di avvocati (la **task force**) dedicata a **impugnare leggi statali in contrasto con la policy** di cui alla sezione II del Policy Framework EO.

Nella **sezione IV** del Policy Framework EO, si attribuisce al Secretary of Commerce il compito di valutare **quali leggi statali possano ritenersi in contrasto** con la policy di cui alla sezione II del Policy Framework EO.

Nella **sezione V** del Policy Framework EO, si prevedono una serie di misure per **impedire l'accesso a fondi governativi** di vario tipo **agli Stati che adottino o mantengano leggi statali in contrasto** con la policy di cui alla sezione II del Policy Framework EO.

Nella **sezione VI** del Policy Framework EO si prevede la possibilità della creazione di uno **standard** da utilizzare per la reportistica di leggi statali in contrasto con la policy di cui alla sezione II del Policy Framework EO.



Nella sezione VII del Policy Framework EO, si prevede che il Presidente della Federal Trade Commission formuli un policy statement per chiarire come possa applicarsi ai modelli di IA la disposizione di cui alla sezione 5 del Federal Trade Commission Act (FTC Act) che proibisce gli atti e le pratiche scorrette o fuorvianti che riguardano il commercio, e che tale policy statement debba in particolare chiarire in quali casi sono vietate alla stregua di questo divieto le **«leggi statali che richiedono alterazioni di outputs veritieri dei modelli di IA»**.

Nella sezione VIII del Policy Framework EO prevede che lo Special Advisor for AI and Crypto del POTUS e l'APST debbano preparare **una cornice uniforme di politica normativa federale per la IA** idonea ad evitare leggi statali in contrasto con la policy di cui alla sezione II del Policy Framework EO, contenente almeno i seguenti punti:

- (i) protezioni per la sicurezza dei bambini;
- (ii) infrastrutture computazionali e data centres per l'IA;
- (iii) approvvigionamento e uso della IA da parte degli Stati.

La **sezione IX** del Policy Framework EO, contiene disposizioni amministrative e finali.

Il Policy Framework EO è stato preceduto da una **lettera del 25.11.2025 rivolta al Congresso degli Stati Uniti da [36 Procuratori generali](#) di opposizione a divieti federali** nei confronti di leggi statali in materia di IA.

Per comprendere con un dato quantitativo i termini della tensione tra i sopra citati executive orders del POTUS, da un lato, e le normative statali in materia di IA negli USA, dall'altro può citarsi il report "[AI Index 2025](#)" del centro HAI (Human-Centered Artificial Intelligence) dell'Università di Stanford. Esso riporta che **le leggi statali "AI-related" approvate negli USA nel periodo 2016-2024 sono in totale 131**.

A tale dato deve aggiungersi il 2025. In questa Rubrica, abbiamo pubblicato contributi relativi ad alcune iniziative legislative statali in materia di IA intraprese negli USA nell'ultimo biennio e quindi anche comprensive del 2025:

- il Transparency in Frontier Artificial Intelligence Act dello **Stato della California del 29.9.2025**, su cui v. infra il contributo n. 49 in questo numero della Rubrica [2025/4(49)LS];
- il RAISE Act dello **Stato di New York del 19.12.2025** sui modelli di intelligenza artificiale "di frontiera", soggetto all'ultimo passaggio parlamentare, su cui v. infra il contributo n. 46 in questo numero della Rubrica [2025/4(46)RP];
- Il New York Algorithmic Pricing Disclosure Act dello **Stato di New York del 10.11.2025**, su cui v. infra il contributo n. 48 in questo numero della Rubrica [2025/4(48)DI];
- il Wellness and Oversight for Psychological Resources Act dello **Stato dell'Illinois del 1 agosto 2025**, su cui v. infra il contributo n. 47 in questo numero della Rubrica [2025/4(47)FF];
- il disegno di legge dello **Stato della Virginia del 7 gennaio 2025** sui sistemi di IA ad alto rischio: High-Risk Artificial Intelligence Developer and Deployer Act (House Bill No. 2094), su cui v. contributo n. 24 nel [numero 1/2025](#) [2025/1(24)LS] in *PeM* 2025, p. 344;

- il **Colorado AI Act del 17.5.2024**, su cui v. contributo n. 3 nel [numero 2/2024](#) [2024/2(3)SO] in *PeM*, 2025, p. 662.

SALVATORE ORLANDO

<https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/>
<https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>

| 1023

2025/4(2)SO

Il “National Security Program” americano del novembre 2025 e il comunicato del Segretario di Stato Rubio del 23.12.2025 sulle azioni intraprese dal Dipartimento di Stato nei confronti di cinque persone tra cui l'ex Commissario UE Thierry Breton per contrastare il “complesso industriale di censura globale”

Il documento del Presidente degli Stati Uniti d’America Donald J. Trump (**POTUS**) intitolato **National Security Strategy** datato novembre 2025 (**NSS**), come noto, abbraccia tutti i temi generali legati alla sicurezza degli Stati Uniti d’America. Nella sezione dedicata all’Unione europea, si legge, tra le altre, la seguente dichiarazione: «We want Europe [...] to abandon its failed focus on regulatory suffocation» (p. 25 NSS).

Si tratta di una dichiarazione coerente all’indirizzo dell’amministrazione dell’attuale Presidente degli Stati Uniti di contrasto alla legislazione europea nel settore del digitale, come indicato già in precedenti provvedimenti e iniziative del POTUS, tra le quali un suo [memorandum ufficiale del 21 febbraio 2025](#) nel quale si afferma che la sua amministrazione considererà di dare risposte quali tariffe per contrastare l’applicazione da parte di governi stranieri di tasse e sanzioni amministrative pecuniarie (*fines*) a società americane nel settore del digitale.

Successivamente, in data 23 dicembre 2025, il Segretario di Stato americano, Marco Rubio, pubblicava un comunicato stampa dal titolo “Annuncio di azioni per combattere il complesso industriale di censura globale” (l’**Annuncio**), nel quale, *inter alia*, annunciava l’adozione di azioni ai sensi della sezione 212(a)(3)(C) dell’Immigration and Nationality Act nei confronti del Sig. Thierry Breton per presunti «tentativi organizzati di costringere le piattaforme digitali americane a censurare, demonetizzare e sopprimere i punti di vista americani a cui essi si oppongono».

Thierry Breton è stato commissario UE per il mercato interno e i servizi nel periodo 2019-2024 e uno degli architetti del regolamento (UE) 2022/2065 (Digital Services Act, **DSA**). Il DSA contiene, tra le altre disposizioni, norme relative alla trasparenza delle piattaforme online e al disegno delle interfacce online, nonché un’articolata disciplina in materia di moderazione dei contenuti, con obblighi e divieti generali imposti a tutte le piattaforme, e con disposizioni particolari per le piattaforme online di dimensioni molto grandi

(VLOPs) e per i motori di ricerca online di dimensioni molto grandi (VLOSEs).

L'Annuncio è stato pubblicato dopo che la piattaforma X (una VLOP) ha ricevuto una sanzione di 120 milioni di euro per violazione del DSA, con provvedimento della Commissione europea del 5.12.2025 (su cui v. *infra* il contributo n. 20 in questo numero di questa Rubrica [2025/4(20)MVT])

Anche negli USA si riscontra una forte tensione tra l'orientamento tradizionale che vede la moderazione dei contenuti online come un'attività censoria - e, pertanto, contraria alla **sezione 230** del Communications Act del 1934, come introdotto dal **Communications Decency Act del 1996** - e un orientamento più recente che fa leva sul **disegno delle piattaforme, piuttosto che sui contenuti** (così rendendo irrilevante l'applicazione della citata sezione 230), per giustificare la reazione ordinamentale a fenomeni di dipendenza e manipolazione derivante da contenuti online. Il caso giurisprudenziale leader negli USA riguarda un'azione intrapresa contro Meta davanti alla Los Angeles Superior Court, attualmente ancora in fase di decisione relativamente alle allegazioni contro Meta, dopo che sono stati conclusi accordi transattivi con gli altri convenuti per le piattaforme Snapchat e TikTok (caso *Kaley G.M. v. Meta et al*, giudice Carolyn Kuhl, Social Media Cases JCCP5255, Lead Case: 22STCV21355).

SALVATORE ORLANDO

<https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>
<https://www.state.gov/releases/office-of-the-spokesperson/2025/12/announcement-of-actions-to-combat-the-global-censorship-industrial-complex>

2025/4(3)PGi

La “Dichiarazione per la sovranità digitale europea” del 18.11.2025: verso un modello europeo di autonomia digitale

Il 18 novembre 2025 i rappresentanti dei governi degli Stati membri dell'Unione europea – tra cui l'Italia – hanno sottoscritto la *Declaration for European Digital Sovereignty* (la **Dichiarazione**), documento politico non vincolante che mira a definire un approccio comune alla sovranità digitale europea. La Dichiarazione si inserisce nel quadro delle più recenti iniziative normative dell'Unione Europea – reg. (UE) 2024/1689 (**AI Act**), reg. (UE) 2022/868 (**Data Governance Act**), reg. (UE) 2023/2854 (**Data Act**), reg. (UE) 2023/1781 (**Chips Act**), [Cybersecurity Strategy](#) - e ne costituisce una cornice di coordinamento, che pone l'accento sulla necessità di integrare gli strumenti già esistenti, evitando frammentazioni o duplicazioni regolatorie. Di particolare rilievo è la definizione europea di *digital sovereignty*, intesa non come autarchia tecnologica, ma come capacità dell'Unione di regolare in modo autonomo infrastrutture digitali, dati e tecnologie sensibili, assicurando che le scelte tecnologiche – pubbliche e private – riflettano valori e interessi

europei. Nella Dichiarazione si afferma esplicitamente che l'autonomia europea non coincide con la chiusura dei mercati, bensì con la possibilità di instaurare rapporti di cooperazione con partner che condividano standard e valori comuni.

La Dichiarazione individua alcune aree prioritarie. Centrale è la **data sovereignty**, articolata come esigenza di ridurre le dipendenze critiche e garantire la protezione dei dati sensibili, anche attraverso l'uso di strumenti quali l'*European Digital Identity Wallet*, *Once-Only Technical System* e *data spaces* settoriali. Si sottolinea altresì la necessità di investimenti coordinati nelle tecnologie strategiche (AI, cloud, HPC, semiconduttori, reti avanzate, cybersecurity), evidenziando come la mobilitazione di capitali privati costituisca un elemento essenziale del disegno europeo.

Particolare attenzione è dedicata alla standardizzazione: la partecipazione attiva dell'Unione europea negli organismi internazionali di normazione è qualificata come condizione per preservare competitività e interoperabilità, evitando dipendenze da standard tecnici extraeuropei. Nel medesimo contesto si colloca il richiamo all'open source, riconosciuto come fattore di autonomia tecnologica, purché integrato in modelli di sicurezza affidabili e verificabili.

Il documento adotta un approccio chiaramente *risk-based* alla gestione delle dipendenze tecnologiche. Esso esclude esplicitamente la prospettiva della *self-sufficiency*, definita irrealistica, e privilegia invece la capacità di agire con autonomia nei settori "sensibili", in particolare nella protezione delle infrastrutture critiche e nei domini più esposti a minacce geopolitiche, disinformazione e manipolazioni algoritmiche.

Rilevante anche il profilo della *governance*: la Dichiarazione auspica meccanismi di coordinamento più efficaci tra Stati membri, una riduzione della frammentazione regolatoria e un approccio *multi-stakeholder* che includa imprese, PA e società civile. Nel testo emerge inoltre un riferimento insistito alla necessità di rafforzare competenze digitali e *literacy*, considerate un presupposto della stessa sovranità digitale.

Pur priva di effetti giuridici vincolanti, la *Declaration for European Digital Sovereignty* chiarisce l'intenzione degli Stati membri di consolidare un modello di autonomia strategica "aperta", capace di integrare sicurezza, competitività, tutela dei diritti e cooperazione internazionale: un obiettivo che, per essere effettivamente perseguito, richiederà interventi normativi mirati relativi a dati, infrastrutture critiche, tecnologie avanzate e governance del digitale.

PAOLA GIACALONE

<https://data.consilium.europa.eu/doc/document/ST-15781-2025-INIT/en/pdf>

2025/4(4)CF

La comunicazione della Commissione europea sulla nuova strategia dell'Unione per i dati "Unlocking Data for AI" COM(2025) 835 final del 19.11.2025

La Comunicazione della Commissione europea del 19 novembre 2025, intitolata *Data Union Strategy – Unlocking data for AI* (COM(2025) 835 final) (la **Comunicazione** e la **Data Union Strategy** o la **Strategia**), si inserisce in una fase di avanzata maturazione del diritto dell'Unione europea dei dati, caratterizzata da una crescente esigenza di razionalizzazione, coordinamento e funzionalizzazione dell'*acquis* esistente. Essa non si presenta, tuttavia, come un ulteriore intervento settoriale destinato ad accrescere la già significativa stratificazione normativa che contraddistingue il diritto digitale dell'Unione; al contrario, assume consapevolmente la fisionomia di atto di indirizzo, volto a riorientare complessivamente – quasi in chiave antitetica – l'architettura giuridica dei dati, rendendola internamente coerente e teleologicamente indirizzata alle nuove condizioni tecnologiche, economiche e geopolitiche determinate dall'ascesa dell'intelligenza artificiale, in particolare nella sua declinazione generativa.

La Comunicazione muove, così, da una constatazione che, pur apparentemente descrittiva, possiede una forte valenza conformativa.

Nonostante, invero, le solide basi poste attraverso strumenti normativi chiave, investimenti in spazi comuni europei, iniziative di politica industriale e tecnologica (delineate, nello specifico, nell'*AI Continent Action Plan* e nella *Apply AI Strategy*, su cui v. in questa Rubrica notizia n. 2 del numero 2/2025 [2025/2(2)DI], in *PeM* 2025, p. 614), l'Unione si confronta oggi con una persistente scarsità di dati utilizzabili per lo sviluppo dell'IA. Tale scarsità – oltretutto – non è soltanto quantitativa, ma anche qualitativa e strutturale, poiché una parte rilevante dei dati disponibili rimane frammentata o sottoutilizzata, anche a causa di un quadro normativo percepito come eccessivamente complesso e disomogeneo.

L'Unione europea dispone, infatti, di uno dei quadri normativi più avanzati a livello globale in materia di protezione dei dati personali, governance della condivisione, accesso e riutilizzo delle informazioni pubbliche e industriali, come dimostrano, tra l'altro, il reg. (UE) 2024/1689 (**GDPR**), il reg. (UE) 2022/868 (**Data Governance Act**), il reg. (UE) 2023/ (**Data Act**) e il rafforzamento del regime dell'open data. Tale apparato regolatorio, costruito progressivamente nell'arco temporale compreso tra il 2016 e il 2024, ha indubbiamente consolidato un modello europeo fondato sulla tutela dei diritti fondamentali, sulla fiducia e sulla sicurezza giuridica; nondimeno, esso manifesta oggi limiti strutturali in termini di effettività, usabilità e capacità di sostenere lo sviluppo e la diffusione dell'intelligenza artificiale su una scala comparabile a quella dei principali attori globali.

In questo contesto, invero, mentre i principali concorrenti globali avanzano rapidamente nello sfruttamento dei dati a fini tecnologici e industriali, l'Unione rischia di vedere ampliarsi lo scarto tra l'elevata ambizione regolatoria e i risultati economico-tecnologici effettivamente conseguiti.

È, dunque, precisamente in tale divario che si colloca la Strategia, con l'esplicito proposito di spostare l'asse dell'azione europea “*from rules to results*”, segnando un passaggio paradigmatico dalla fase costituente del diritto dei dati – dominata, appunto, dalla produzione di norme e principi – a una fase attuativa, incentrata sulla concreta messa a valore delle risorse informative. In questa prospettiva, il dato non è più considerato

esclusivamente come oggetto di protezione o di limitazione, bensì come infrastruttura strategica per l'innovazione, la competitività e la sovranità tecnologica dell'Unione.

All'interno di tale cornice, la Comunicazione dialoga necessariamente con il pacchetto *Digital Omnibus* (sul quale v. in questo numero di questa Rubrica le notizie n. 5 e n. 6 *infra* [2025/4(5)ESt] e [2025/4(6)ESt]), che assume un ruolo centrale nell'economia della strategia, costituendone il naturale completamento giuridico. Mentre la *Data Union Strategy* definisce la visione complessiva, individua le criticità strutturali e delinea le priorità di intervento in materia di dati, il *Digital Omnibus* è infatti chiamato a fornire l'infrastruttura normativa necessaria a rendere tale visione operativa, attraverso un'azione di semplificazione, consolidamento e chiarificazione del diritto europeo dei dati. In particolare, la proposta del *Digital Omnibus* di fondere più strumenti giuridici in un quadro unitario e coerente, accompagnata da misure di supporto all'attuazione del Data Act – quali clausole contrattuali tipo, *standard* per i servizi *cloud* e un *helpdesk* dedicato – mira a ridurre l'incertezza giuridica, ad abbattere i costi di *compliance* e a consentire agli operatori economici, soprattutto alle piccole e medie imprese (PMI) – per le quali l'accesso ai dati rappresenta una condizione essenziale per la scalabilità e la sopravvivenza competitiva nei mercati digitali – di concentrare le proprie risorse sull'innovazione.

In tale assetto, la *Data Union Strategy* individua tre assi prioritari di intervento: il rafforzamento dell'accesso ai dati per l'intelligenza artificiale, anche attraverso strumenti operativi quali i cd. *Data Labs* e servizi affidabili di pseudonimizzazione; la razionalizzazione delle regole sulla condivisione dei dati, inclusa la riforma dei meccanismi di consenso in materia di *cookie*, al fine di ridurre la “*consent fatigue*” senza – tuttavia – comprimere le tutele; e, infine, il rafforzamento della posizione dell'Unione nei flussi internazionali di dati, contrastando barriere commerciali ingiustificate e promuovendo condizioni di concorrenza eque a livello globale.

Questi rappresentano, secondo la prospettiva perseguita dalla *Data Union Strategy*, la fase evolutiva della Strategia europea per i dati del 2020 (su cui v. in questa Rubrica la notizia n. 1 nel numero 2/2020 [2020/2(1)FR] in PeM 2020, p. 149), la quale aveva di fatto posto le basi giuridiche e istituzionali di un mercato unico dei dati fondato, a sua volta, su tre pilastri fondamentali: la fiducia nei meccanismi di condivisione, la centralità della tutela dei diritti fondamentali e la promozione della circolazione volontaria delle informazioni come fattore di innovazione e crescita economica. È in tale fase che, in effetti, si collocano interventi normativi di primaria rilevanza, quali il *Data Governance Act*, il *Data Act* e il rafforzamento del quadro giuridico in materia di *open data*, che hanno progressivamente chiarito le condizioni di accesso, utilizzo e riutilizzo dei dati lungo l'intera catena del valore informativo.

Accanto all'intervento normativo, la Strategia del 2020 aveva altresì previsto un complesso di misure di accompagnamento istituzionale e infrastrutturale, tra cui il ruolo di coordinamento attribuito allo *European Data Innovation Board* e l'avvio di un processo di standardizzazione finalizzato alla costruzione di un *European Trusted Data Framework*.



Pur tuttavia, la Commissione riconosce che – nonostante taluni, decisivi, progressi – permangono criticità rilevanti, riconducibili, in particolare, a una implementazione nazionale disomogenea della normativa rilevante e alle persistenti incertezze circa il rapporto tra condivisione dei dati e tutela dei segreti commerciali, queste amplificate – altresì – dalla costante evoluzione tecnologica.

La Comunicazione prende dunque atto di tale mutamento, evidenziando come l'irruzione dell'intelligenza artificiale generativa e l'intensificarsi della competizione globale per il controllo delle risorse informative abbiano radicalmente modificato le condizioni di operatività del diritto dei dati. In tale scenario, emerge con particolare evidenza che la questione centrale non è più – o non è più soltanto – la carenza di regole, bensì l'incapacità dell'attuale quadro normativo e infrastrutturale di rendere concretamente disponibili, interoperabili e giuridicamente utilizzabili, su larga scala, grandi volumi di dati di elevata qualità.

Se, invero, la Strategia del 2020 aveva costruito un'architettura giuridica della fiducia, volta a rendere possibile la condivisione dei dati in un contesto di elevata protezione dei diritti, la *Data Union Strategy* mira ora a compiere un ulteriore salto qualitativo, trasformando tale architettura in una vera e propria infrastruttura operativa. L'obiettivo, cioè, non sembra più soltanto quello di rendere lecita e sicura la circolazione dei dati, ma di garantirne l'effettiva utilizzabilità come *input* essenziale per lo sviluppo, l'addestramento e la diffusione dei sistemi di intelligenza artificiale all'interno dell'ecosistema europeo.

In questo senso, la Comunicazione segna una discontinuità metodologica rispetto al passato: il diritto dell'Unione dei dati non è più concepito (prevalentemente) come strumento di contenimento dei rischi e di prevenzione degli abusi, ma viene progressivamente rifunzionalizzato come leva di politica industriale, tecnologica e competitiva.

Tale mutamento di prospettiva non implica (quantomeno, in via astratta) un arretramento rispetto ai valori fondativi dell'Unione, né una compressione delle garanzie poste a tutela dei diritti fondamentali; piuttosto, esso riflette la consapevolezza che un diritto dei dati esclusivamente difensivo rischia di tradursi, nel medio periodo, in un fattore di marginalizzazione tecnologica. La *Data Union Strategy* si colloca allora all'intersezione tra continuità assiologica e innovazione funzionale, proponendosi di riconciliare l'elevato livello di tutela giuridica raggiunto dall'Unione con l'esigenza di rendere i dati una risorsa effettivamente mobilitabile per l'innovazione e la sovranità digitale europea.

Ora, il cuore argomentativo della Comunicazione è rappresentato – alla luce delle considerazioni sinora svolte – dall'individuazione di tre sfide strutturali e interconnesse che l'Unione europea è chiamata ad affrontare con carattere di urgenza, in un contesto in cui le tecnologie e i servizi basati sull'intelligenza artificiale stanno ridefinendo in profondità gli equilibri economici, industriali e geopolitici a livello globale. Tali sfide – la *Data scarcity*, la *Regulatory complexity* e la *Global competition* – non vengono tuttavia presentate come criticità contingenti, bensì come nodi problematici (da sciogliere) che incidono direttamente sulla capacità dell'ordinamento

europeo di sostenere uno sviluppo dell'IA competitivo, affidabile e coerente con i propri valori fondativi.

In primo luogo, la Comunicazione individua così nella *Data scarcity*, intesa come carenza strutturale di *datasets* di alta qualità per l'addestramento dei sistemi di intelligenza artificiale avanzata, un vero e proprio collo di bottiglia per l'innovazione. L'ascesa dell'IA generativa, dei *large language models* (LLM) e dei modelli di *Agentic AI*, ha reso l'accesso a *dataset* caratterizzati da elevato volume, ampia diversità, specificità settoriale e grado di "novità", un fattore determinante di competitività globale.

Come evidenziato dalla Commissione sulla base di studi recenti, la dimensione dei *dataset* utilizzati per l'addestramento dei modelli linguistici di grandi dimensioni è infatti soggetta a una crescita esponenziale, con un raddoppio approssimativo ogni sei mesi, mentre le proiezioni indicano un possibile esaurimento delle fonti di dati pubblicamente disponibili entro un orizzonte temporale relativamente breve.

Il primo pilastro della *Data Union Strategy* viene dunque costruito come risposta strutturale al divario – tipicamente europeo – tra la disponibilità "formale" della risorsa informativa e la sua effettiva traducibilità in *input* operativo per l'innovazione, segnatamente per lo sviluppo e l'addestramento dell'intelligenza artificiale.

In tale scenario, la sfida per l'Unione si articola su un duplice piano: da un lato, rendere più ampiamente disponibili *dataset* di alta qualità, inclusi quelli di natura settoriale e specialistica; dall'altro, garantire l'accesso, su scala adeguata, alle infrastrutture computazionali necessarie per la loro elaborazione. La Commissione sottolinea invero come molte imprese europee, in particolare le PMI e le *start-up*, soffrano proprio di un *deficit* congiunto di volume e varietà dei dati, nonché di un accesso insufficiente alle capacità di calcolo disponibili a livello europeo e che, in assenza di interventi strutturali e coordinati, tale situazione rischia di tradursi in una dipendenza tecnologica crescente e in un progressivo arretramento competitivo dell'Unione nel panorama globale dell'IA.

Così, elemento cardine del primo pilastro è il rafforzamento e la messa a sistema dei *Common European Data Spaces* (CEDS) – già implementati dalla Strategia del 2020 – i quali cessano di essere rappresentati come mere sperimentazioni di settori economici strategici e ambiti di interesse pubblico, per essere – invece – qualificati come infrastruttura portante del mercato unico dei dati, fondata su *cloud*, regole di *governance* chiaramente determinate e meccanismi fiduciari di scambio tra attori pubblici e privati. In tal senso, la "fase successiva" delineata dalla Comunicazione consiste nel passaggio dalla pluralità disorganica di ecosistemi informativi alla costruzione di un *data ecosystem* senza soluzione di continuità, interoperabile e capace di incidere a livello unionale, anche mediante strumenti tecnici di raccordo e centri di supporto destinati ad agevolare soprattutto le PMI nella fruizione delle infrastrutture e delle regole.

In questo quadro, la Comunicazione introduce – a fianco dei CEDS – la figura dei *Data Labs* come snodo operativo essenziale: non meri "contenitori" o depositi di *dataset*, questi si configurano quali fornitori di servizi specializzati, destinati a collegare i CEDS all'ecosistema dell'IA, traducendo

la disponibilità dei dati in utilizzabilità tecnica. La Commissione insiste, in effetti, sulla funzione eminentemente strutturale dei *Data Labs*: questi offrono ambienti sicuri, strumenti pratici e supporto esperto per operazioni quali il *data pooling*, la *curation*, l'etichettatura e la pseudonimizzazione, fino all'anonimizzazione e alla generazione di dati sintetici, in modo da consentire – in particolare a *start-up*, *scale-up* e PMI – l'accesso a *dataset* di qualità senza perdita di controllo da parte dei *data holders*.

È precisamente in tale “catena di trasformazione” che l'accesso ai dati viene reso compatibile con la protezione degli interessi giuridicamente qualificati attraverso l'integrazione di tecniche *privacy-preserving* e decentralizzate, nonché tramite garanzie di riservatezza e modelli di trattamento dei dati.

La costruzione del pilastro non si esaurisce, peraltro, nella dimensione “micro” degli strumenti operativi; essa si articola altresì in una dimensione “macro” di infrastrutture e investimenti. Da un lato, infatti, la Commissione collega espressamente i *Data Labs* alle *AI Factories (EuroHPC)* e ad un futuro potenziamento verso *AI Gigafactories*, configurando un ecosistema integrato tra capacità computazionale e accesso ai dati. Dall'altro lato, annuncia un intervento normativo *ad hoc* – il *Cloud and AI Development Act* – finalizzato a garantire capacità sostenibili di *data center* e servizi sovrani di *cloud* e IA, riducendo dipendenze infrastrutturali *extra-UE*.

Particolare rilievo assume, inoltre, l'attenzione riservata ai “*strategic data assets*”: *dataset* pubblici (e in particolare i *high-value datasets*), risorse scientifiche, patrimoni culturali e linguistici, oltre ai dati giuridici e giudiziari attraverso lo sviluppo di un *European legal data space* basato su identificatori e metadati comuni. In tale contesto, la Commissione prospetta persino l'esplorazione di un *contract terms data pool* per l'automazione contrattuale: indicazione che, letta in controtelaio, rivela la proiezione del diritto dei dati oltre l'IA “industriale”, verso l'IA applicata ai processi giuridici e amministrativi.

In secondo luogo, la Comunicazione individua nella *Regulatory complexity* e nella frammentazione del quadro normativo una delle principali cause dell'inefficienza del mercato unico dei dati. A seguito della Strategia europea per i dati del 2020, l'Unione ha infatti adottato una serie di regolazioni di grande rilevanza, ciascuna delle quali ha affrontato specifiche dimensioni della catena del valore dei dati, quali i meccanismi di condivisione, la distribuzione equa del valore economico e la rimozione di requisiti di localizzazione eccessivamente onerosi. Tuttavia, come anticipato, l'interazione complessa tra tali strumenti e il *GDPR*, unitamente a un'attuazione disomogenea a livello degli Stati membri, ha prodotto un paesaggio regolatorio frammentato, caratterizzato da incertezza giuridica e da un significativo aumento dei costi di *compliance*, con effetti particolarmente gravosi per le imprese di minori dimensioni.

Così, il secondo pilastro – dedicato, appunto, alla semplificazione e razionalizzazione delle regole – costituisce il punto di saldatura tra visione strategica e impianto normativo; in tale cornice, la Comunicazione identifica segnatamente nel *Digital Omnibus* lo strumento cardine di modernizzazione e consolidamento del diritto orizzontale dei dati, diretto a eliminare oneri

superflui e a rendere l'ordinamento più praticabile per gli operatori, preservando i principi fondamentali dell'economia europea dei dati.

Infine, la Comunicazione affronta la sfida della *Global competition*, adottando una lettura esplicitamente geopolitica del dato quale *asset* strategico e assumendo la *data sovereignty* quale categoria ordinante del futuro digitale europeo. Nell'attuale competizione internazionale sull'intelligenza artificiale, l'accesso a dati di elevato valore costituisce invero un vantaggio decisivo, e le politiche di localizzazione, controllo e restrizione dei flussi informativi sono sempre più utilizzate come strumenti di potere economico e politico.

Alla luce di tali dinamiche, la Commissione afferma dunque la necessità di riconoscere il dato come risorsa strategica primaria per l'Unione, imponendo un rafforzamento degli investimenti in *dataset* sicuri, interoperabili e di alta qualità, coerenti con i valori e gli *standard* europei. Il rafforzamento della capacità dell'Unione di raccogliere, curare e utilizzare i propri dati viene così configurato non soltanto come un obiettivo di politica industriale, ma come un imperativo di sicurezza e di sovranità digitale, volto a garantire flussi informativi vantaggiosi, a proteggere i dati non personali sensibili e a sostenere l'autonomia strategica europea in un contesto di crescente rivalità tecnologica.

In chiusura, appare opportuno collocare la *Data Union Strategy* entro una più ampia traiettoria di politica del diritto dell'Unione, cogliendone – con la necessaria cautela – i tratti di un possibile cambio di rotta dell'impostazione europea in materia di dati, soprattutto se la Comunicazione del 2025 viene letta in combinazione con il disegno di rifusione e semplificazione normativa sotteso al *Digital Omnibus*.

Pur senza rinnegare esplicitamente l'impianto assiologico che ha sinora caratterizzato l'*acquis* europeo – fondato sulla centralità della tutela dei diritti fondamentali, sulla fiducia e sulla legalità del trattamento – la Strategia manifesta infatti un mutamento significativo di accento nell'azione dell'Unione, la quale viene consapevolmente riallineata, secondo la formula dichiaratamente evocata del *from rules to results*, verso una valorizzazione più marcata della dimensione produttiva, abilitante e infrastrutturale del diritto dei dati. In tal senso, il dato viene progressivamente assunto non solo come oggetto di protezione, ma come fattore essenziale di competitività, scalabilità e impatto economico dell'innovazione, in particolare nell'ecosistema dell'intelligenza artificiale.

In questa prospettiva, la *Data Union Strategy* segna un passaggio cruciale nell'evoluzione del diritto europeo dei dati, poiché mira – almeno in parte – a contenere e riequilibrare la fase “costituente” che ha caratterizzato il decennio precedente, contrassegnata da una proliferazione di strumenti normativi e dalla costruzione di un perimetro garantistico ampio e articolato, spesso percepito, sul piano applicativo, come prevalentemente restrittivo dell'utilizzo dei dati. Al contempo, essa apre una fase eminentemente attuativa, incentrata sull'effettività delle regole e sulla traduzione operativa della risorsa informativa in infrastruttura funzionale allo sviluppo, all'addestramento e al dispiegamento dei sistemi di intelligenza artificiale.

Il tratto rivelatore di tale passaggio è rinvenibile nell'enfasi posta non soltanto sul consolidamento dei *CEDS*, ma soprattutto sulla predisposizione di un insieme coerente di strumenti destinati a rendere i dati concretamente utilizzabili: dai *Data Labs* agli ambienti di trattamento fidati, dalle tecniche *privacy-preserving* al *data pooling*, dagli *standard* di qualità ai dati sintetici. L'obiettivo dichiarato è, propriamente, quello di ridurre l'inerzia strutturale che separa il dato "disponibile" dal dato effettivamente "impiegabile" per l'addestramento e il *deployment* dei sistemi di IA, superando così uno dei principali colli di bottiglia dell'ecosistema europeo dell'innovazione.

Una lettura orientata induce, tuttavia, a interrogarsi sulla tensione strutturale che tale riconfigurazione inevitabilmente porta con sé. La funzionalizzazione del diritto dei dati a fini di politica industriale e tecnologica, soprattutto se inscritta nel contesto del *Digital Omnibus*, rischia infatti di proiettare l'*acquis* europeo da un paradigma di protezione prevalentemente "limitativa" verso un paradigma più marcatamente "abilitante". In tale nuovo assetto, la semplificazione normativa può assumere, almeno in parte, la fisionomia di una liberalizzazione regolata dell'uso dei dati; la Comunicazione stessa lascia intravedere tale direzione quando individua nell'incertezza giuridica uno dei principali fattori di disincentivo alla condivisione dei dati e, correlativamente, una delle cause dell'insufficiente disponibilità di *dataset* idonei allo sviluppo dell'IA, nonché quando, più in generale, propone la semplificazione come strumento per ridurre i costi di *compliance* e rendere l'ordinamento europeo più "*innovation friendly*".

Proprio per questo, la questione decisiva diviene quella dell'equilibrio tra valorizzazione economico-tecnologica del dato e presidio sostanziale dei diritti fondamentali. La trasformazione del dato in "risorsa strategica" dell'Unione presuppone infatti che la riduzione della complessità normativa – pur necessaria per garantire l'effettività del mercato unico dei dati – non si traduca, nella prassi applicativa, in un arretramento delle garanzie, né in un indebolimento del controllo sui processi di raccolta, riuso e circolazione delle informazioni. Al contempo, deve riconoscersi che un diritto dei dati concepito esclusivamente come limite, e strutturalmente incapace di rendere possibile la costruzione e l'addestramento di modelli competitivi, rischia di produrre – di converso – un effetto paradossale, trasformandosi esso stesso in fattore di marginalizzazione tecnologica e, in ultima analisi, di perdita di sovranità digitale.

In definitiva, la *Data Union Strategy*, letta unitamente al *Digital Omnibus*, sembra rappresentare il tentativo più ambizioso di rifondare il diritto europeo dei dati come diritto della circolazione regolata e dell'uso responsabile dell'informazione: un diritto che non abdica alla propria identità valoriale, ma la riconfigura in chiave funzionale, assumendo l'innovazione – e segnatamente l'intelligenza artificiale – come banco di prova dell'effettività del mercato unico e come criterio ordinante della razionalizzazione dell'*acquis*.

CARLA FAILLA

<https://digital-strategy.ec.europa.eu/en/library/data-union-strategy-unlocking-data-ai>

2025/4(5)ESt

Il pacchetto “Digital Omnibus”: la proposta della Commissione europea COM(2025) 837 final del 19.11.2025 di modifica del GDPR, del Data Act, del regolamento sullo sportello unico digitale e delle direttive e-privacy, NIS2 e CER, nonché di abrogazione della direttiva Open Data, del Data Governance Act, del regolamento P2B e del regolamento sulla libera circolazione dei dati non personali

| 1033

Il 19 novembre 2025, la Commissione europea (la **Commissione**) ha pubblicato due proposte di regolamento nel quadro del cd. pacchetto “Digital Omnibus”, comprendente una serie di misure volte a promuovere lo sviluppo digitale dell’UE. Il Digital Omnibus è in linea di continuità con le finalità di semplificazione normativa, competitività ed attrazione di investimenti dichiarate dal “[Pacchetto Omnibus](#)”, che comprende una pluralità di misure già annunciate a partire dal febbraio 2025 in molti altri settori (c.d. [Omnibus I](#)).

Nello specifico, il Digital Omnibus riguarda due proposte di regolamento:

- la COM(2025) 837 relativa al cd. “*data acquis*” europeo di modifica dei regolamenti (UE) 2016/679 (**GDPR**), 2018/1724 (**sullo sportello unico digitale**), 2018/1725 (**EUDPR**), 2023/2854 (**Data Act**) e le direttive 2002/58/CE (**e-privacy**), 2022/2555 (**NIS2**) e 2022/2557 (**CER**) e di abrogazione dei regolamenti (UE) 2018/1807 (**sulla libera circolazione dei dati non personali**), 2019/1150 (**P2B**), 2022/868 (**Data Governance Act**) e della direttiva (UE) 2019/1024 (**Open Data**).
- la COM(2025) 836 specificamente dedicata al regolamento (UE) 2024/1689 (**AI Act**) (su cui v. *infra* il contributo n. 6 in questo numero di questa Rubrica [2025/4(6)ESt]).

Gli emendamenti legislativi proposti nella COM(2025) 837 (la **Proposta**) si concentrano sullo sblocco di opportunità nell'utilizzo dei dati come risorsa fondamentale nell'economia UE, anche in vista dello sviluppo e dell'utilizzo di soluzioni di IA nel mercato interno. Si tratta di un obiettivo coerente alla Strategia europea dei dati di cui alla COM(2025) 835 final significativamente intitolata “**Unlocking data for AI**” (sulla quale v. *supra* in questo numero di questa Rubrica la notizia n. 4 [2025/4(4)CF]).

Le basi giuridiche di adozione della Proposta sono gli artt. 114 e 16 del TFUE, riflettendo i presupposti giuridici di adozione degli atti normativi oggetto di emendamento.

Il presupposto di questa iniziativa legislativa pare risiedere nella complessità giuridica e nel conseguente rischio di sovrapposizioni, disallineamenti definitivi e dubbi sull'interrelazione tra i diversi strumenti legislativi del cd. “*data acquis*”.

Per questo motivo, la Proposta include innanzitutto una semplificazione dei regolamenti UE sul libero scambio dei dati, ossia il Data Governance Act, il Data Act e la Direttiva open data, attraverso la **previsione di un unico**



strumento legislativo - consolidato nel Data Act - per l'economia europea dei dati con l'abrogazione degli altri strumenti menzionati.

In conseguenza del disegno di consolidazione delle norme provenienti dalle fonti abrogate, viene ampliato l'ambito di applicazione del Data Act, per includervi:

- le disposizioni in materia di **servizi di intermediazione e di organizzazione per l'altruismo dei dati** (norme provenienti dal Data Governance Act: **nuovo Capitolo VII-bis del Data Act**);
- le norme relative alla libera circolazione dei **dati non personali** e ai divieti di localizzazione dei dati (norme provenienti dal regolamento sulla libera circolazione dei dati non personali: **nuovo Capitolo VII-ter del Data Act**);
- la disciplina del riutilizzo di dati e documenti detenuti da enti pubblici (norme provenienti dalla direttiva open data e dal Data Governance Act: **nuovo Capitolo VII-quater del Data Act**).

Nel merito, *inter alia*, la Proposta prevede:

- la **semplificazione** di una serie di regole (già contenute nel Data Governance Act, e che confluirebbero nel Data Act consolidato) come, ad esempio, le disposizioni sull'**altruismo dei dati** e i **servizi di intermediazione dei dati**, al dichiarato fine di migliorare l'attività di tali meccanismi;
- una nuova norma ai sensi dell'art. 4(8) Data Act che consente ai detentori di dati di rifiutare la divulgazione di **segreti commerciali** a un utente quando sussiste un rischio elevato di acquisizione, uso o divulgazione illecita verso **paesi terzi**, o entità sotto il loro controllo, soggetti a giurisdizioni con tutele più deboli rispetto a quelle disponibili in UE;
- una nuova disposizione applicabile alle richieste di dati da parte degli enti pubblici durante le **emergenze pubbliche**, quando necessarie per rispondere a un'emergenza pubblica oppure per mitigare o sostenere il superamento di tale circostanza;
- la modifica del Data Act per eliminare l'obbligo per i fornitori di *smart contract* di conformarsi ai c.d. **requisiti essenziali relativi ai contratti intelligenti** per l'esecuzione degli accordi di condivisione dei dati, come attualmente previsti nel Data Act, prevedendo invece una delega alla Commissione per adottare norme armonizzate;
- l'abrogazione di diverse altre disposizioni ritenute obsolete, specialmente in materia di libero scambio di **dati non personali** con le eccezioni nel divieto di localizzazione dei dati nell'Unione (nuovo Capo VII-ter);
- la possibilità per le pubbliche amministrazioni di stabilire diverse condizioni e di imporre **costi maggiori per il riutilizzo dei dati** da loro detenuti **da parte dei gatekeeper**, nel senso inteso dal DMA;
- l'estensione delle disposizioni che facilitano il rispetto della legislazione europea in materia di dati per le piccole e medie imprese alle *Small mid cap companies* (SMC), in linea di continuità con altre proposte intese a favorire questa categoria di recente introdotta nell'ordinamento giuridico (tra le quali la proposta di regolamento COM(2025) 501 final del 21.5.2025 di modifica del GDPR per l'estensione a questa categoria di determinate misure di attenuazione disponibili per le PMI: su cui v. in questa Rubrica la notizia n. 5

nel [numero 2/2025](#) [2025/2(5)EMI], in *PeM* 2025, p. 622) e come proposto anche nel pacchetto Omnibus I.

Per quanto riguarda la **protezione dei dati personali**, la proposta di Regolamento introduce numerosi e “mirati” emendamenti al GDPR e all’EUDPR nonché della direttiva e-privacy. In particolare, ed *inter alia*, la Proposta prevede:

- la **modifica della definizione di dato personale**, relativizzandone la natura, con particolare riguardo al **dato pseudonimizzato** che non manterrebbe in tutti i casi la natura di dato personale, contestualmente, conferendo alla Commissione il potere di adottare atti di esecuzione per specificare i mezzi e i criteri volti a determinare se i dati risultanti dalla pseudonimizzazione non costituiscano più dati personali per determinati soggetti;
- l'introduzione delle **definizioni di «apparecchiatura terminale», «browser web», «servizio di media», «fornitore di servizi di media», «interfaccia online» e «ricerca scientifica»;**
- la **modifica della formulazione del principio di limitazione delle finalità**, per cui il successivo trattamento di dati personali è considerato compatibile con le finalità originarie a prescindere dalle specifiche condizioni di liceità applicabili a tali ipotesi;
- **due nuove «esenzioni» al divieto generale di trattare categorie particolari di dati** (nuovo art. 9(2) lettere (k) e (l) del GDPR), qualora (1) il trattamento avvenga nel contesto dello **sviluppo e del funzionamento di un sistema o modello di IA**, o 2) **il trattamento dei dati biometrici sia necessario per la conferma dell'identità di un interessato**, se i dati biometrici o i mezzi necessari per tale attività di verifica sono sotto il controllo esclusivo dell'interessato;
- la modifica dell'art. 12(5) del GDPR, per cui **il titolare ha facoltà di rifiutare di dare seguito alla richiesta di accesso o applicare un costo ragionevole per l'istanza qualificabile come «eccessiva» o «manifestamente infondata»;**
- la **semplificazione dei requisiti di informativa**, ove il titolare possa “ragionevolmente” ritenere che l'interessato sia a conoscenza del trattamento in vigore di un rapporto “chiaro e circoscritto” con l'interessato, salvo ricorrano specifiche circostanze (trasmissione dei dati a destinatari, trasferimento verso un Paese terzo, effettuazione di processi decisionali automatizzati e trattamenti con rischio elevato per i diritti dell'interessato);
- **l'integrale sostituzione dei primi due paragrafi dell'art. 22 GDPR**, con una nuova formulazione che sancisce la liceità di decisioni fondate su un trattamento esclusivamente automatizzato (con conseguente soppressione del riferimento al diritto dell'interessato a non essere soggetto a tale decisione) alle condizioni fissate nel paragrafo 2 dell'art. 22 (precisando che, se la decisione sia necessaria per la stipulazione o l'esecuzione di un contratto, si possa prescindere dalla verifica dell'esistenza di un'alternativa meno invasiva);
- la **modifica dei presupposti, tempi e modalità per la notifica di una violazione di dati personali**, da effettuare solo in caso di rischio



“elevato” per i diritti dell’interessato, con estensione dei termini per la notifica (da 72 a 96 ore), tramite un punto di contatto unico europeo trasversale ai sensi del Regolamento (UE) 910/2014 (**eIDAS**), 2022/2554 (**DORA**) e della direttiva CER;

- la **modifica dell’art. 35 GDPR**, prevedendo a livello UE la definizione di elenchi unici di operazioni di trattamento soggetti, o meno, alla valutazione d’impatto, verso l’armonizzazione della nozione di “rischio elevato”, con contestuale obbligo dell’EDPB di predisporre delle proposte di tali elenchi, di un modello e di una metodologia comuni di DPIA, da adottare con atto di esecuzione della Commissione UE;
- una **disciplina unificata di manifestazione del consenso per l’accesso a e la memorizzazione di informazioni sul terminale dell’utente** (di cui all’attuale art. 5(3) della direttiva e-privacy), trasponendo nel GDPR l’unica base normativa cui fare riferimento per tutti i trattamenti svolti su o a partire da un tale terminale.

ELISABETTA STRINGHI

<https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>

2025/4(6)ESt

(segue) il pacchetto “Digital Omnibus”: la proposta della Commissione europea “Digital Omnibus on AI” COM(2025) 836 final del 19.11.2025 di modifica dell’AI Act

Gli emendamenti legislativi al reg. (UE) 2024/1689 (**AI Act** o **AIA**) proposti nella COM(2025) 836 del 19.11.2025 (la **Proposta**) sono finalizzati ad assicurare un’attuazione più efficiente delle norme già concordate a livello politico. Come si evince dalla relazione di accompagnamento alla Proposta, ad avviso della Commissione europea (la **Commissione**) tali emendamenti non sono destinati a modificare l’impatto dell’AI Act sui diritti fondamentali, poiché – così si argomenta - la natura mirata delle modifiche previste non incide né sull’ambito di applicazione dei sistemi di intelligenza artificiale (IA) disciplinati né sui requisiti sostanziali applicabili a tali sistemi. L’art. 114 del Trattato sul funzionamento dell’Unione europea (**TFUE**) è la base giuridica di adozione della Proposta, che consta di 3 articoli e 26 considerando.

Appare opportuno cominciare con il segnalare le modifiche previste dalla Proposta alla **decorrenza dell’applicazione della maggior parte delle disposizioni dell’AI Act**. Per gli obblighi relativi ai sistemi di IA ad alto rischio di cui al capo III, viene introdotto un meccanismo che collega l’entrata in applicazione di tali norme alla disponibilità di misure di supporto alla conformità all’AI Act sui sistemi ad alto rischio, quali **norme armonizzate, specifiche comuni e linee guida della Commissione**. Tale **disponibilità sarà confermata dalla Commissione mediante decisione**, a seguito della quale le norme sui sistemi di IA ad alto rischio inizieranno ad applicarsi **dopo un adeguato periodo transitorio**. La Proposta aggiunge che tale flessibilità

dovrà applicarsi solo per un periodo limitato, e dovrà essere fissata una data certa entro la quale le norme si applicheranno in ogni caso; inoltre, è opportuno distinguere tra le due tipologie di sistemi di IA qualificati come ad alto rischio e prevedere un periodo transitorio più lungo per i sistemi di IA che rientrano nella classificazione di alto rischio ai sensi dell'art 6, par. 1 e dell'Allegato I dell'AI Act. In proposito, viene chiarito che le modifiche necessarie per integrare i requisiti per i sistemi di IA ad alto rischio nella normativa settoriale elencata nella sezione B dell'Allegato I si applicano a decorrere dall'entrata in vigore del Regolamento "Digital Omnibus on AI". Venendo alle altre modifiche, la Proposta prevede a beneficio delle *Small mid cap companies* (SMC), una serie di misure volte a supportare l'innovazione di tali imprese. In particolare, sono estese alle SMC le agevolazioni regolatorie già previste per le PMI, in materia di **documentazione tecnica** e di istituzione di un **sistema di gestione della qualità** che tenga conto delle loro dimensioni.

Viene riformulato l'art. 4 AIA, obbligando la Commissione e gli Stati membri a promuovere un «sufficiente livello» di **alfabetizzazione** in materia di IA, mentre i fornitori e i *deployer* di sistemi di IA sono solo incoraggiati ad adottare le misure per assicurare tale livello di consapevolezza tra i loro dipendenti e operatori.

È prevista l'introduzione di un nuovo articolo 4-*bis*, che sostituirebbe l'art. 10(5) AIA e che fornirebbe una base giuridica ai fornitori e ai *deployer* di sistemi e modelli di IA per **trattare in via eccezionale le categorie particolari di dati personali** ex art. 9(1) reg. (UE) 2016/679 (GDPR), **al fine di garantire il rilevamento e la correzione dei *bias* e la protezione dei diritti fondamentali, a determinate condizioni.**

Viene, inoltre, **soppresso l'obbligo per i fornitori di registrare i sistemi di IA** nel *database* UE dei sistemi ad alto rischio di cui all'Allegato III all'AI Act, qualora i fornitori si ritengano esentati dalla classificazione «ad alto rischio» ai sensi dell'art. 6(3) AIA (ad es. perché utilizzati esclusivamente per attività meramente preparatorie). Quindi, il fornitore è tenuto a conservare la documentazione interna che dimostri la valutazione effettuata e la giustificazione dell'esenzione, senza alcun obbligo di notifica o di registrazione esterna.

Per quanto concerne l'Autorità di notifica e il coordinamento con la legislazione armonizzata UE di sicurezza dei prodotti, è introdotta una nuova procedura in base alla quale gli Stati membri sono tenuti a garantire che un organismo di valutazione della conformità che presenti domanda di designazione sia ai sensi dell'AI Act, sia ai sensi della legislazione armonizzata di cui alla sezione A dell'Allegato I dell'AI Act, possa presentare un'**unica domanda** ed essere sottoposto a un'**unica procedura di valutazione per la designazione**. Viene, inoltre, chiarito il rapporto tra la procedura di valutazione della conformità prevista dall'art. 43 AIA nei casi in cui un sistema di IA ad alto rischio sia disciplinato dalla legislazione armonizzata UE elencata nella sezione A dell'Allegato I dell'AI Act, nonché nei casi in cui un sistema di IA sia classificato come ad alto rischio sia ai sensi dell'Allegato I sia ai sensi dell'Allegato III dell'AI Act: sia nel primo, sia nel

secondo caso nella valutazione di conformità si deve tener conto della **legislazione di armonizzazione rilevante** e si segue la relativa procedura.

Sono, inoltre, introdotte modifiche in materia di *sandbox* regolatorie per l'IA di cui all'art. 57 AIA, autorizzando l'AI Office a istituire una **sandbox regolatoria a livello UE** per determinati sistemi di IA rientranti nella sua competenza esclusiva di vigilanza e imponendo agli Stati membri di rafforzare la **cooperazione transfrontaliera tra sandbox nazionali**. Sono conferiti appositi poteri di esecuzione alla Commissione per la definizione delle modalità di istituzione, sviluppo, attuazione, funzionamento, *governance* e vigilanza delle *sandbox* regolatorie per l'IA.

La Proposta modifica anche la **sperimentazione dei sistemi di IA ad alto rischio in condizioni reali** al di fuori delle *sandbox* regolatorie per l'IA, disciplinata dall'art. 60 AIA, estendendo la possibilità di testare i sistemi di IA ad alto rischio in condizioni reali al di fuori di questi spazi controllati anche ai sistemi di IA ad alto rischio disciplinati dalla sezione A dell'Allegato I all'AI Act, ossia i sistemi coperti dalla legislazione armonizzata UE.

Il potere della Commissione previsto dall'art. 72 dell'AI Act di adottare un atto di esecuzione in materia di piano di **monitoraggio post-commercializzazione** è sostituito dal potere di adottare linee guida a tal proposito.

Viene rafforzata la competenza dell'AI Office in materia di vigilanza e *enforcement* nei confronti di taluni **sistemi di IA basati su un modello di IA per finalità generali**, quando il modello e il sistema sono forniti dallo **stesso fornitore**. La vigilanza e l'applicazione della conformità dei sistemi di IA integrati in piattaforme o motori di ricerca online di grandi dimensioni (cd. **VLOPs e VLOSEs**) rientrano nella competenza dell'AI Office e, dunque, sottratti alla competenza della Commissione. Alla Commissione è conferito il potere di adottare atti di esecuzione per definire i poteri di applicazione e le procedure per l'esercizio di tali poteri da parte dell'AI Office, introducendo un **rinvio al regolamento (UE) 2019/1020 sulla vigilanza del mercato e sulla conformità dei prodotti**, per assicurare specifiche garanzie procedurali ai fornitori interessati. Inoltre, è attribuito alla Commissione il potere di effettuare valutazioni di conformità dei sistemi di IA basati su un modello di IA per finalità generali, entrambi forniti dallo stesso fornitore.

Viene riformulato anche l'**art. 77 AIA** con riferimento ai poteri delle autorità o degli organismi incaricati della tutela dei diritti fondamentali e alla cooperazione con le Autorità di vigilanza. In particolare, viene ampliato il raggio d'azione delle Autorità di tutela dei diritti fondamentali, che non è più limitato solo ai sistemi di IA ad alto rischio di cui all'Allegato III dell'AIA, ma è esteso a **tutti i sistemi di IA**. Il potere d'accesso e richiesta documentale di tali Autorità è esteso anche alle «informazioni», ma viene al contempo ridimensionato ed esclusivamente riferito a **documentazione e informazioni formate e in disponibilità delle Autorità di vigilanza**. Queste ultime sono tenute a concedere alle Autorità di tutela dei diritti fondamentali l'accesso alle informazioni o alla documentazione pertinenti, anche richiedendo tali informazioni o documentazione al fornitore o al deployer «ove necessario». Le Autorità cooperano strettamente e si prestano reciproca assistenza necessaria all'esercizio dei rispettivi mandati, al fine di garantire

un'applicazione coerente dell'AI Act e del diritto UE in materia di tutela dei diritti fondamentali. La cooperazione include, in particolare, lo scambio di informazioni, ove necessario, per l'efficace vigilanza o applicazione dell'AIA e della restante legislazione antidiscriminatoria dell'Unione.

Infine, sono apportate modifiche all'**art. 111 AIA**. Nello specifico è introdotto un periodo transitorio di 6 mesi per i fornitori che devono integrare retroattivamente soluzioni tecniche nei propri sistemi di IA generativa, al fine di renderli leggibili dalle macchine e rilevabili come contenuti generati o manipolati artificialmente.

ELISABETTA STRINGHI

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836>

2025/4(7)SO

Approvato dalla Commissione europea il 1.8.2025 il primo codice di buone pratiche per i modelli di IA per finalità generali

Il 1 agosto 2025 la Commissione europea (la **Commissione**) ha approvato il primo 'codice di buone pratiche per i modelli di IA per finalità generali' (il **Codice GPAI 2025**).

I codici di buone pratiche per i modelli di IA per finalità generali costituiscono uno strumento previsto dal regolamento (UE) 2024/1689 (**AI Act** o **AIA**). L'AI Act stabilisce la loro funzione, la possibilità e le conseguenze della loro approvazione da parte della Commissione, il loro rapporto con le «norme armonizzate» ex art. 40 AIA, e la loro valutazione da parte dell'Ufficio per l'IA e del comitato costituiti ai sensi del medesimo AI Act (**l'Ufficio per l'IA** e il **EAIB**).

Quanto alla loro funzione, si legge nel Considerando 117 AIA che i codici di buone pratiche costituiscono «uno strumento essenziale per i fornitori di modelli di IA per finalità generali ai fini di un'adeguata conformità agli obblighi previsti dall'AI Act», e che «i fornitori dovrebbero poter fare affidamento su codici di buone pratiche per dimostrare la conformità agli obblighi». Il medesimo Considerando 117 AIA aggiunge che «la Commissione può decidere di approvare un codice di buone pratiche e conferire ad esso una validità generale all'interno dell'Unione o, in alternativa, di stabilire norme comuni per l'attuazione dei pertinenti obblighi, qualora un codice di buone pratiche non possa essere portato a termine o ritenuto adeguato da parte dell'ufficio per l'IA entro la data di applicazione del presente regolamento».

L'articolo 56 AIA (contenuto nel capo V dell'AI Act, intitolato 'Modelli di IA per finalità generali') prevede *inter alia* che l'Ufficio per l'IA incoraggi l'adozione di codici di buone pratiche e che l'Ufficio per l'IA e l'EAIB «mirano a garantire» il rispetto da parte dei codici di buone pratiche degli obblighi posti a carico dei fornitori di modelli di IA per finalità generali previsti dall'art. 53 AIA e degli obblighi posti a carico dei fornitori di modelli di IA per finalità generali con rischio sistemico, previsti dall'art. 55 AIA.



L'art. 56 AIA prevede inoltre che quando la Commissione approva un codice di buone pratiche (come atto di esecuzione, da adottarsi secondo la relativa procedura d'esame), gli conferisce una validità generale all'interno dell'Unione.

Gli artt. 53(4) e 55(2) AIA, a loro volta, dispongono che i fornitori di modelli di IA per finalità generali e quelli di modelli di IA per finalità generali con rischio sistemico **possono basarsi su codici di buone pratiche per dimostrare la conformità ai loro obblighi ai sensi dell'AIA finché non siano pubblicate norme armonizzate che contemplano tali obblighi**, la conformità alle quali ultime «garantisce» a quel punto a tali fornitori «una presunzione di conformità».

Invece, i fornitori che **non** aderiscono a un codice di buone pratiche approvato, debbono – sempre secondo gli artt. 53(4) e 55(2) AIA – dimostrare «mezzi alternativi adeguati di conformità ai fini di approvazione da parte della Commissione».

Nel pubblicare il Codice GPAI 2025, la Commissione ha dichiarato che esso è stato scritto da [esperti indipendenti](#) in un processo multi-stakeholder, al termine di una lunga [fase di elaborazione](#), in esito alla quale, il 1 agosto 2025 l'Ufficio IA ha dato la sua valutazione positiva e la Commissione lo ha approvato. La tempistica riflette la previsione di cui all'ultimo capoverso dell'art. 56 AIA a tenore del quale, «[q]ualora entro il 2 agosto 2025 un codice di buone pratiche non potesse essere portato a termine o l'Ufficio per l'IA non avesse fornito una valutazione positiva, la Commissione avrebbe potuto prevedere, mediante atti di esecuzione, norme comuni per l'attuazione degli obblighi di cui agli articoli 53 e 55 [AIA] [...]»

Il Codice GPAI 2025 è stato [pubblicato il 10 luglio 2025](#) (prima dell'approvazione da parte della Commissione). Per facilitarne la fruizione, la Commissione ha pubblicato

- (i) delle [linee guida sugli obblighi dei fornitori di modelli IA per finalità generali](#);
- (ii) delle domande e risposte [\(Q&A\) sul Codice GPAI 2025](#).

I firmatari del Codice GPAI 2025 hanno costituito una “[task-force](#)” con lo scopo di scambiarsi opinioni in merito all'applicazione in concreto del medesimo codice, e l'Ufficio per l'IA ha pubblicato un “vademecum” preparato dalla task-force con la lista dei primi firmatari, che risultano essere le seguenti società (altre se ne sono aggiunti successivamente, e potranno ancora aggiungersene, il codice essendo aperto alla firma):

- Accexible,
- AI Alignment Solutions,
- Aleph Alpha,
- Amazon,
- Anthropic,
- Black Forest Labs,
- Bria,
- Cohere,
- Cyber Institute,
- Domyn,

- Dweve,
- Fastweb,
- Google,
- Humane Technology,
- IBM,
- LINAGORA,
- Microsoft,
- Mistral,
- OpenAI,
- Open Hippo,
- ServiceNow,
- Virtuo Turing,
- WRITER.

Il Codice GPAI 2025 si compone di 3 capitoli, intitolati e dedicati, rispettivamente alla **Trasparenza**, al **Diritto d'autore**, e alla **Sicurezza**. Il capitolo sulla Sicurezza si applica soltanto ai fornitori di modelli IA per finalità generali con rischio sistemico, ex art. 55 AIA.

SALVATORE ORLANDO

<https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>

2025/4(8)FPa

La prima bozza del codice di buone pratiche sulla trasparenza dei contenuti generati dalla IA pubblicata il 17.12.2025

La crescente circolazione di contenuti generati dalla, o con l'ausilio della, intelligenza artificiale (IA) pone una serie di problematiche in merito all'affidabilità e alla veridicità di quanto appare online. Accanto ai casi di plateali *fake news*, questo strumento viene altresì impiegato per svolgere delle funzioni quali creazione di contenuti, scritti, video o di altro genere, che, per la loro natura, sono in grado di confondere anche l'utente o il consumatore più attento. Non sorprende, pertanto, che la risposta normativa ai rischi derivanti da un uso opaco dell'IA si sia concentrata, tra gli altri profili, sul principio di trasparenza. Tale principio trova una declinazione esplicita nell'articolo 50 del regolamento (UE) 2024/1689 (**AI Act** o **AIA**), il quale stabilisce che gli utenti debbano essere informati del fatto che stanno interagendo con un sistema di IA, salvo che ciò non risulti evidente per una persona fisica "ragionevolmente ben informata, attenta e prudente, tenendo conto delle circostanze e del contesto di utilizzo" (art. 50(1) AIA). La trasparenza assume così una funzione essenziale di prevenzione dei rischi di *impersonation* e *deception*, che possono manifestarsi indipendentemente dalla qualificazione del sistema come ad alto rischio.

In questo quadro si inserisce la prima bozza del *Codice di buone pratiche sulla trasparenza dei contenuti generati o manipolati dall'IA*, pubblicata dalla Commissione europea il 17 dicembre 2025 (il **Codice**). Il Codice mira



a garantire che i contenuti generati o manipolati dalla IA siano **contrassegnati attraverso formati leggibili da macchine, rilevabili e interoperabili**, consentendo al contempo agli individui di identificare *deepfake* e testi generati dall'IA, in particolare quando diffusi su questioni di interesse pubblico (si vedano, in tal senso, i Considerando 132, 133 e 135 e l'art. 50(7) dell'AI Act).

Il processo di elaborazione del Codice ha coinvolto un numero elevato di *stakeholder*, provenienti dall'industria, dal mondo accademico, dalla società civile e dagli Stati membri, a conferma della rilevanza sistemica del tema e della volontà di costruire uno strumento condiviso.

L'impostazione del codice - Un elemento particolarmente significativo del Codice risiede nella sua struttura, articolata attorno alla **distinzione tra obblighi in capo ai provider**, ossia i fornitori dei sistemi di IA, e quelli gravanti sui **deployer**, vale a dire i soggetti che utilizzano tali sistemi. Questa distinzione, formalizzata anche nella creazione di due gruppi di lavoro separati, non costituisce un mero accorgimento organizzativo, ma riflette una scelta di fondo sul piano regolatorio. Essa chiarisce, infatti, che la responsabilità della trasparenza non può essere concentrata esclusivamente sull'utilizzatore finale del contenuto, ma deve essere distribuita lungo l'intera filiera dell'IA, dalla progettazione del sistema fino alla diffusione del contenuto generato o manipolato. Allo stato dell'arte, difatti, non esiste una tecnologia che sia unica e infallibile nell'individuare i contenuti generati da AI: a questo scopo, nella bozza, si suggerisce di adottare un **approccio multilivello, ossia combinare metadati con altre tecniche come fingerprinting**. In particolare, le aziende che forniscono sistemi di AI dovranno essere in grado di mettere a disposizione strumenti di verifica, per consentire a utenti e piattaforme, e Autorità di controllare se un contenuto è generato con l'IA.

Per gli utilizzatori dei sistemi, invece, gli obblighi consistono nel **segnalare** in modo chiaro e immediato i *deepfake*, ossia contenuti audiovisivi artificialmente generati o manipolati che appaiono autentici. Nell'ottica di contrastare la diffusione di contenuti ingannevoli e fenomeni di disinformazione, i *deployer* dovranno inoltre indicare quando video, immagini o testi sono stati generati o alterati dall'intelligenza artificiale, in particolare se diffusi al pubblico su **temi di interesse generale**. Tale obbligo assume una rilevanza specifica nel caso dei contenuti informativi, in cui il rischio di interferenze con la formazione dell'opinione pubblica risulta particolarmente elevato.

Pur trattandosi di una prima bozza, e dunque di un testo suscettibile di ulteriori modifiche, emerge già con chiarezza l'impostazione di fondo del Codice. Esso propone una tassonomia comune dei contenuti integralmente generati dall'IA e di quelli prodotti con il suo ausilio, **senza operare una distinzione netta tra le due ipotesi**. Se da un lato tale scelta risponde a un'esigenza di semplificazione e di maggiore certezza applicativa, dall'altro essa solleva interrogativi rilevanti, soprattutto in prospettiva di attribuzione delle responsabilità. In particolare, in casi quali la diffusione di contenuti diffamatori o ingannevoli, una differenziazione più marcata tra contenuti

pienamente automatizzati e contenuti frutto di un intervento umano significativo potrebbe risultare maggiormente funzionale sul piano giuridico.

Possibili sviluppi

Svolte le considerazioni di carattere descrittivo, appare opportuno soffermarsi su alcuni profili di diritto sostanziale e di metodo che emergono dall'impostazione del Codice di buone pratiche e che risultano rilevanti ai fini della sua corretta collocazione nel quadro delineato dall'AI Act.

Essere trasparenti sulla trasparenza

Quanto al primo elemento, l'approccio seguito dai gruppi di lavoro ha valorizzato un elemento spesso trascurato nel dibattito sull'AI Act: l'articolo 50 AIA non si esaurisce nella qualificazione dei sistemi come a "rischio limitato", ma introduce una logica trasversale che attraversa l'intero impianto regolatorio. Le obbligazioni di trasparenza ivi previste, infatti, si applicano indipendentemente dalla classificazione del sistema come 'ad alto rischio' e operano come meccanismo di raccordo tra il modello *risk based* e le esigenze di tutela dell'ecosistema informativo. Ebbene, l'art. 50 AIA funziona come una clausola di permeabilità del sistema, idonea a intercettare rischi che non rientrano agevolmente nelle categorie rigide dell'Allegato III, ma che possono produrre effetti significativi sui diritti fondamentali, sulla fiducia del pubblico e sul corretto funzionamento del dibattito democratico.

Dunque, il Codice sembra valorizzare proprio questa dimensione, rafforzando l'idea che la trasparenza non possa essere confinata al solo momento della diffusione del contenuto, né gravare esclusivamente sull'utilizzatore finale. Al contrario, come si premetteva, essa richiede un coordinamento tra scelte progettuali, strumenti tecnici messi a disposizione dai *provider* e obblighi informativi in capo ai *deployer*. Letto in questa chiave, il Codice può essere interpretato come un primo tentativo di dare contenuto operativo all'art. 50 dell'AI Act, colmandone alcune ambiguità applicative e anticipando una possibile evoluzione verso standard più vincolanti.

In tale contesto, pur non costituendo l'oggetto diretto del Codice, si auspica un più chiaro raccordo tra le diverse declinazioni del principio di trasparenza previste dall'AI Act. In particolare, appare opportuno chiarire la relazione tra gli obblighi di trasparenza che gravano sui *provider* ai sensi dell'articolo 13 AIA e quelli disciplinati dall'art. 50 AIA, cui il Codice è specificamente dedicato.

L'art. 13 AIA impone ai *provider* obblighi informativi funzionali principalmente a garantire un uso corretto e conforme del sistema da parte dei *deployer*, attraverso la predisposizione di istruzioni d'uso chiare, complete e comprensibili. Si tratta, dunque, di una trasparenza che opera prevalentemente all'interno della filiera, orientata a rendere intelligibili le caratteristiche, le finalità e i limiti del sistema di IA ai soggetti che lo integrano o lo utilizzano in uno specifico contesto applicativo.

Diversamente, l'art. 50 AIA proietta la trasparenza verso l'esterno, ponendo l'accento sulla necessità di informare gli utenti finali e il pubblico circa l'origine artificiale o la manipolazione dei contenuti generati dall'IA. Il tenore della disposizione, così come l'impostazione del Codice, suggerisce una trasparenza prevalentemente rivolta ai destinatari del contenuto, più che ai soggetti coinvolti nelle fasi di sviluppo e utilizzo del sistema. Tale

distinzione, sebbene concettualmente utile, rischia tuttavia di risultare eccessivamente rigida sul piano operativo. In assenza di un coordinamento esplicito tra questi due livelli di trasparenza, il *provider* potrebbe trovarsi a gestire obblighi informativi formalmente distinti ma sostanzialmente interdipendenti. Un chiarimento in tal senso appare dunque utile, anche al fine di evitare sovrapposizioni, lacune o incoerenze applicative.

La qualificazione normativa del Codice

Dal punto di vista della qualificazione normativa, sebbene il Codice di buone pratiche si configuri formalmente come uno strumento di adesione volontaria, il suo inquadramento all'interno dell'AI Act è idoneo a rafforzarne la portata giuridica e istituzionale. L'AI Act affida infatti all'AI Office il compito di incoraggiare e facilitare l'elaborazione di codici di pratica a livello dell'Unione, al fine di garantire un'attuazione efficace degli obblighi relativi alla rilevazione e alla segnalazione dei contenuti generati o manipolati dall'IA (Considerando 135 e art. 50(7) AI Act). Una volta finalizzato, il Codice potrà essere formalmente approvato dalla Commissione mediante atti di esecuzione, divenendo così un punto di riferimento ufficiale per l'implementazione dell'art. 50 AIA. In questa prospettiva, risulta utile richiamare il precedente rappresentato dal *Codice di buone pratiche sulla disinformazione* (su cui v. in questa Rubrica il contributo n. 6 del [numero 4/2022](#) [2022/4(6)DI] in *PeM*, 2022, p. 710 e in *Atlante*, p. 259) il quale, attraverso un processo di progressiva istituzionalizzazione, è divenuto un pilastro dell'applicazione del regolamento (UE) 2022/2065 (**Digital Services Act** o **DSA**).

Analogamente, il Codice sembra destinato a svolgere una funzione di cerniera tra *soft law* e *hard law*: uno strumento flessibile, costruito con il contributo degli *stakeholder*, ma inserito in una cornice regolatoria che consente all'Unione europea di evolvere rapidamente verso soluzioni più prescrittive qualora l'autoregolazione non si rivelasse sufficiente. Per imprese e piattaforme, l'adesione al Codice non rappresenta dunque soltanto una scelta di natura reputazionale, ma costituisce anche un'opportunità di posizionamento anticipato rispetto a standard che potrebbero, nel prossimo futuro, assumere carattere obbligatorio. In questo senso, il Codice contribuisce a rafforzare la dimensione sistemica dell'art. 50 AIA, confermandone il ruolo non marginale, ma strutturale, nell'architettura europea di *governance* dell'intelligenza artificiale.

FEDERICA PAOLUCCI

<https://digital-strategy.ec.europa.eu/en/library/first-draft-code-practice-transparency-ai-generated-content>

2025/4(9)LCo

L'AI Act Whistleblower Tool annunciato il 24.11.2025

Il 24 novembre 2025 la Commissione europea (la **Commissione**) ha lanciato uno strumento denominato "[AI Act Whistleblower Tool](#)", un applicativo

online attraverso il quale è possibile segnalare in forma confidenziale illeciti o violazioni normative relative all'applicazione del regolamento (UE) 2024/1689 (**AI Act** o **AIA**). Si tratta di un mezzo facilmente accessibile realizzato con l'obiettivo di dare piena attuazione alla previsione di cui all'art. 87 AIA, secondo cui la direttiva (UE) 2019/1937 sul whistleblowing (**dir. whistleblowing**) si applica alle violazioni dell'AI Act alla protezione delle persone che segnalano tali violazioni. Uno strumento che il legislatore europeo mette a disposizione nel solco dell'azione congiunta di hard e soft law, con l'intento di colmare il divario informativo che atavicamente condiziona l'operato dei policymakers tramite una vigilanza sul rispetto delle norme e dei diritti fondamentali, sulle modalità di gestione del rischio e di addestramento dei modelli, che passa dalle informazioni provenienti dall'interno dei processi produttivi. Il tool per l'IA è solo l'ultimo di una serie di strumenti analoghi introdotti in diversi settori (come servizi e mercati digitali, antitrust) a seguito dell'entrata in vigore della dir. whistleblowing. Il whistleblowing può essere definito come il meccanismo che permette di segnalare comportamenti illeciti o violazioni di norme, garantendo riservatezza, sicurezza e protezione contro eventuali ritorsioni nei confronti di chi effettua la segnalazione ed è uno strumento già da anni sperimentato negli USA.

Nell'ambito dell'AI Act la protezione degli informatori è una componente del risk assessment, approccio caratterizzato dall'attribuzione di obblighi diversi di valutazione e mitigazione in base alla classificazione di rischio del sistema. La segnalazione dell'informatore contribuisce al processo di verifica del rispetto di queste regole, ma la reattività nell'individuare e agire sul vulnus da parte degli organi preposti dipende anche dall'efficacia delle tutele riconosciute agli informatori, che trovano la loro disciplina proprio nella dir. whistleblowing. In tal senso, il canale europeo messo a disposizione dall'Ufficio IA prevede forme di crittografia avanzata per consentire la trasmissione di informazioni sensibili anche senza rivelare l'identità del whistleblower, sì da garantire confidenzialità, anonimato, sicurezza dei dati e tracciabilità dell'intero processo. Non solo, in quanto è prevista una tutela giuridica contro ritorsioni quali licenziamento, retrocessione, intimidazione, inserimento nelle liste nere; consulenza e assistenza legale indipendente; tutela contro l'attivazione di clausole contrattuali come quella per violazione del patto di riservatezza. Invero, affinché si realizzi a pieno la protezione giuridica degli informatori prevista dalla Direttiva bisognerà attendere la piena attuazione dell'AI Act, a partire dal 2 agosto 2026 (segnatamente, la data di decorrenza delle norme sulle misure applicabili ai sistemi ad alto rischio previste dal medesimo regolamento, tra cui proprio l'art. 87 AIA).

Il whistleblower tool è un ulteriore elemento di una disciplina del whistleblowing fondata su una logica multilivello, che ha lo scopo di guidare l'informatore verso lo strumento più efficace in base alla natura della violazione e alle esigenze proprie dell'informatore stesso. Il giusto tempismo nel far emergere le violazioni può essere decisivo nel contesto IA, dove la complessità tecnica e regolatoria spesso può complicare l'individuazione delle condotte illecite. Il modello si articola su tre livelli complementari, ognuno con una funzione specifica per la protezione del whistleblower e nella

gestione delle segnalazioni: canali interni aziendali, canale esterno nazionale e il nuovo canale esterno europeo. Se il raccordo tra i primi due canali di segnalazione sembra più definito, è sulla relazione tra il secondo e terzo strumento che occorre soffermarsi maggiormente.

Ai sensi della dir. whistleblowing (e del d.lgs. 24/2023 che ha recepito tale direttiva nell'ordinamento interno) le organizzazioni con più di 50 dipendenti sono tenute a predisporre un canale interno per ricevere segnalazioni su violazioni o pratiche aziendali rischiose nel rispetto della riservatezza dell'informatore. Nonostante il lodevole intento, la reale efficacia del canale può risentire della struttura dell'organizzazione aziendale (che potrebbe compromettere il preteso anonimato) e di pregiudizi socioculturali.

A livello esterno è previsto un canale gestito in maniera autonoma da ciascuno Stato membro. In Italia la funzione è svolta dall'Autorità Nazionale Anticorruzione (ANAC), che mette a disposizione uno strumento accessibile tramite piattaforma digitale che garantisce rigorosi criteri di riservatezza e tracciabilità, al fine di intercettare in modo tempestivo violazioni di particolare rilievo. L'ANAC deve rispondere nel termine di tre mesi (sei in casi di straordinaria particolarità e complessità), altrimenti all'informatore è consentito rendere pubblica la segnalazione.

Anche l'AI Act Whistleblower Tool è un canale esterno, basato su crittografia certificata e possibilità di scelta dell'anonimato e che consente di centralizzare le informazioni raccolte e di supportare le attività di analisi e governance a livello dell'Unione. Rispetto agli altri canali, il coinvolgimento dell'Ufficio IA potenzia la risposta complessiva dinanzi alle condotte non conformi, aumentando l'efficacia degli interventi predisposti. L'Ufficio IA si configura come l'organo centrale dell'Unione Europea per la governance e la supervisione dell'intelligenza artificiale: coordina il monitoraggio, l'analisi dei rischi e il supporto tecnico, fornendo orientamenti operativi agli Stati membri e alle istituzioni europee e promuovendo standard comuni e buone prassi a livello comunitario. La sua finalità principale è garantire che la progettazione e l'impiego dei sistemi di intelligenza artificiale si svolgano nel pieno rispetto dei diritti fondamentali, della sicurezza e della trasparenza, sostenendo concretamente l'attuazione dell'AI Act e delle relative misure di compliance.

Osservando la struttura multilivello un tema fondamentale che emerge è quello del canale idoneo verso cui dirigere la segnalazione: sappiamo che, in termini generali, al canale esterno ci si rivolge quando si è scelto di non attivare il canale interno o la segnalazione interna non abbia avuto conseguenze; quando l'informatore abbia il ragionevole timore che la segnalazione non venga affrontata efficacemente o che dalla stessa possano provenire ritorsioni o nel caso abbia il fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse. Ciò che non è del tutto esplicita è la casistica attraverso la quale l'informatore possa orientarsi nella scelta del canale esterno nazionali o europei, onde evitare il sovrapporsi di strumenti che svolgano le medesime funzioni e il moltiplicarsi di segnalazioni aventi lo stesso contenuto, causa di una possibile frammentazione dell'azione di vigilanza. La questione emerge a causa del fatto che gli Stati membri devono ancora integrare l'AI Act rispetto

alla dir. whistleblowing, per cui non c'è ancora certezza su come saranno strutturati esattamente i canali di segnalazione relativi alle sospette violazioni dell'AI Act, sebbene una dichiarazione dei presidenti e dei vicepresidenti del Codice di condotta dell'UE raccomandi l'istituzione di un canale di segnalazione dedicato per l'Ufficio IA.

Certamente, l'Ufficio europeo dispone di competenze professionali specifiche e modalità di azione e raccordo nei confronti delle autorità nazionali e degli Stati membri per cui appare logico che le segnalazioni riconducibili a fenomeni di ampia portata applicativa, finanche sovranazionali, come quelli legati ai grandi sviluppatori di IA, possano essere segnalati a livello eurounitario, mentre invece segnalazioni che abbiano una portata locale potrebbero essere effettuate con gli strumenti nazionali. Altresì, potrebbe essere preferito il tool comunitario nei casi in cui le violazioni siano riconducibili a regolamenti europei, ad applicazione diretta e vincolanti. In tal senso va evidenziato che fino alla piena attuazione dell'AI Act del 2 agosto del 2026 le materie oggetto della possibile segnalazione saranno solo le violazioni che riguardino certe attività già individuate dalla normativa vigente e che possano riguardare (indirettamente) il settore IA, tra cui: gli appalti pubblici; servizi, prodotti e mercati finanziari; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; sicurezza alimentare; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi, atteso che sono già previste dalle disposizioni Ue sul whistleblowing recepite negli ordinamenti nazionali (ex art. 2, c. 1 lett. a, n. 3 del D. Lgs. 24/2023). Non va dimenticato, inoltre, che l'attuazione della dir. whistleblowing non è stata uniforme in tutti gli Stati Membri, in particolare con riferimento alle misure di protezione e tutela contro le ritorsioni, per cui il tool comunitario può offrire uno strumento accessibile, equidistante dalle frammentazioni nazionali e immediatamente efficace a tutti i cittadini comunitari, che potrebbero riconoscerlo come un mezzo più lontano dal rischio di ritorsione territoriale.

La piattaforma è indirizzata alle persone che sono in relazione professionale (governata dalle leggi europee) con i fornitori dei modelli di intelligenza artificiale, come dipendenti, lavoratori autonomi, azionisti e membri dell'organo di amministrazione, direzione o vigilanza di un'impresa, i volontari e i tirocinanti retribuiti e non retribuiti e i candidati all'impiego, ma anche le persone ad essi connesse o chi ha terminato il rapporto professionale. Spesso tali soggetti sono quelli con la maggiore facilità di individuare violazioni o pratiche rischiose. In questo senso sembra che uno strumento del genere possa concorrere a delineare un sistema di governance partecipativa e condivisa, dove la sicurezza e affidabilità dell'intero ecosistema è affidata anche alla vigilanza degli attori della filiera "dal basso". Le segnalazioni relative all'AI Act, infatti, possono incidere in concreto sui diritti fondamentali dei cittadini o sulla fiducia collettiva verso l'uso dell'IA: tra le varie ipotesi, potranno emergere algoritmi che discriminano lavoratori o che profilano indebitamente, senza garanzie di affidabilità e reale possibilità di sottrarsi consumatori o cittadini. Un lavoratore coinvolto nello sviluppo di sistemi ad alto rischio può, ad esempio, accorgersi che, in violazione degli

obblighi imposti sugli sviluppatori dei sistemi GPAI, i dati di addestramento non rispettano i requisiti di riservatezza o contengono bias discriminatori, oppure che la documentazione tecnica obbligatoria non viene aggiornata correttamente dal fornitore, compromettendo la trasparenza e spiegabilità dei processi: in sostanza l'individuo in connessione professionale potrà verificare come vengono gestiti i rischi sistemici quando la lettera normativa viene traspota in prassi commerciale.

A livello pratico il form consente di trasmettere una segnalazione in modo sicuro e, se richiesto, completamente anonimo, secondo una specifica policy che prevede l'utilizzo di una piattaforma certificata ISO 27001 per l'invio dei report. Si potranno descrivere dettagliatamente i fatti con la possibilità di allegare elementi documentali. Chi intende preservare l'anonimato potrà selezionare l'opzione apposita e prestare attenzione (come suggerito da appositi alert) a non includere nel testo o negli allegati riferimenti diretti o indiretti alla propria identità o a quella di terzi (così che lo stesso Ufficio IA non sia poi tenuto, su richiesta di accesso ex art. 17 del regolamento (UE) 2018/1725 (**EUDPR**), da parte dell'interessato, a una disclosure *de facto* sull'identità degli informatori). Infine, verrà generata una secure inbox protetta da una password e da un numero identificativo, mediante la quale l'informatore può comunicare con il gruppo incaricato senza rivelare la propria identità, ricevendo aggiornamenti sul procedimento e potendo rispondere a eventuali richieste di chiarimenti. Tale sistema risulta pienamente conforme al recente parere n. 581 del 9 ottobre 2025 del Garante italiano per la protezione dei dati personali, il quale in materia di linee guida ANAC sulle segnalazioni interne affermava che la posta elettronica ordinaria o certificata non rappresenta uno strumento adeguato (in assenza di specifiche contromisure) a tutelare pienamente l'anonimato.

Ciò che appare chiaro, anche ad una prima analisi dello strumento, è che affinché il canale si riveli funzionale sarà necessario che la formazione e l'informazione (attraverso report e follow-up da pubblicarsi regolarmente da parte dell'Ufficio europeo IA) in materia di IA dovranno essere pervasivi a tutti i livelli e, al contempo, dovranno risultare chiare le prerogative delle autorità nazionali ed europee, così che l'informatore possa operare una scelta il più possibile consapevole sull'an e sul quomodo e non si manifesti una deriva paralizzante e frammentata, l'esatto opposto dell'uniformità e reattività che si vorrebbero perseguire attraverso la centralizzazione delle segnalazioni esterne. Inoltre, affinché il sistema del whistleblowing possa risultare realmente efficace si dovrà tener conto della fragilità applicativa della tutela dell'anonimato, se, sull'altare del bilanciamento fra diritti, anche garantire il diritto di accesso ai dati da parte dell'interessato può metterlo a rischio, e dovrà essere implementata efficacemente la protezione giuridica dell'informatore, assente in attesa della piena attuazione dell'AI Act e tutta da verificare a partire dal 2 agosto 2026, tenendo conto dei differenti stati di attuazione da parte degli ordinamenti interni della dir. whistleblowing che offrono tutele diversificate ai cittadini in base allo Stato Membro di appartenenza.

Concludendo, il canale individuato dalla Commissione, pur non privo di criticità, emerge come un precipitato di un modello di governance condivisa

e dal basso che persegue l’auspicio della partecipazione proattiva di tutti gli attori e operatori coinvolti, ciascuno secondo le funzioni svolte, con lo scopo di garantire una più concreta protezione dei diritti fondamentali delle persone.

LORENZO COREA

| 1049

<https://digital-strategy.ec.europa.eu/en/news/commission-launches-whistleblower-tool-ai-act>
<https://ai-act-whistleblower.integrityline.app/>

2025/4(10)TDMCDV

Lo studio sull'utilizzo della IA nel settore della sanità pubblicato dall'Ufficio per le pubblicazioni dell'Unione europea l'8.8.2025

L'8.8.2025 è stato pubblicato il report finale “*Study on the deployment of AI in healthcare*” commissionato dalla Direzione generale per la salute e la sicurezza alimentare della Commissione Europea (DG SANTE) e redatto da Pricewaterhouse Coopers EU Services EEIG e da Open Evidence (lo **studio**).

Muovendo dalle potenzialità dell'Intelligenza Artificiale (IA) nel contribuire ad affrontare alcune delle criticità di fronte alle quali i sistemi sanitari contemporanei si trovano (par. 4), lo studio prende atto della lentezza con cui strumenti basati sull'IA trovano diffusione e applicazione nella pratica clinica (par. 6). Pertanto, attraverso un approccio metodologico misto – che combina una revisione della letteratura con attività di consultazione degli stakeholder (par. 3) – lo studio si propone di individuare i principali ostacoli all'adozione dell'IA in ambito sanitario (che includono problematiche tecnologiche e legate ai dati, complessità giuridiche e regolatorie, fino a criticità organizzative e di modello di business, nonché barriere sociali e culturali) e di incentivare strategie efficaci per superare tali difficoltà (parr. 7-8), offrendo spunti di rilievo nel contesto privilegiato dell'Unione europea (UE).

Di particolare interesse è il par. 5, intitolato “*Current EU regulatory landscape*” (pp. 31-36), in cui lo studio presenta una panoramica del quadro regolatorio che, a livello europeo, potrà direttamente o indirettamente influenzare l'adozione di sistemi di IA in ambito sanitario. Si distingue tra (i) un piano regolatorio orizzontale (*cross-sector*) e (ii) uno settoriale (*healthcare-specific*).

A livello orizzontale, spiccano il regolamento (UE) 2024/1689 sull'intelligenza artificiale (**AI Act** o **AIA**) e la nuova direttiva sulla responsabilità da prodotto difettoso (dir. (UE) 2024/2853, **PLD2**). L'AI Act, come noto, introduce una regolamentazione uniforme dei sistemi di IA basata sul rischio, imponendo cioè divieti di commercializzazione e uso per i sistemi che introducono un livello di rischio inaccettabile e graduando l'intensità dei requisiti di sicurezza obbligatori imposti su *provider* e *deployer* di sistemi di IA ad alto rischio, a rischio basso (requisiti di trasparenza) e a rischio minimo (codici di condotta volontari). Lo studio fornisce una classificazione delle tipologie di sistemi di IA impiegabili in ambito sanitario in base ai livelli di

rischio delineati dall'AIA, al fine di contribuire a conferire chiarezza rispetto alle concrete obbligazioni gravanti sui fornitori e, soprattutto, sui *deployer* di tali sistemi (ospedali, altre organizzazioni sanitarie e operatori sanitari privati).

In particolare, lo studio evidenzia che sarebbero assoggettati ai divieti a norma dell'art. 5 AIA i sistemi di IA impiegati per finalità di *social scoring* degli individui per l'attribuzione di *health benefits*. Sarebbero, invece, da considerarsi “ad alto rischio” i sistemi di IA costituenti prodotti coperti dalla legislazione europea sulla sicurezza dei dispositivi medici (v. *infra*) inclusa nell'Allegato I e quelli impiegati in uno o più dei settori ad alto rischio ricompresi nell'Allegato III (valutazione dei rischi e determinazione dei prezzi nell'ambito di assicurazioni sanitarie, valutazione e classificazione delle chiamate d'emergenza e per il *triage* medico, valutazione da parte di autorità pubbliche dell'ammissibilità alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria). Sarebbero soggetti a soli obblighi di trasparenza i provider e deployer di sistemi di IA consistenti in chatbots che forniscono consigli di benessere, *deepfake* medici generati dall'IA o sensori alimentari impiegati in servizi domiciliari. Rischio minimo o nullo sarebbe quello introdotto, infine, da sistemi di IA impiegati nella ricerca e nello sviluppo farmaceutici e in mere attività amministrative attinenti alla salute.

Nel complesso, gli stakeholder riconoscono che l'AI Act affronta alcune criticità rilevanti del settore sanitario, ma ne evidenziano anche le difficoltà di attuazione concreta a livello ospedaliero. Mentre le strutture sanitarie appaiono in larga parte poco preparate e preoccupate per gli oneri organizzativi, finanziari e formativi della compliance, gli sviluppatori di IA risultano mediamente più pronti. In tutti i casi, emerge una forte esigenza di supporto, orientamento e formazione per facilitare l'applicazione efficace della normativa.

La PLD2, dall'altro lato, svolgerà un ruolo importante in sanità, così da applicarsi ai casi in cui i sistemi di IA vengono integrati in dispositivi medici e diagnostici e nel monitoraggio dei pazienti. Poiché la responsabilità del produttore diventerà verosimilmente centrale nella governance dei danni causati da dispositivi medici intelligenti, lo studio evidenzia come l'aggiornamento operato dalla PLD2 – con il suo adattamento alla realtà produttiva odierna, caratterizzata da prodotti interamente o parzialmente digitali e/o automatizzati – si pone nell'ottica del superamento di alcune criticità legate al rapporto tra IA e responsabilità, tra cui *in primis* le difficoltà probatorie incontrate dai danneggiati, nell'ottica di individuare un compromesso fra trasparenza e tutela dell'innovazione.

A livello settoriale, viene segnalata la rilevanza di alcuni strumenti regolatori aventi direttamente ad oggetto il settore della sanità. Il regolamento (UE) 2017/745 sui dispositivi medici (**MDR**) e il regolamento (UE) 2017/746 relativo ai dispositivi medico-diagnostici in vitro (**IVDR**) stabiliscono requisiti di sicurezza e prestazionali per i dispositivi medici e per i dispositivi medici diagnostici in vitro, compresi quelli che incorporano l'IA. Entrambi i regolamenti adottano una classificazione basata sul rischio, dove i dispositivi ad alto rischio sono soggetti a procedure di valutazione della conformità per

mezzo di organismi notificati indipendenti. Il regolamento (UE) 2021/2282 sulla valutazione delle tecnologie sanitarie (**HTAR**) istituisce un quadro per la valutazione clinica coordinata delle tecnologie sanitarie negli Stati membri dell'UE, compresi i prodotti farmaceutici, i dispositivi medici ad alto rischio e i dispositivi medico-diagnostici in vitro. Il suo obiettivo principale è consentire una valutazione clinica più rapida e coerente e ridurre i ritardi nell'accesso dei pazienti alle tecnologie sanitarie innovative. Infine, il regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari (**reg. EHDS**) istituisce un quadro uniforme e sicuro per lo scambio di dati sanitari tra gli Stati membri dell'UE. Il suo obiettivo generale è quello di migliorare l'erogazione dell'assistenza sanitaria, l'accesso dei pazienti ai propri dati sanitari e un uso (sia primario, sia secondario) più ampio dei dati sanitari per la ricerca, i processi decisionali e l'innovazione, compreso lo sviluppo e l'implementazione dell'IA nell'assistenza sanitaria. In particolare, il reg. EHDS fornisce una base strategica per sostenere lo sviluppo dell'IA in sanità, favorendo la disponibilità di dati di qualità, interoperabili e affidabili, nel rispetto di elevati standard di sicurezza e tutela della privacy.

Come riassunto anche nella parte conclusiva (par. 9, pp. 108-109), dallo studio emerge come l'IA possa contribuire in modo decisivo a rispondere alle principali sfide dei sistemi sanitari, ma la sua adozione resta limitata a causa di numerosi ostacoli. Tra questi figurano la frammentazione e la scarsa interoperabilità dei dati, infrastrutture IT inadeguate, difficoltà di valutazione delle prestazioni e del valore aggiunto delle soluzioni di IA, nonché carenze nei meccanismi di monitoraggio e trasparenza, che incidono sulla fiducia dei professionisti sanitari. A ciò si aggiungono la complessità del quadro regolatorio, l'assenza di chiari modelli di finanziamento e rimborso, e fattori sociali e culturali legati alla fiducia, alle competenze digitali e al rapporto medico-paziente. Lo studio evidenzia la necessità di strategie coordinate e di un impegno congiunto tra istituzioni, operatori sanitari, sviluppatori e pazienti per favorire un'adozione dell'IA efficace, equa e sostenibile, valorizzando anche le buone pratiche emerse a livello internazionale.

TOMMASO DE MARI CASARETO DAL VERME

Link al testo dello studio: <https://op.europa.eu/en/publication-detail/-/publication/9ddf7bf8-62bf-11f0-bf4e-01aa75ed71a1/language-en>

2025/4(11)VF

Il regolamento (UE) 2025/2518 del 26.11.2025 che stabilisce norme procedurali aggiuntive sull'applicazione del GDPR

Il 26 novembre 2025 il Parlamento europeo e il Consiglio dell'Unione europea hanno adottato il Regolamento (UE) 2025/2518 (il **Regolamento**), che stabilisce norme procedurali aggiuntive sull'applicazione del reg. (UE) 2016/679 (**GDPR**). Il Regolamento, pubblicato nella Gazzetta ufficiale dell'Unione europea il 12 dicembre 2025, risponde all'esigenza di introdurre una disciplina procedurale uniforme per la gestione dei reclami e lo

svolgimento di indagini da parte delle autorità di controllo nei casi di trattamenti transfrontalieri di dati personali basati su un reclamo o avviati d'ufficio (art. 1). A tal fine vengono dettate norme procedurali comuni destinate a integrare le discipline nazionali in materia di procedimenti amministrativi, con la precisazione che gli aspetti non armonizzati dal Regolamento sono regolati dalle norme nazionali sui procedimenti amministrativi e giudiziari in ossequio al principio di autonomia procedurale degli Stati membri e salva la necessità di rispettare i principi di effettività e di equivalenza (considerando 3).

Nel far salve le definizioni contenute nel GDPR, il Regolamento introduce la nozione di «parte sottoposta a indagine», riferita al titolare o al responsabile del trattamento sottoposto a indagine per una presunta violazione connessa a un trattamento transfrontaliero (art. 2).

L'art. 3 del Regolamento sancisce poi alcuni principi generali relativi alla gestione dei reclami e allo svolgimento di indagini nel contesto di trattamenti transfrontalieri di dati personali, prescrivendo alle autorità di controllo di svolgere i procedimenti in modo rapido ed efficiente e di cooperare tra loro in modo sincero ed efficace fornendo assistenza senza ritardo alle reciproche richieste. Consente inoltre al soggetto che ha proposto un reclamo di comunicare esclusivamente con l'autorità di controllo cui ha presentato il reclamo a norma dell'art. 77 del GDPR e impone agli Stati membri di garantire una tutela giurisdizionale effettiva alle decisioni dei reclami proposti.

Il Capo II del Regolamento è dedicato alla disciplina dei reclami relativi a trattamenti transfrontalieri. In particolare, l'art. 4, par. 1, individua in modo tassativo le informazioni che deve contenere il reclamo affinché possa essere dichiarato ricevibile (che comprendono l'identità e i dati di contatto del reclamante, le informazioni necessarie a individuare il titolare o il responsabile del trattamento, nonché una descrizione sufficientemente circostanziata della presunta violazione del GDPR). La norma precisa altresì che, ai fini della ricevibilità, non possono essere richieste informazioni ulteriori rispetto a quelle espressamente indicate, facendo al contempo salva l'applicabilità delle modalità e dei requisiti amministrativi previsti dal diritto nazionale dell'autorità di controllo cui il reclamo è presentato. L'art. 4, par. 3, chiarisce poi che, ai fini della ricevibilità del reclamo, il reclamante non è tenuto a contattare preventivamente la parte sottoposta a indagine, salvo il caso in cui esso riguardi l'esercizio di un diritto dell'interessato che presuppone una previa richiesta al titolare del trattamento.

Ciò posto, spetta poi all'autorità di controllo cui è stato presentato il reclamo verificarne la ricevibilità. Se il reclamo non contiene le informazioni richieste, l'autorità di controllo lo dichiara irricevibile entro due settimane dal ricevimento e ne comunica i motivi al reclamante (art. 4, par. 2). Quando non dichiara il reclamo irricevibile, l'autorità cui è presentato procede a una valutazione preliminare, volta ad accertare se il caso riguarda un trattamento transfrontaliero, a individuare l'autorità di controllo competente ad agire quale autorità capofila e a verificare l'eventuale applicabilità dell'articolo 56, paragrafo 2, del GDPR (secondo cui ogni autorità di controllo è competente per i reclami o le violazioni riguardanti unicamente uno stabilimento nel suo

Stato membro o che incidono in modo sostanziale sugli interessati unicamente nel suo Stato membro) (art. 4, par. 4). La determinazione così svolta sulla ricevibilità del reclamo è vincolante per l'autorità di controllo capofila e viene a questa trasmessa ai fini della prosecuzione del procedimento, con contestuale informazione al reclamante (art. 4, par. 5).

Accanto alla procedura ordinaria, il Regolamento introduce una procedura di risoluzione rapida dei reclami riguardanti l'esercizio dei diritti dell'interessato di cui al Capo III del GDPR (art. 5). Tale procedura può essere attivata dall'autorità di controllo cui è stato presentato il reclamo o dall'autorità di controllo capofila cui sia stato trasmesso il reclamo, le quali dichiarano il reclamo privo di oggetto se accertano, sulla base di elementi di prova, la cessazione della presunta violazione. In tali casi, le stesse autorità informano il reclamante delle ragioni della risoluzione, delle sue conseguenze e della possibilità di sollevare obiezioni entro un termine di quattro settimane. La mancata presentazione di obiezioni comporta l'adozione di una decisione che attesta la risoluzione del reclamo, senza però pregiudicare l'esercizio dei poteri correttivi dell'autorità di controllo capofila ai sensi dell'articolo 58 del GDPR.

Il Capo III del Regolamento (UE) 2025/2518 contempla norme che disciplinano la cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate nei casi di trattamento transfrontaliero, in attuazione dell'articolo 60 del GDPR. In particolare, il Regolamento individua le condizioni di applicazione della procedura di cooperazione semplice (art. 6), le modalità di scambio delle informazioni (art. 9), la gestione delle osservazioni tra autorità (art. 10), e fa salva la possibilità per le autorità di controllo di utilizzare gli strumenti di assistenza reciproca e le operazioni congiunte previsti dagli articoli 61 e 62 del GDPR al fine di raggiungere un consenso sui casi riguardanti un trattamento transfrontaliero (art. 11).

Le norme successive regolano i termini per la presentazione di un progetto di decisione da parte dell'autorità di controllo capofila (art. 12) e sanciscono la legittimità e validità della decisione definitiva e delle altre misure procedurali eventualmente adottate dopo la scadenza dei termini previsti dal Regolamento medesimo (art. 14).

Gli artt. 16-18 disciplinano poi la procedura per l'adozione di una decisione di rigetto o di archiviazione del reclamo. In particolare, qualora l'autorità di controllo capofila intenda respingere o archiviare in tutto o in parte un reclamo, prima di presentare un progetto di decisione comunica i motivi della propria decisione all'autorità di controllo cui è stato presentato il reclamo, la quale informa il reclamante. Quest'ultimo può comunicare le sue opinioni, che vengono poi trasmesse all'autorità di controllo capofila entro i termini stabiliti all'art. 16. Se ritiene che queste osservazioni non modifichino l'opportunità di rigettare o archiviare il reclamo, l'autorità di controllo capofila, in cooperazione con l'autorità di controllo cui è stato presentato il reclamo, elabora un progetto di decisione e lo trasmette alle altre autorità di controllo interessate ai sensi dell'art. 60, par. 3, GDPR. La decisione di rigetto o archiviazione successivamente adottata viene poi comunicata al reclamante ai sensi dell'art. 60, par. 8, GDPR da parte dell'autorità di controllo cui è stato



presentato il reclamo, la quale deve altresì informarlo della disponibilità del ricorso giurisdizionale ai sensi dell'art. 78 del GDPR (art. 18).

Qualora non intenda rigettare o archiviare il reclamo, l'autorità di controllo capofila adotta una constatazione preliminare (in cui espone i principali risultati dell'indagine con esposizione delle accuse sollevate in modo esaustivo e sufficientemente chiaro) e la trasmette alle altre autorità di controllo interessate, le quali possono formulare osservazioni. La constatazione, eventualmente modificata sulla base delle osservazioni delle autorità di controllo interessate, viene poi notificata alle parti sottoposte all'indagine, le quali possono accedere al fascicolo amministrativo, formulare osservazioni, chiedere di essere ascoltate e produrre documenti entro i termini ivi stabiliti (art. 19). La constatazione preliminare viene altresì trasmessa al reclamante, il quale può comunicare le proprie opinioni per iscritto entro il termine fissato dall'autorità di controllo capofila (art. 20).

L'art. 21 disciplina l'adozione della decisione definitiva da parte dell'autorità di controllo capofila, la quale deve preliminarmente elaborare un progetto di decisione da trasmettere alle altre autorità di controllo interessate. Qualora queste ultime non sollevino obiezioni entro i termini previsti nella medesima disposizione, l'autorità di controllo capofila adotta la decisione definitiva e la notifica allo stabilimento principale o allo stabilimento unico del titolare del trattamento o responsabile del trattamento. La stessa viene poi comunicata al reclamante unitamente alle informazioni indicate all'art. 21, par. 2.

Qualora invece una o più delle autorità di controllo interessate intenda formulare obiezioni sul progetto di decisione, l'art. 23 del Regolamento prescrive che esse siano pertinenti e motivate sulla scorta dei parametri ivi indicati. L'art. 22 riconosce poi il diritto delle parti sottoposte a indagine di essere ascoltate sul progetto di decisione eventualmente riveduto a seguito delle obiezioni pertinenti e motivate delle autorità di controllo interessate.

Il Capo IV definisce e regola il fascicolo amministrativo dell'indagine e il fascicolo di cooperazione. Il primo contiene tutti i documenti ottenuti o prodotti dall'autorità di controllo capofila e dalle altre autorità di controllo interessate, riuniti dall'autorità di controllo capofila durante la procedura di indagine (art. 24). Il secondo mira a garantire lo scambio di informazioni pertinenti tra l'autorità di controllo capofila e le altre autorità di controllo interessate (art. 25). Il Regolamento sancisce e regola il diritto della parte sottoposta a indagine e del reclamante di accedere al fascicolo amministrativo, limitandolo al caso in cui la relativa decisione potrebbe pregiudicare i loro interessi (art. 24, par. 2) ed escludendolo rispetto alle informazioni e ai documenti considerati riservati poiché contengono segreti commerciali o altre informazioni riservate conformemente al diritto dell'Unione o nazionale (art. 25). Il fascicolo di cooperazione non è invece accessibile alle parti sottoposte a indagine, ai reclamanti e ai terzi, ma solo alle autorità di controllo ed eventualmente al comitato per la composizione delle controversie in caso di deferimento della questione ai sensi dell'art. 65 del GDPR o di richiesta di un provvedimento d'urgenza ai sensi dell'art. 66 del GDPR.

Il Capo V del Regolamento disciplina le procedure di composizione delle controversie ai sensi dell'articolo 65 del GDPR, stabilendo i termini per il

deferimento della questione al comitato per la composizione delle controversie e i documenti che devono essere trasmessi, e garantendo al reclamante e alla parte sottoposta a indagine il diritto di essere ascoltati. Il Capo VI del Regolamento detta invece norme procedurali sulla richiesta di un parere d'urgenza o di una decisione vincolante d'urgenza del comitato a norma dell'art. 66, parr. 2 e 3, del GDPR.

Le disposizioni finali regolano l'entrata in vigore e l'applicazione temporale del Regolamento (Capo VII), prevedendo che le norme relative ai reclami, alla cooperazione e ai diritti procedurali si applicano alle indagini avviate e ai reclami presentati dopo il 2 aprile 2027, mentre le disposizioni sulla composizione delle controversie e sulle procedure d'urgenza trovano applicazione ai casi deferiti dopo il medesimo termine.

VIRGINIA FUSCO

<https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX:32025R2518>

2025/4(12)VM

La comunicazione della Commissione europea “DigitalJustice@2030” COM(2025) 802 final del 20.11.2025: la competitività dell’Unione Europea attraverso la modernizzazione dei sistemi giudiziari e la formazione degli operatori del diritto.

Il 20 novembre 2025, la Commissione europea (la **Commissione**) ha presentato il “*Digital Justice package 2030*” (il **pacchetto**), un’iniziativa volta a modernizzare i sistemi giudiziari all’interno dell’Unione Europea (UE) e incrementare la formazione in ambito digitale degli operatori del diritto, nell’ottica di rafforzare la **competitività dell’UE** a livello globale.

Il pacchetto rientra nell’ambito del più ampio programma politico del “*Decennio digitale 2030*”, istituito con la [Decisione \(UE\) 2022/2481](#) del Parlamento europeo e del Consiglio del 14 dicembre 2022. Tale programma, infatti, pone tra i suoi obiettivi la digitalizzazione dei servizi pubblici in termini di accessibilità ed efficienza, così da consentire alle imprese e ai cittadini europei di interagire con le amministrazioni di competenza direttamente online.

Come si evince dal relativo [comunicato stampa](#), il pacchetto consta di **due diverse strategie** che prevedono un **novero determinato di misure** funzionali al pieno compimento della trasformazione digitale nello specifico settore della giustizia. Com’è noto, infatti, proprio la trasformazione digitale costituisce una delle principali priorità dell’agenda politica della Commissione europea, al pari della transizione verde.

In tale prospettiva, la **modernizzazione dei servizi pubblici** rappresenta uno dei pilastri della competitività europea, e il settore giudiziario occupa un ruolo centrale in questa evoluzione. Sistemi di giustizia digitalizzati offrono maggiore trasparenza, riducono i tempi di gestione delle procedure e generano un ambiente più favorevole agli investimenti. L’esperienza della pandemia ha mostrato, infatti, quanto infrastrutture tecnologiche adeguate



rendano i Tribunali più resilienti e capaci di operare anche in condizioni critiche. Ed è proprio in tale ottica che va inteso, nelle sue diverse componenti, il pacchetto presentato dalla Commissione europea.

Entrando nel merito delle misure, come anticipato in precedenza, l'iniziativa lanciata dall'Istituzione dell'UE delinea una tabella di marcia suddivisa in due specifiche e complementari strategie. La prima di queste, denominata “[DigitalJustice@2030 Strategy](#)”, mira a garantire una maggiore competitività dell'UE, integrando nei sistemi giudiziari tecnologie all'avanguardia come l'intelligenza artificiale (IA) ed ulteriori strumenti digitali, al fine di migliorare l'efficienza della giustizia rendendo quest'ultima più accessibile a tutti e riducendo i relativi costi.

La strategia in esame comprende **14 misure di supporto per gli Stati membri dell'UE**. Nell'ottica della relativa elaborazione, la Commissione europea ha tentato di convertire in azioni concrete quanto espresso nella “[Dichiarazione di Budapest sul nuovo patto per la competitività europea](#)” dell'8 novembre 2024, nonché gli obiettivi strategici e operativi della “[Strategia europea in materia di giustizia elettronica 2024-2028](#)” - tra cui migliorare l'accesso alla giustizia digitale e rafforzare la cooperazione giudiziaria digitale - e le priorità riportate nelle “[Conclusioni del Consiglio sull'uso dell'intelligenza artificiale nel settore della giustizia](#)” del 16 dicembre 2024. Con specifico riguardo alle predette misure, secondo quanto previsto nella relativa **Comunicazione** [[COM\(2025\) 802 final](#)], la Commissione europea si adopererà al fine di garantire:

1. la creazione di un **archivio dinamico degli strumenti digitali**, in particolare quelli basati sull'IA, utilizzati nel settore della giustizia in tutta l'UE, che sarà disponibile sul [portale europeo della giustizia elettronica](#) entro la fine del 2026;
2. lo **scambio di buone pratiche** tra gli Stati membri in materia di strumenti digitali, in particolare l'IA, utilizzati nel settore della giustizia;
3. l'elaborazione di un “**toolbox**” informatico entro la fine del 2026, promuovendone il relativo uso;
4. un maggiore approfondimento sull'utilizzo dei sistemi di IA ad alto rischio nel settore della giustizia, in particolare definendo le **linee guida pertinenti** nell'ambito del [Regolamento \(UE\) 2024/1689 \(AI Act\)](#) entro febbraio 2026, con il contributo della comunità giudiziaria;
5. l'individuazione, insieme agli Stati membri e alle altre parti interessate, dei settori in cui l'UE può sostenere gli stessi nell'adozione dell'IA nel settore della giustizia, eventualmente con **linee guida specifiche sugli scopi e sulle modalità** attraverso cui utilizzare gli strumenti di IA;
6. la completa adozione dell’**European Legislation Identifier** (ELI) e dell’**European Case Law Identifier** (ECLI), in collaborazione con l’[Ufficio delle pubblicazioni dell'UE](#);
7. lo **sviluppo di applicazioni tecnologiche nel settore giudiziario**, compresi strumenti di IA per la giustizia, migliorando la disponibilità e la riutilizzabilità dei dati giuridici e giudiziari (compresa la giurisprudenza e la legislazione), insieme all'Ufficio delle pubblicazione dell'UE;
8. entro la fine del 2027, **requisiti tecnici comuni** volontari a livello UE per le videoconferenze;

9. la **partecipazione a distanza alle udienze penali degli indagati o degli imputati** provenienti da un altro Stato membro tramite videoconferenza, nel contesto della revisione della [Direttiva 2014/41/UE](#) relativa all'ordine europeo di indagine e nel rispetto delle necessarie garanzie procedurali. Verrà valutata, inoltre, la necessità di includere norme volte a facilitare la **partecipazione a distanza delle vittime di reati**, nonché le necessarie garanzie, tenendo conto dell'esito dei negoziati sulla revisione della [Direttiva 2012/29/UE](#) in materia di diritti, assistenza e protezione delle vittime di reato;

10. l'esame della **fattibilità** e l'analisi dei **costi** e dei **benefici** delle diverse opzioni per superare i problemi di interoperabilità delle videoconferenze transfrontaliere nei procedimenti giudiziari;

11. l'attuazione della propria proposta di continuare a finanziare progetti e azioni a livello dell'UE e degli Stati membri nell'ambito del prossimo **Quadro Finanziario Pluriennale (QFP)** attraverso il [Justice Programme](#);

12. un fermo sostegno alla digitalizzazione dei sistemi giudiziari nazionali nell'ambito del prossimo QFP attraverso i **Piani di Partenariato Nazionali e Regionali**;

13. un'analisi, entro la fine del 2028, sugli **effetti di un'ulteriore digitalizzazione dei procedimenti transfrontalieri** in materia civile e commerciale, al di là dell'ambito di applicazione del [Regolamento \(UE\) 2023/2844](#) sulla digitalizzazione;

14. lo sviluppo di un **sistema europeo di accesso elettronico** (*European Electronic Access Point*) da estendere successivamente alla totalità delle cause civili e commerciali con implicazioni transfrontaliere.

Nella propria disamina, la Commissione europea ha illustrato le **ragioni pratiche** che rendono le misure sopra elencate necessarie per assicurare all'UE un alto livello di competitività in campo internazionale, sfruttando la trasformazione digitale.

In primo luogo, sussiste tra gli Stati membri una disomogeneità nei progressi raggiunti in materia di digitalizzazione dei sistemi giudiziari nazionali. Tali differenze, di fatto, variano nei diversi Paesi UE, pur comprendendo alcuni fattori comuni, come le divergenti priorità politiche nazionali e la disponibilità di risorse umane e finanziarie. Quanto precisato emerge dall'analisi condotta nel contesto del **Quadro di valutazione UE della giustizia 2025** [[COM\(2025\) 375 final](#)]. Nel dettaglio, si tratta di uno strumento che raccoglie dati utili sulla digitalizzazione dei sistemi giudiziari degli Stati membri, ma che non fornisce contestualmente una descrizione o una panoramica dei meccanismi e delle iniziative adottate a livello nazionale. Per tale ragione, la Commissione europea e il Consiglio dell'UE hanno avviato un processo di monitoraggio e mappatura degli strumenti di digitalizzazione dei Paesi UE, al fine di introdurre successivamente un apposito **"archivio dinamico"** (*Misura 1*) in cui riportare tutte le informazioni utili sulle soluzioni applicate nei singoli Stati membri e consentire lo scambio di buone pratiche (*Misura 2*). Come si evince dalla relativa *Comunicazione*, l'obiettivo alla base dell'intera strategia risiede nella necessità di garantire l'**interoperabilità transfrontaliera** dei sistemi giudiziari all'interno dell'UE.



La seconda ragione pratica messa in risalto dalla Commissione europea concerne gli **effetti legati all'assenza di standard comuni** di digitalizzazione tra gli Stati membri. Nello specifico, il livello di frammentazione digitale costituisce in linea generale un limite in termini di costi e di efficienza. Ed è proprio in tale contesto che si inserisce la proposta di realizzare di uno specifico **“toolbox”** informatico-digitale (*Misura 3*) quale strumento volto a raccogliere quelle specifiche ed efficaci soluzioni digitali già testate negli Stati membri, così da ammortizzare lo sforzo dei Paesi UE sotto il profilo delle tempistiche realizzative e applicative, nonché delle risorse economico-finanziarie.

In terzo luogo, la Commissione europea ha posto l'accento sui **rischi derivanti dallo sfruttamento del potenziale trasformativo dell'IA** nei sistemi giudiziari, soprattutto in relazione al rispetto e alla tutela dei diritti fondamentali. Sebbene l'uso efficace ed efficiente degli strumenti di IA possa indubbiamente contribuire alla crescita economica, alla competitività e alla riduzione degli oneri amministrativi, il carattere antropocentrico del processo decisionale resta un valore imprescindibile nell'interpretazione e nell'applicazione del diritto. Muovendo da tale assunto, secondo le argomentazioni della Commissione europea, una corretta digitalizzazione dei sistemi giudiziari che non comporti rischi per i diritti fondamentali richiede un maggiore approfondimento sull'**utilizzo dei sistemi di IA ad alto rischio** nel settore della giustizia (*Misura 4*), in particolare mediante la definizione di **linee guida** (*Misura 5*) elaborate alla luce della disciplina sul rischio contenuta all'interno dell'*AI Act*.

Una quarta ragione a sostegno dell'importanza della *DigitalJustice@2030 Strategy* è legata all'**accessibilità** e alla **trasparenza** dei documenti e dei dati legislativi e giurisprudenziali nazionali e dell'UE. Attualmente, la relativa reperibilità è supportata da diversi strumenti non coordinati, sebbene non sempre i testi di riferimento siano disponibili online. Da ciò discende la difficoltà, per gli operatori della giustizia (si pensi ai giudici), di individuare, comprendere, interpretare e applicare il diritto di un altro Stato membro nel proprio ordinamento, soprattutto in ipotesi di casi transfrontalieri, con conseguenti ed eventuali ritardi, effetti negativi nell'amministrazione della giustizia e significativo indebolimento della crescita economica e della competitività. Il potenziamento dell'**European Legal Data Space** prospettato dalla Commissione europea mira a fronteggiare tali esigenze, agevolando ulteriormente l'accesso online alla legislazione e alla giurisprudenza (*Misura 6*) e favorendo la disponibilità a un maggior numero di dati giudiziari (*Misura 7*) per sviluppare strumenti di IA adeguati alle esigenze dei sistemi giudiziari. La **manca di interoperabilità tra le diverse piattaforme di videoconferenza** utilizzate dagli Stati membri, unita ai relativi rischi negativi, costituisce un'ulteriore criticità attuale individuata dalla Commissione europea nella propria analisi. Di fatto, sebbene lo strumento della videoconferenza sia disciplinato e adoperato in alcuni casi di cooperazione transfrontaliera europea in materia civile e penale, non esistono attualmente disposizioni a livello dell'UE volte a regolare la partecipazione a distanza di un indagato o imputato alle udienze penali di un altro Stato membro per fini diversi dalla raccolta di prove. Si tratta di un contesto da cui

discendono diverse **problematiche concrete**, tra cui costi di viaggio e difficoltà pratiche, soprattutto per le persone più vulnerabili. Le diverse soluzioni software e hardware adottate dagli Stati membri, in quanto poco interoperabili, contribuiscono altresì ad aumentare i rischi in materia di protezione dei dati personali e della privacy. Secondo la Commissione europea, pertanto, affrontare le **sfide legate all'interoperabilità dei sistemi** (*Misura 10*) rappresenta un passo fondamentale per il corretto svolgimento delle udienze mediante videoconferenza. In tale prospettiva, risulta preliminare l'elaborazione di **requisiti tecnici comuni** nell'UE (*Misura 8*), al fine di garantire in modo più efficace la **partecipazione a distanza degli indagati e degli imputati** nei procedimenti penali transfrontalieri, così come delle **vittime di reato** (*Misura 9*).

Per sfruttare compiutamente il potenziale della digitalizzazione al fine di incrementare la competitività dell'UE a livello globale, occorre altresì che gli operatori della giustizia siano in grado di acquisire le competenze, le conoscenze e la consapevolezza necessarie per un ottimale utilizzo degli strumenti di IA. Per tale ragione, il pacchetto in esame include una seconda strategia volta a garantire il raggiungimento di tale obiettivo. Si tratta dell'iniziativa denominata “**European Judicial Training Strategy 2025-2030**”, delineata dalla Commissione europea a corredo e supporto della *DigitalJustice@2030 Strategy*.

La **formazione dei professionisti della giustizia** in materia di digitalizzazione costituisce un presupposto fondamentale per colmare quelle lacune che sussistono in tale settore e per assicurare lo sviluppo di un ambiente favorevole al rafforzamento delle competenze nell'uso degli strumenti e delle infrastrutture digitali, altresì mediante l'adeguata conoscenza del diritto sostanziale e procedurale dell'UE e nazionale adattato alle esigenze dell'economia e della società digitali.

Come per la precedente, anche questa seconda strategia prevede un novero di misure specifiche, contenute in un'apposita **Comunicazione** [[COM\(2025\) 801 final](#)]. Nel dettaglio:

- (i)** garantire a tutti i professionisti della giustizia l'**accesso a corsi di formazione** per sviluppare le loro competenze in materia di IT e IA, assicurandosi che tali corsi siano adeguati ai rispettivi ruoli e responsabilità;
- (ii)** elaborare **moduli di formazione specifici e adeguati** a corredo di tutti gli atti giuridici dell'UE nel settore della cooperazione giudiziaria e del mutuo riconoscimento che includano una componente digitale. Fornire, contestualmente, una formazione appropriata, accessibile a tutti gli utenti, a corredo degli strumenti e delle infrastrutture informatiche nella disponibilità dei professionisti della giustizia;
- (iii)** per ogni atto giuridico in materia di cooperazione giudiziaria che rientra nell'ambito di applicazione del regolamento (UE) 2023/2844 sulla digitalizzazione, fornire un **modulo di formazione** sull'uso degli strumenti digitali istituiti da tale atto, disponibile in tutte le lingue dell'UE;
- (iv)** invitare le reti europee dei professionisti della giustizia a identificare, documentare e promuovere sistematicamente le **esperienze positive** e gli **insegnamenti** tratti dall'introduzione di strumenti e infrastrutture informatiche nel settore della giustizia;



(v) introdurre progressivamente un **quadro di certificazione delle competenze digitali** dei professionisti della giustizia, che rifletta le esigenze e le caratteristiche specifiche delle diverse professioni;

(vi) garantire che i programmi nazionali di formazione iniziale e le offerte di formazione continua per i professionisti della giustizia includano il **diritto sostanziale pertinente all'economia e alla società digitali**, compresa la protezione dei diritti delle persone fisiche e delle imprese nello spazio digitale, nonché la **cooperazione giudiziaria transfrontaliera dell'UE e gli strumenti di mutuo riconoscimento** in materia civile, commerciale e penale, con particolare attenzione alla digitalizzazione;

(vii) esortare le reti europee dei professionisti della giustizia a identificare, documentare e promuovere regolarmente lo **scambio delle migliori pratiche** apprese grazie alla formazione;

(viii) rendere disponibile a tutti i professionisti della giustizia una **formazione specifica sull'importanza, l'utilità e l'impatto della digitalizzazione**, in particolare in relazione all'uso dell'IA, sui ruoli e le responsabilità degli operatori del diritto;

(ix) formare i leader e i manager del settore giudiziario affinché promuovano attivamente la **transizione digitale** e progettino **processi di trasformazione inclusivi**;

(x) integrare in ogni programma di formazione giudiziaria un **modulo sugli aspetti correlati alla digitalizzazione**;

(xi) promuovere lo **scambio professionale transfrontaliero** al fine di sviluppare la consapevolezza digitale;

(xii) incentivare l'adozione di **programmi nazionali di formazione iniziale e offerte di formazione continua** per i professionisti della giustizia che prevedano lo studio dell'*acquis* dell'UE in materia di Stato di diritto, diritti fondamentali e non discriminazione, compresa l'applicazione della Carta dei diritti fondamentali dell'Unione europea (CDFUE), i diritti processuali e i meccanismi di ricorso esistenti;

(xiii) garantire che i programmi nazionali di formazione iniziale e continua destinati ai professionisti della giustizia comprendano l'**applicazione del diritto dell'UE** nella pratica quotidiana, la **legislazione dell'UE** nuova e modificata, la **giurisprudenza pertinente** della Corte di giustizia dell'Unione Europea, la **cooperazione giudiziaria transfrontaliera** in materia civile e penale, l'*acquis* del **mercato unico dell'UE**, nonché i **diritti** e le **garanzie processuali** degli indagati, degli imputati, delle persone ricercate e delle vittime di reati;

(xiv) assicurarsi che la formazione degli operatori della giustizia nei **Paesi candidati e potenziali candidati** includa l'*acquis* dell'UE, con particolare attenzione allo Stato di diritto e ai diritti fondamentali, nonché la professionalità dei giudici nell'esercizio della funzione giudiziaria;

(xv) garantire che i **finanziamenti dell'UE** siano utilizzati dalle reti europee degli enti di formazione per coordinare gli sforzi dei rispettivi membri e realizzare sinergie tra la formazione finanziata dall'UE e quella finanziata a livello nazionale, al fine di promuovere un ambiente favorevole alla digitalizzazione della giustizia.

Nella propria analisi, la Commissione ha evidenziato l'**apporto essenziale**

che la digitalizzazione e l'adozione di soluzioni basate sull'IA forniscono nel potenziamento della capacità delle Pubbliche Amministrazioni di erogare servizi efficienti ed economicamente vantaggiosi per gli utenti. E tale impatto positivo assume un rilievo particolare se contestualizzato nel settore della giustizia, poiché incrementa la qualità dei sistemi giudiziari, nonché l'accesso alla giustizia stessa.

Concepiti in tal senso, **la digitalizzazione e l'IA diventano strumenti volti a fornire nuove linfa** alla crescita e alla competitività delle economie dell'UE, attraendo investimenti. Sistemi giudiziari connotati da efficacia, qualità e trasparenza elevate, nei quali gli operatori del diritto possono concentrarsi esclusivamente - o in misura prevalente - nell'amministrazione della giustizia, accrescono la fiducia degli investitori e rendono gli Stati membri più resilienti alle crisi.

VINCENZO MIGNANO

https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2754

2025/4(13)AA

L'Agenda dei consumatori 2030 adottata dalla Commissione europea il 19.11.2025

Il 19 novembre 2025 la Commissione europea (la **Commissione**) ha adottato l'agenda dei consumatori 2030, denominata “*A new impulse for consumer protection, competitiveness and sustainable growth*”. Il documento – che intende dar seguito anche al c.d. “Rapporto Letta” (“*More than a market – Speed, Security, Solidarity*”) dell'aprile 2024 – racchiude i principali obiettivi di politica dei consumi dell'Unione per i prossimi cinque anni, articolati su quattro ambiti:

1. **Action Plan for consumers in the Single Market**, composto da una serie di misure volte a prevenire ed eliminare le discriminazioni basate su nazionalità, residenza o luogo di stabilimento, a facilitare la mobilità nel territorio UE e ad agevolare l'accesso a servizi finanziari transnazionali. Tra le misure annunciate si segnalano, ad esempio:

- interventi sull'*EU Digital Identity Wallet*;
- una valutazione dell'efficacia del regolamento in materia di *geo-blocking* (reg. UE 2018/302);
- misure finalizzate a impedire ingiustificate limitazioni territoriali delle forniture, che si affianchino agli strumenti già oggi consentiti dalle regole sulla concorrenza;

2. **sostenibilità dei consumi**, con riguardo soprattutto a questioni come il diritto alla riparazione dei prodotti, il loro riutilizzo, il contrasto al *greenwashing* e altri aspetti legati all'economia circolare. L'Agenda prefigura, a titolo esemplificativo, le seguenti misure:

- il lancio di una piattaforma *online* per le riparazioni su scala europea e altre iniziative volte a supportare gli Stati membri nell'implementazione della direttiva sul diritto alla riparazione



(dir. UE 2024/1799) e della direttiva sull'*empowerment* dei consumatori per la transizione verde (dir. UE 2024/825);

- lo studio di possibili regole volte a limitare l'impatto ambientale del settore dell'*e-commerce*;

| 1062

3. **effettività dell'enforcement** delle norme di *consumer protection*, soprattutto con riferimento a quelle sulle pratiche commerciali scorrette e sulla vendita di prodotti non sicuri. In questo senso, la Commissione si propone di intervenire soprattutto riformando il reg. (UE) 2017/2394 sulla cooperazione tra autorità nazionali in materia di tutela dei consumatori (c.d. *Consumer Protection Cooperation Regulation*), ma anche valutando l'istituzione di una *EU Market Surveillance Authority* e studiando modalità per rafforzare l'implementazione della direttiva sulle azioni rappresentative (dir. UE 2020/1828);

4. **correttezza delle pratiche commerciali e protezione del consumatore nell'ambiente digitale.** È su tale ultimo ambito che si è maggiormente concentrata l'attenzione dei commentatori, con riguardo soprattutto alla prospettiva dell'adozione di un nuovo ***Digital Fairness Act***, ossia un regolamento che – affiancandosi al *Digital Services Act*, al *Digital Markets Act* e all'*AI Act*, e raccogliendo gli spunti emersi dal “*Digital fairness fitness check of EU consumer law*” dell'ottobre 2024 – rafforzi la protezione dei consumatori *online* soprattutto con riguardo a pratiche suscettibili di alterare la capacità dei consumatori stessi di assumere decisioni e di sfruttare varie forme di **vulnerabilità**, tra cui in particolare quelle caratterizzanti i consumatori **minorenni**. Il riferimento è, ad esempio, a dinamiche di manipolazione cognitiva e comportamentale quali quelle veicolate dai *dark pattern*, da talune pratiche tipiche dell'*influencer marketing* o da alcune forme di «*unfair personalisation*».

Stando a quanto dichiarato nell'Agenda, con il *Digital Fairness Act* la Commissione si propone altresì di semplificare alcune regole relative agli obblighi in capo alle imprese, con particolare riguardo agli obblighi informativi previsti per talune tipologie di contratti.

Le esigue informazioni emergenti dall'Agenda UE non consentono, allo stato, di formulare più ampi rilievi sulle azioni che la Commissione si propone di intraprendere. Rinviamo dunque ad altre sedi per ogni più dettagliata disamina, ci limitiamo qui a dare atto di come, se si guarda soprattutto a quanto annunciato con riguardo al futuro *Digital Fairness Act*, uno degli aspetti che potrebbero rivelarsi di maggior interesse sia rappresentato proprio dall'interazione tra:

- da un canto, i prefigurati interventi con i quali si vorrebbe rimodulare, riducendoli, gli obblighi informativi in capo alle imprese (obblighi che sembrano aver dato, negli anni, scarsa prova di sé nell'incrementare il livello di protezione dei consumatori);
- dall'altro, la prospettiva dello sviluppo di una nozione potenzialmente nuova di “vulnerabilità” del consumatore, specifica per l'ambiente digitale e che possa anche superare quella sviluppata anni orsono in materia di pratiche commerciali scorrette.

ANDREA AMIDEI

https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/2030-consumer-agenda_it

2025/4(14)BP

Il primo report del 18.11.2025 del Comitato europeo per i servizi digitali (EBDS) in cooperazione con la Commissione europea sui più significativi e ricorrenti rischi sistemici e sulle relative misure di mitigazione ai sensi del Digital Services Act

Il 18 novembre 2025 è stata pubblicata dal Comitato Europeo per i Servizi Digitali (European Board for Digital Services, **EBDS** o il **Comitato**) in cooperazione con la Commissione europea (la **Commissione**), ai sensi dell'art. 35(2) reg. (UE) 2022/2065 (Digital Services Act, **DSA**, sul quale, v. in questa Rubrica la notizia n. 1 del n. 4/2022 [2022/4(1)ST] in *PeM* 2022, p..., e in *Atlante*, p. ...), la prima relazione annuale «sui più significativi e ricorrenti rischi sistemici e sulle relative misure di mitigazione» (la **Relazione**).

La Relazione si compone di cinque paragrafi e un allegato.

Il primo paragrafo dà sinteticamente conto del *background* normativo e dei contenuti affrontati. Si richiamano, in particolare, gli artt. **34 e 35(1) DSA**, che sanciscono per i fornitori di piattaforme online di dimensioni molto grandi (**VLOPs**) e di motori di ricerca online di dimensioni molto grandi (**VLOSEs**) il dovere di individuare, analizzare e valutare almeno una volta all'anno gli eventuali rischi sistemici derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, nonché il dovere di adottare misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici individuati; e si richiama l'art. **35(2) DSA**, che richiede invece la pubblicazione da parte dell'EBDS, in cooperazione con la Commissione, di relazioni annuali sui più rilevanti e ricorrenti rischi sistemici identificati e sulle migliori pratiche che consentono di attenuarli. Precisandosi quindi più oltre che il periodo di riferimento della relazione è compreso tra il 17 febbraio 2024 e il 16 febbraio 2025, si dichiara che essa intende, appunto, fornire una panoramica di tali rischi individuati dai VLOPs e VLOSEs e dalle “parti interessate”, quali ricercatori indipendenti e “organizzazioni della società civile”, e una panoramica di alcune pratiche di mitigazione di questi. Per quanto riguarda tali ultime pratiche, il Comitato specifica, peraltro, che la relazione, per questa “prima edizione”, si concentra solo sulle pratiche effettivamente in uso o proposte, rinviando alle “future edizioni” - sulla base dell'esperienza acquisita con l'attuazione concreta del DSA - per la identificazione delle “migliori pratiche” per la mitigazione dei rischi sistemici.

Il secondo paragrafo elenca le fonti utilizzate per la redazione della relazione. Segnatamente, si tratta: delle relazioni sulle valutazioni dei rischi che i fornitori di VLOPs e di VLOSEs hanno trasmesso nel 2023 e nel 2024 alla Commissione e al coordinatore dei servizi digitali del luogo di

stabilimento ai sensi dell'art. 42(4) DSA; delle relazioni redatte dalle organizzazioni di revisione indipendenti ai sensi dell'art. 37(4) DSA; di “altro materiale” reso dai fornitori di VLOPs e di VLOSEs, quali - tra gli altri - il registro sulla «trasparenza della pubblicità online» di cui all'art. 39 DSA e la relazione «sulle attività di moderazione dei contenuti» di cui all'art. 15; di contributi raccolti attraverso studi commissionati dalla Commissione e dai coordinatori dei servizi digitali (studi che sono puntualmente menzionati nell'allegato); di studi di esperti indipendenti presso istituti di ricerca e organizzazioni della società civile e contributi dei cc.dd. segnalatori attendibili di cui all'art. 22 DSA e delle autorità degli Stati membri (anche tali risorse sono puntualmente elencate nell'allegato).

Il terzo paragrafo, il più corposo, è dedicato all'analitica **disamina dei più rilevanti e ricorrenti rischi sistemici individuati**. È **suddiviso in quattro sottosezioni** che nei loro contenuti seguono la struttura dell'art. 34(1), lett. a) - d), DSA. Ogni sottosezione si conclude con dei “riquadri” che riportano esempi concreti di rischi sistemici ed esempi di come alcuni dei “fattori di rischio” elencati all'art. 34(2) DSA possano influenzare tali rischi sistemici.

La prima sottosezione è dedicata, come appunto vuole l'art. 34(1), lett. a), DSA, **al rischio di diffusione di contenuti illegali tramite i servizi forniti dai fornitori di VLOPs e VLOSEs**.

Più in particolare, nell'ambito di tale “categoria”, i più significativi e ricorrenti rischi rilevati riguardano:

- la vendita e/o la pubblicità di **prodotti illegali** (compresi prodotti pericolosi, non conformi e/o contraffatti quali cosmetici, giocattoli o articoli elettronici, armi da fuoco, esplosivi, prodotti medici e sanitari) e lo svolgimento di attività illegali (come, ad esempio, la fornitura o la pubblicità di servizi sessuali illegali, servizi che consentono l'ingresso, il transito o il soggiorno non autorizzati nell'Unione, il reclutamento in reti criminali, la vendita o lo scambio di ingenti somme di denaro contante e di sostanze stupefacenti illegali, servizi di attacchi informatici);
- la diffusione, specialmente attraverso i social media e i motori di ricerca, di **materiale pedopornografico e di “contenuti terroristici”** (l'elogio, l'agevolazione, il sostegno, il reclutamento di terroristi);
- la diffusione di discorsi di **incitamento all'odio** e di istigazione a commettere reati motivati dall'odio;
- la diffusione di **contenuti che violano i diritti di proprietà intellettuale** (marchi, diritti di design, brevetti e diritti d'autore, in particolare in relazione a merci contraffatte, film e musica piratati e servizi di streaming illegali).

La seconda sottosezione riporta i più significativi rischi relativi ai diritti fondamentali.

Rispetto, anzitutto, al **diritto alla libertà di espressione e di informazione** si osserva che i rischi individuati non riguardano singoli contenuti, ma piuttosto i sistemi utilizzati per diffondere o moderare questi ultimi (**sistemi di raccomandazione, sistemi pubblicitari, sistemi di moderazione dei contenuti**). Si segnala quindi, più in particolare, che tali rischi consistono

nella ingiustificata restrizione alla possibilità per gli utenti di esprimersi online e nella mancanza di accesso a una pluralità di opinioni. Nel “riquadro” dedicato ai “fattori” che possono influenzare i rischi sistemici relativi alla libertà di espressione e informazione si menziona, tra gli altri, l’eccessiva moderazione dei contenuti, che può essere aggravata da carenze nei meccanismi di ricorso e/o da un eccessivo affidamento a mezzi automatizzati senza un’adeguata revisione umana. Vengono, poi, riportati:

- rischi relativi al diritto fondamentale alla **non discriminazione** (quali la promozione di stereotipi e la diffusione su larga scala di pregiudizi nei confronti di gruppi specifici);
- rischi per i diritti dei **minori** (circa i quali si rinvia alla quarta sottosezione);
- rischi correlati al diritto alla tutela dei **consumatori** (relativi, ad esempio, alla messa in opera di: pratiche commerciali sleali, design che creano dipendenza, frodi, false recensioni), che, si rileva nel “riquadro esemplificativo”, possono essere esacerbati dal targeting mirato nei confronti di persone vulnerabili (quali gli anziani) o dalla introduzione di funzionalità di *gamification* che portano allo shopping compulsivo, nonché dall’impiego di sistemi di IA generativa (specialmente per facilitare le truffe); e, infine,
- rischi per i **diritti fondamentali alla vita privata e familiare e alla protezione dei dati** (si richiamano, in particolare e tra gli altri, i rischi legati alla diffusione non consensuale di immagini intime o di altre informazioni personali anche sensibili).

Come vuole, poi, l’art. 34(1)(c) DSA, **la terza sottosezione è relativa agli effetti negativi sul dibattito civico, i processi elettorali e la sicurezza pubblica.**

In termini generali, rispetto a tali rischi, diverse piattaforme di social media e motori di ricerca hanno riconosciuto come critico il ruolo svolto dai loro **sistemi algoritmici di raccomandazione dei contenuti** nella diffusione virale di narrazioni fuorvianti, nonché il ruolo che i **meccanismi algoritmici di ranking** possono giocare nell’esacerbare la disinformazione (si vedano, sul punto, in particolare, i “riquadri” esemplificativi al termine della sottosezione). Più in dettaglio, circa il dibattito civico, molti fornitori di VLOPs e VLOSEs hanno segnalato rischi legati, tra l’altro, alla **mancanza di diversità dei contenuti**, alla **polarizzazione**, alla diffusione su larga scala di **teorie cospirazioniste falsamente autorevoli** (presentandosi, ad esempio, sotto la veste di “fonti ufficiali”, come provenienti da istituzioni pubbliche, o di ricerche sottoposte a revisione paritaria).

Circa i processi elettorali, i rischi sistemici individuati includono la disinformazione e la misinformazione:

- sulle **date delle elezioni**,
- sull’**eleggibilità** dei candidati,
- sulle **procedure di registrazione** degli elettori.

Sono stati inoltre evidenziati **rischi derivanti dall’IA generativa**, in particolare il fatto che i **chatbot** basati su questa potrebbero rispondere in modo errato a domande relative alle elezioni.

Vengono, poi, altresì in evidenza rischi legati alla **disinformazione dannosa per i candidati a cariche pubbliche**, che possono essere soggetti a **furti di**

identità e alla messa in circolo di **contenuti “sintetici”** che li rappresentano falsamente.

Quanto infine alla **sicurezza pubblica**, i rischi segnalati sono, tra l’altro, legati alla diffusione virale di *fake news* relative a catastrofi naturali o a eventi quali sparatorie, attacchi terroristici o conflitti armati. Uno dei rischi più comunemente segnalati riguarda, in particolare, il **riutilizzo di vecchi contenuti**, come video di attentati o sparatorie di massa, presentati come eventi in tempo reale con l’obiettivo di scatenare il panico.

La quarta sottosezione ha infine ad oggetto i rischi relativi alla violenza di genere, alla protezione della **salute pubblica** e dei **minori** e alle conseguenze negative per il **benessere fisico e mentale** della persona.

Circa la prima, si osserva che l’uso diffuso dei servizi di intermediazione online ha contribuito alla comparsa e all’amplificazione della **violenza informatica di genere**, la quale risulta peraltro colpire in modo sproporzionato le **donne appartenenti a gruppi emarginati**, tra cui le **minoranze etniche** o religiose, le persone con **disabilità** e le **comunità LGBTIQ+**. Vengono altresì evidenziati rischi quali lo *stalking*, **l’adescamento**, **l’incitamento all’odio basato sul genere**, **la condivisione dolosa o non consensuale di dati personali** e di materiale sessualmente esplicito.

Rispetto alla salute pubblica, si segnalano rischi derivanti dalla **disinformazione o misinformation** in materia, ad esempio, di **vaccini** o di **gravi patologie** quali l’ebola, l’HIV o il diabete. Si evidenziano, poi, i rischi legati alla **vendita di prodotti medici** illegali, contraffatti o di qualità inferiore agli standard, nonché la vendita di **dispositivi medici, integratori o prodotti farmaceutici** non autorizzati (quali, ad esempio, i farmaci dimagranti). Si menzionano anche i rischi legati alla promozione di **sostanze legali ma nocive**, quali alcol, tabacco e farmaci soggetti a prescrizione medica. Quanto alla protezione dei minori, tra i rischi figurano, ad esempio, la presenza e la diffusione di **materiale pedopornografico**, il c.d. *“grooming”*, **il cyberbullismo**, **la promozione dell’autolesionismo**, **l’esposizione a contenuti violenti** e alle *“sfide pericolose”* diffuse sui **social media**. Sono altresì rilevati rischi relativi allo **sfruttamento commerciale dei minori** come *influencer*, anche da parte dei loro genitori o tutori, e i rischi legati all’impiego di **tecniche di marketing ingannevoli**. Circa il benessere fisico e mentale, sono infine individuati rischi riguardanti il **suicidio e l’autolesionismo**, **la diffusione di “standard corporei irrealistici”** e di **strategie errate o dannose contro i disturbi alimentari**. Vengono anche, tra gli altri, menzionati i rischi derivanti dall’**eccessivo tempo trascorso davanti allo schermo**, quali miopia e affaticamento della vista, nonché il fatto che gli utenti, in particolare i minori, possano trascurare attività essenziali quali il sonno, l’esercizio fisico e le interazioni sociali di persona.

Il quarto paragrafo è rivolto invece alla ricognizione delle **pratiche di attenuazione dei rischi individuati**. È **suddiviso in nove sottosezioni**, che pure seguono la struttura dell’art. 35(1) DSA (fatta eccezione per le misure di cui all’art. 35(1), lett. j), DSA, relative ai diritti dei minori, che non hanno una sottosezione dedicata in quanto già presentate nelle altre sottosezioni). In ogni modo, si precisa in termini generali, le pratiche individuate non devono essere

considerate isolatamente, ma piuttosto come “elementi” di una “combinazione di misure” volte a garantire la mitigazione dei rischi.

La prima sottosezione è dedicata alla misura dell’**adeguamento** della progettazione, delle caratteristiche e del funzionamento **dei servizi e delle interfacce online**. Tra le altre misure adottate o suggerite, figurano: la **limitazione *by default* della personalizzazione dei contenuti**, l’**utilizzo di “nudge” e “circuit breakers”**, ad esempio per ricordare agli utenti determinate regole prima della pubblicazione di contenuti, la **disattivazione per impostazione predefinita delle notifiche** (per evitare il rischio di dipendenza dal servizio), la **sfocatura di immagini e video** accompagnata da messaggi di avvertimento (ad esempio, per i contenuti che contengono violenza). Tra le misure per proteggere i minori, sono menzionate: la **limitazione dell’accesso alle funzioni di IA agli utenti adulti**, la **facilità di reperimento dei feed di contenuti educativi**, l’**utilizzo di “classificatori di contenuti” per diverse fasce d’età**, il **filtraggio dei risultati di ricerca** che il fornitore classifica come inappropriati per i minori, la **disattivazione predefinita delle funzioni di “scorrimento infinito” e riproduzione automatica**, la predisposizione di **strumenti di “parental control”** che consentano ai genitori di impostare limiti giornalieri per l’utilizzo delle app e di ricevere notifiche sul tempo trascorso dai figli davanti allo schermo.

La seconda sottosezione riguarda l’**«adeguamento delle condizioni generali e la loro applicazione»**. Sul punto, tutti i fornitori riferiscono di monitorare e aggiornare regolarmente i propri termini e condizioni. Rispetto in particolare alla tutela dei minori, alcuni fornitori hanno dichiarato di aver introdotto nei loro termini e condizioni disposizioni che limitano l’accesso dei minori ai loro servizi, nonché di effettuare regolari controlli di verifica dell’età.

La terza sottosezione, la più ampia, è **relativa alle procedure di moderazione dei contenuti**. I fornitori dei servizi, si riporta, menzionano sia **metodi di moderazione dei contenuti “proattivi”** (ovvero da parte dei fornitori stessi, con revisioni sia automatizzate che umane) che metodi **“reattivi”** (su segnalazione degli utenti). Si segnala altresì l’**utilizzo dell’IA**, sottolineandone tanto i vantaggi (ad esempio, la velocità di reazione) quanto i limiti (ad esempio, in punto di spiegabilità delle decisioni): in tal senso, si evidenzia, essa può al contempo rappresentare sia un fattore di rischio che una misura di mitigazione. Anche la **revisione umana**, tuttavia, non va esente da critiche; in particolare, si rileva la necessità che i moderatori umani siano ben formati e consapevoli dei contesti, delle lingue e delle culture locali. A livello operativo, si evidenzia come cruciale che il team di moderazione dei contenuti sia in stretta relazione con il team legale, al fine di potergli agilmente segnalare i cc.dd. “casi limite”. Viene, poi, tra le altre misure, menzionato anche l’uso di **filtri dei contenuti basati sull’età** per i minori (ad esempio, filtri diversi per gli utenti che si immaginano avere meno di 13 anni, tra i 13 e i 15 anni, tra i 16 e i 18 anni). Quanto ai contenuti più frequentemente citati come colpiti dalle “misure di moderazione”, si riportano: i contenuti illegali (inclusi i prodotti che violano la proprietà intellettuale e i prodotti non conformi o pericolosi); quelli che violano i termini e le condizioni, quali ad esempio i contenuti inappropriati per l’età, gli insulti e le molestie,

comportamenti discriminatori; contenuti provenienti da organizzazioni criminali; contenuti variamente “manipolatori”.

La quarta sottosezione, pure piuttosto ampia, è dedicata ai sistemi algoritmici, compresi i sistemi di raccomandazione. Tra le misure menzionate, si evidenzia: la progettazione di sistemi per la raccomandazione di contenuti diversificati e provenienti da fonti affidabili; la possibilità per gli utenti di reimpostare il proprio profilo di raccomandazione per ricalcare quello di un diverso utente o di disattivare *tout court* il sistema di raccomandazione, nonché la possibilità di segnalare un “disinteresse” rispetto a contenuti specifici o di richiedere di ridurre il tempo di esposizione a taluni contenuti; ancora, la possibilità di consentire all’utente di selezionare parole chiave per la visualizzazione o il filtraggio dei contenuti; l’uso di avvisi per aiutare gli utenti a comprendere perché determinati contenuti vengono loro raccomandati. Quanto in particolare ai minori, alcuni fornitori affermano di aver implementato ulteriori misure specifiche, quali la raccomandazione di contenuti più adatti alla loro età; altresì, si è proposto da parte delle organizzazioni della società civile, di limitare per impostazione predefinita le interazioni con utenti sconosciuti e dunque la possibilità che soggetti estranei contattino i minori tramite messaggi diretti.

La quinta sottosezione riguarda i sistemi di pubblicità e l’adozione di misure mirate volte a limitare o ad adeguare la presentazione della pubblicità associata al servizio prestato. Tra le riportate misure di mitigazione, si richiamano: l’adozione di processi di verifica degli inserzionisti (ad esempio, solo le organizzazioni della società civile verificate possono pubblicare annunci pubblicitari su determinati argomenti sensibili come i conflitti armati); il preliminare filtraggio degli annunci pubblicitari (finalizzato ad esempio all’esecuzione di controlli specifici per individuare gli annunci che potrebbero promuovere truffe, frodi, contenuti e servizi illegali o disinformazione, nonché prodotti come alcol e tabacco); l’utilizzo di requisiti minimi di audience per evitare un targeting troppo mirato; il divieto di pubblicità di contenuti generati dall’IA su argomenti sensibili come le elezioni, e la necessità di una “autodichiarazione” da parte degli inserzionisti sull’uso dell’IA nella creazione di una pubblicità. Quanto alle sanzioni in caso di violazione delle misure, i fornitori hanno principalmente menzionato la rimozione della pubblicità dalla piattaforma.

La sesta sottosezione considera, cumulativamente, le misure di cui all’art. 35(1), lett. f) e lett. k), DSA, ovvero, rispettivamente, **il rafforzamento dei processi interni, delle risorse, della sperimentazione, della documentazione o della vigilanza sulle attività dei fornitori e il ricorso a un contrassegno** ben visibile per fare in modo che un elemento di un’informazione, sia esso un’immagine, un contenuto audio o video, generati o manipolati, che assomigli notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che a una persona appaia falsamente autentico o veritiero, sia distinguibile quando è presentato sulle loro interfacce online. Tra le diverse misure menzionate e suggerite, compaiono: il ricorso all’IA per individuare contenuti creati dall’IA medesima (quali, ad esempio, i *deepfake*); la compilazione di un elenco degli account individuati come falsi; l’adozione di misure per impedire agli utenti “banditi” di rientrare nella piattaforma con

alias diversi o tramite intermediari; la possibilità che sistemi basati sull'IA confrontino i contenuti pubblicati con *database* e fonti affidabili per facilitare il lavoro dei cc.dd. “*fact-checkers*”.

La settima sottosezione è relativa alla misura di cui all'art. 35(1), lett. g), DSA, ovvero all'avvio o all'adeguamento della cooperazione con i **segnalatori attendibili** ex art. 22 DSA e all'attuazione della decisione degli **organismi di risoluzione extragiudiziale delle controversie** ex art. 21 DSA. Rispetto a queste misure, alcuni fornitori hanno dichiarato la compilazione di report provenienti dai segnalatori attendibili; il coinvolgimento di questi ultimi nei processi di sviluppo della sicurezza dei prodotti; la creazione di *dashboard* per consentirgli di seguire lo stato delle loro segnalazioni; la creazione di *partnership* con organizzazioni della società civile e autorità pubbliche affinché svolgano ruoli simili a quelli dei segnalatori attendibili.

L'ottava sottosezione si occupa della adozione di codici di condotta. Tra questi, alcuni fornitori hanno fatto riferimento al [Code of Conduct on Countering Illegal Hate Speech Online](#) e al [Code of Conduct on Disinformation](#) (precedentemente, *Code of Practice on Disinformation*) e alle misure di mitigazione ivi menzionate. Viene, inoltre, riportata la creazione di “sistemi di risposta rapida” per lo scambio di informazioni con le organizzazioni della società civile, i *fact-checkers*, altre piattaforme e le autorità.

La nona e ultima sottosezione è relativa all'adozione di misure di sensibilizzazione e all'adattamento delle interfacce online al fine di dare ai destinatari del servizio maggiori informazioni. Tra le misure menzionate dai fornitori: la creazione di “pannelli informativi autorevoli” in caso di particolari eventi quali elezioni o crisi; la messa in atto di campagne di alfabetizzazione sui media e la creazione di “pagine di assistenza” per il benessere degli utenti e di “guide” dedicate a genitori e tutori; la visualizzazione di banner con informazioni che gli utenti devono prendere in considerazione prima di commentare o caricare contenuti; l'adozione di etichette che informano che un *account* è stato verificato o che i contenuti sono stati controllati.

Infine, **il quinto paragrafo**, dal titolo «*outlook*» (prospettive), ha un po' il sapore di una *excusatio*. Come sottolineato anche in apertura, infatti, si ribadisce che la relazione costituisce la “prima edizione”, per quindi aggiungersi che l'accumulo delle edizioni future potrà fornire, nel tempo, una prospettiva a lungo termine sui rischi sistemici più rilevanti e ricorrenti. In particolare, si conclude, gli sviluppi nell'attuazione e applicazione di altre disposizioni del DSA, quali i meccanismi di accesso ai dati di cui all'art. 40 DSA, contribuiranno ad arricchire le informazioni che consentiranno una comprensione sempre migliore dei rischi sistemici e delle misure di mitigazione di cui agli artt. 34 e 35 DSA.

BENIAMINO PARENZO

<https://digital-strategy.ec.europa.eu/en/news/digital-services-act-report-lays-out-landscape-systemic-risks-online>

<https://digital-strategy.ec.europa.eu/en/news/press-statement-european-board-digital-services-following-its-16th-meeting>

| 1070

2025/4(15)BG

Le Linee guida EDPS dell'11.11.2025 Guidance for risk management of AI systems

Il documento del Garante europeo della protezione dei dati (**EDPS**) *Guidance for Risk Management of Artificial Intelligence systems* dell'11.11.2025 (le **Linee guida** o il **Documento**), si prefigge di fornire orientamenti alle istituzioni, gli organi e gli organismi dell'Unione europea (**IUE**) che operano in qualità di titolari del trattamento di dati personali ai sensi del regolamento (UE) 2018/1725 (**EUDPR**), con lo scopo di supportarli nell'identificazione e della mitigazione di taluni dei rischi per i diritti fondamentali degli interessati scaturenti nell'ambito dello sviluppo, dell'approvvigionamento e dell'implementazione di sistemi di intelligenza artificiale (IA).

Ed infatti, lo sviluppo, l'approvvigionamento e l'implementazione di sistemi di intelligenza artificiale (IA) implicanti il trattamento di dati personali da parte delle IUE sollevano rischi di rilevante entità per i diritti fondamentali e le libertà degli interessati, tra i quali assume peculiare pregnanza la tutela della riservatezza e della protezione dei dati personali. Il principio di responsabilizzazione (accountability), previsto dall'art. 4(2), e dall'art. 71(4) EUDPR, quale cardine della disciplina, impone alle IUE l'onere di individuare e mitigare siffatti rischi, nonché di comprovare le modalità attraverso le quali hanno adempiuto a tale obbligo.

Ai sensi dell'art. 1(3) EUDPR, l'EDPS sorveglia l'applicazione delle disposizioni dell'EUDPR a tutti i trattamenti di dati personali effettuati da un'istituzione o un organo dell'Unione europea. Inoltre, il regolamento (UE) 2024/1689 (**AI Act** o **AI**) ha designato l'EDPS quale autorità di vigilanza del mercato competente ai sensi del medesimo AI Act per le IUE che rientrano nell'ambito di applicazione del medesimo regolamento (artt. 3, n. 48 e 70(9) AIA).

Il Documento si articola in diverse sezioni. La prima esamina la metodologia di gestione dei rischi secondo la norma ISO 31000:2018. La seconda illustra il ciclo di vita tipico dello sviluppo dei sistemi di IA, nonché le distinte fasi che caratterizzano il loro approvvigionamento. La terza sezione approfondisce i concetti di interpretabilità e spiegabilità quali questioni trasversali, rilevanti ai fini della conformità all'insieme delle disposizioni oggetto della guida. Infine, la quarta sezione declina i quattro principi generali sopra enunciati — correttezza, esattezza, minimizzazione dei dati e sicurezza — in rischi specifici, ciascuno dei quali viene successivamente descritto e correlato a misure tecniche che i titolari del trattamento possono implementare al fine di mitigare i rischi medesimi.

Metodologia di gestione del rischio

Le Linee guida, come si è detto, si fondano sulle definizioni di rischio elaborate nella norma ISO 31000:2018. Conformemente a tale *standard* internazionale, la gestione del rischio si configura quale processo sistematico

mediante il quale un'organizzazione può presidiare e governare i rischi. Il nucleo fondamentale di tale processo è costituito dalla fase di valutazione del rischio, nel corso della quale l'organizzazione procede all'identificazione, all'analisi e alla successiva ponderazione dei rischi medesimi.

Gli orientamenti si incentrano precipuamente sul rischio di non conformità rispetto a taluni principi di protezione dei dati per i quali i controlli che i titolari del trattamento sono tenuti ad implementare possano rivestire natura tecnica.

L'attenzione è rivolta a due profili specifici del processo di gestione del rischio, ovverosia l'identificazione del rischio e il trattamento del rischio, atteso che gli aspetti attinenti all'analisi e alla valutazione del rischio risultano strettamente dipendenti dal contesto specifico del trattamento e, pertanto, si ritiene opportuno rimetterne la valutazione a ciascuna organizzazione in conformità ai propri criteri di rischio.

Il ciclo di vita dei sistemi di IA

Ai fini delle Linee guida, un sistema di IA è inteso ai sensi dell'articolo 3(1) AIA come *“un sistema basato su macchina progettato per operare con vari livelli di autonomia, che può esibire capacità di adattamento dopo l'implementazione e che, per obiettivi espliciti o impliciti, inferisce, dall'input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali”*.

I rischi possono manifestarsi in differenti stadi del ciclo di vita dello sviluppo di un sistema di IA. Risulta pertanto imprescindibile acquisire piena cognizione delle peculiarità che contraddistinguono il ciclo di vita dello sviluppo di un sistema di IA rispetto a un ciclo di vita di sviluppo convenzionale (dunque, relativo a sistemi non fondati sull'IA). Il ciclo di vita dello sviluppo di sistemi di IA si articola tipicamente nelle fasi di seguito enunciate:

- i. *Inception/Analisi*: tale fase iniziale implica la definizione puntuale della problematica che il sistema di IA si prefigge di risolvere, nonché la selezione dell'architettura del modello di IA.
- ii. *Acquisizione e preparazione dei dati*: i dati personali di addestramento necessari sono funzionali agli obiettivi perseguiti dal sistema di IA e devono essere opportunamente formattati, verificati in relazione ai requisiti qualitativi e giuridici applicabili, nonché normalizzati anteriormente al loro impiego.
- iii. *Sviluppo*: tale fase ricomprende la selezione degli algoritmi idonei, l'addestramento del sistema di IA sui dati previamente predisposti, l'esecuzione dei test e l'ottimizzazione degli iperparametri al fine di perfezionarne le prestazioni.
- iv. *Verifica e validazione*: successivamente alla fase di sviluppo, il sistema di IA è sottoposto a rigorosi processi di verifica e validazione volti ad accertare la conformità ai requisiti funzionali e non funzionali definiti nella fase di *inception*.
- v. *Fasi successive*, che ricomprendono l'implementazione, l'operatività e il monitoraggio, la validazione continua (qualora il sistema di IA si



avvalga dell'apprendimento continuo), la rivalutazione e la dismissione.

Interpretabilità e spiegabilità come condizioni *sine qua non*

L'interpretabilità e la spiegabilità sono questioni trasversali nell'approvvigionamento, nello sviluppo e nell'implementazione di sistemi di IA e costituiscono presupposti imprescindibili per le IUE operanti in qualità di titolari del trattamento al fine di assicurare l'adempimento dei propri obblighi derivanti dall'EUDPR. Nondimeno, interpretabilità e spiegabilità non devono essere confuse con la trasparenza: i primi due concetti attengono alla misura in cui il titolare del trattamento comprende il funzionamento del proprio sistema di IA, mentre quest'ultima concerne l'obbligo del titolare di fornire informazioni significative agli interessati.

L'interpretabilità concerne il grado in cui un modello o una decisione “*black box*” risulta comprensibile per l'essere umano. Si riferisce alla possibilità di comprendere il processo attraverso il quale un modello di IA giunge alle proprie determinazioni. Un modello dotato di interpretabilità funziona in modo trasparente, rendendo manifeste le correlazioni tra *gli input* ricevuti e *gli output* prodotti. Laddove un algoritmo sia interpretabile, un operatore umano sarà in grado di descriverne il funzionamento in termini chiari e accessibili. Tale caratteristica riveste un'importanza fondamentale al fine di consentire agli utenti di comprendere i modelli di riporvi adeguata fiducia e di IA.

La spiegabilità nell'IA si incentra sulla fornitura di spiegazioni chiare e coerenti per specifiche previsioni o decisioni del modello. Essa attiene alla capacità di chiarire come un modello di IA prende decisioni in maniera accessibile agli utenti finali. Un modello spiegabile fornisce spiegazioni chiare e intuitive per i propri *output*, agevolando gli utenti nella comprensione delle ragioni sottese a un particolare risultato.

La distinzione tra interpretabilità e spiegabilità risiede nel fatto che la prima concerne la comprensione del funzionamento interno dei modelli di IA, mentre la seconda si incentra sulla spiegazione delle decisioni assunte da tali modelli. Inoltre, l'interpretabilità è tipicamente destinata agli esperti di IA e ai ricercatori, mentre la spiegabilità si incentra sulla comunicazione efficace delle decisioni del modello agli utenti finali. Pertanto, la spiegabilità richiede una presentazione delle informazioni maggiormente semplice e intuitiva. Ciò risulta necessario al fine di garantire, tra l'altro, che: (i) l'organizzazione possa riporre fiducia nel sistema di IA affinché operi conformemente alle previsioni; (ii) gli errori e i *bias* dei modelli possano essere tempestivamente individuati; (iii) l'organizzazione possa rilevare le ipotesi di utilizzo improprio del sistema di IA; (iv) i criteri decisionali risultino conformi agli obiettivi dell'organizzazione; e infine (v) il sistema di IA sia suscettibile di verifica.

I sistemi di IA non interpretabili o non esplicabili presentano rischi significativi perché operano come “*black box*” in cui i meccanismi interni e i processi decisionali rimangono opachi agli utenti umani, rendendo difficile comprendere come e perché determinati output o decisioni sono stati generati. Quali possibili misure di mitigazione, gli orientamenti indicano: (i) una documentazione appropriata che contempli la tipologia di architettura di IA

impiegata, i dettagli sulla provenienza dei dati personali di addestramento, le informazioni sulle modalità operative del sistema di IA e sul grado di accuratezza tra diversi gruppi, una descrizione dei potenziali *bias* e delle limitazioni del sistema; (ii) il ricorso a tecniche di spiegabilità quali LIME o SHAP; e (iii) l'analisi statistica degli output del sistema di IA.

V. Rischi associati ai principali principi di protezione dei dati

V.I. Principio di correttezza (*fairness*)

Sebbene l'EUDPR non definisca esplicitamente la correttezza, essa costituisce un principio generale del diritto della protezione dei dati, sancito dall'articolo 8(2) della Carta dei diritti fondamentali dell'UE (CDFUE), mentre l'obbligo per i titolari di conformarsi al principio del trattamento corretto è stabilito dall'articolo 4(1)(a) dell'EUDPR.

Il Comitato europeo per la protezione dei dati (EDPB) ha avuto modo di precisare che la correttezza costituisce un principio di carattere generale, il quale esige che i dati personali non siano oggetto di trattamento in maniera indebitamente pregiudizievole, illecitamente discriminatoria, inattesa ovvero fuorviante nei confronti dell'interessato. Al fine di assicurare la correttezza del trattamento, è opportuno procedere a una valutazione delle modalità con cui il trattamento medesimo inciderà sugli interessi e sui diritti fondamentali delle persone interessate, sia in quanto gruppo sia individualmente considerate, e i dati personali non devono essere impiegati secondo modalità suscettibili di produrre effetti pregiudizievoli ingiustificati in capo agli interessati.

Un rischio di rilevante entità, idoneo a determinare la non conformità al principio di correttezza nel contesto in esame, è rappresentato dalla sussistenza di *bias*. Sebbene non esista una definizione univoca e universalmente recepita di *bias* nell'ambito dell'intelligenza artificiale, tale nozione si riferisce comunemente alla produzione di risultati iniqui, pregiudizievoli ovvero sistematicamente erronei, che favoriscono o discriminano determinati gruppi di persone o tipologie di *input*.

Tra le cause originarie del *bias* in un contesto di intelligenza artificiale possono annoverarsi: il *bias* algoritmico, allorché la progettazione del sistema di IA sia di per sé idonea a generare risultati distorti; i dati personali di addestramento, qualora questi ultimi presentino distorsioni che il sistema di IA apprenderà, producendo conseguentemente risultati parimenti viziati; ulteriori *bias* di matrice umana, laddove gli sviluppatori o i soggetti preposti all'addestramento ovvero all'utilizzo di un sistema di IA introducano, consapevolmente o inconsapevolmente, i propri pregiudizi nella progettazione o nell'implementazione dei sistemi medesimi.

Gli orientamenti identificano cinque rischi specifici relativi al principio di correttezza: (i) *bias* causato dalla mancanza di qualità dei dati nei dati personali di addestramento; (ii) *bias* nei dati personali di addestramento; (iii) *overfitting* sui dati personali di addestramento; (iv) *bias* algoritmico; e infine (v) *bias* di interpretazione. Per ognuno di tali rischi sono proposte corrispondenti misure di mitigazione.

V.II. Principio di esattezza (*accuracy*)

Secondo l'articolo 4(1)(d) EUDPR, i dati personali devono essere esatti e, ove necessario, aggiornati, e deve essere compiuto ogni passo ragionevole per



garantire che i dati personali inesatti, avuto riguardo alle finalità per le quali sono trattati, siano cancellati o rettificati senza indugio.

Contrariamente al significato del principio di protezione dei dati dell'esattezza, nel contesto dell'IA, l'accuratezza (“*statistical accuracy*”) è una metrica di *performance* che misura quanto spesso un sistema di IA indovina la risposta corretta diviso per il numero totale di previsioni.

Il mancato accertamento dell'accuratezza statistica può creare un rischio di *non compliance* con il principio dell'esattezza dei dati quando conduce alla diffusione di modelli di IA che producono dati personali inesatti, e un modello di IA può generare informazioni errate o insensate (inclusi dati personali) che non erano presenti nei suoi dati personali di addestramento o nell'input ricevuto.

Per gestire efficacemente i rischi di protezione dei dati nell'approvvigionamento di un sistema di IA pre-addestrato, le organizzazioni devono concentrarsi sulla comprensione dei processi di sviluppo impiegati dal fornitore di IA, ponendo domande riguardanti il sistema di IA nel suo complesso e approfondendo i dettagli su come i rischi rilevanti sono stati adeguatamente gestiti. L'organizzazione dovrebbe invitare il fornitore a produrre: (i) documentazione generale sulle specifiche tecniche e l'architettura; (ii) documentazione sull'interfaccia utente e le API; (iii) documentazione su trasparenza, interpretabilità e spiegabilità; (iv) documentazione sulle misure di cybersecurity relative all'integrità del modello; e infine (v) documentazione sulle pratiche di governance dei dati personali; procedure e risultati di validazione e *test*.

V.III. Principio di minimizzazione dei dati

Per apprendere accuratamente i *pattern*, effettuare previsioni affidabili e generalizzare bene a nuovi dati non visti, i sistemi di IA sono spesso addestrati su *dataset* di grandi dimensioni; tuttavia, le IUE devono garantire la conformità con il principio di minimizzazione dei dati sancito dall'articolo 4(1)(c), secondo cui i dati personali devono essere “*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*”.

Data la dipendenza dei modelli di *machine learning* dai loro dati di addestramento, vi è una tendenza a raccogliere e trattare quanti più dati di addestramento possibile, e la raccolta di grandi volumi di dati senza criteri chiari o pertinenza può condurre all'accumulo di informazioni che potrebbero non essere necessarie per gli obiettivi del sistema di IA e potrebbero essere contrarie al principio di minimizzazione dei dati.

V.IV. Principio di sicurezza

L'obbligo di garantire la sicurezza dei dati personali è sancito dall'articolo 4(1)(f) dell'EUDPR, secondo cui i dati personali devono essere trattati in modo da garantire un'adeguata sicurezza, inclusa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danno accidentali, utilizzando misure tecniche o organizzative appropriate.

Data la quantità di dati richiesti per addestrare il sistema di IA, questi dati personali di addestramento sono preziosi e, se la loro riservatezza è compromessa, potrebbero essere utilizzati per colpire individui i cui dati sono stati divulgati; la riservatezza potrebbe essere compromessa sfruttando vulnerabilità specifiche dell'IA come gli attacchi di inversione del modello

(*model inversion attacks*), e un altro esempio potrebbe essere la manipolazione dei dati personali di addestramento (*data poisoning*) o del modello di IA stesso (*model poisoning*) per introdurre errori nel sistema di IA.

I principali rischi individuati dall'EDPS per la presente categoria sono: (i) divulgazione di dati personali di addestramento tramite *output* del sistema di IA; (ii) conservazione di dati personali e violazioni dei dati personali; e infine (iii) fuga di dati personali attraverso interfacce di programmazione delle applicazioni (**API**).

V.V. Diritti degli interessati

Similmente a quanto disposto dal reg. (UE) 2016/679 (**GDPR**), l'EUDPR conferisce agli interessati vari diritti individuali, tra cui il diritto di accesso (art. 17 EUDPR), alla rettifica (art. 16 EUDPR), alla cancellazione (art. 19 EUDPR), alla limitazione (art. 20 EUDPR), alla portabilità dei dati (art. 22 EUDPR) e all'opposizione (art. 23 EUDPR). La natura complessa dei sistemi di IA può rendere più difficile per le IUE dare seguito a tali diritti, specialmente quando gli interessati esercitano tali diritti rispetto ai dati personali contenuti nei dataset di addestramento, che il modello potrebbe poi "memorizzare" e rigurgitare nella fase di inferenza.

Gli orientamenti identificano due rischi fondamentali: (i) identificazione incompleta dei dati personali trattati e (ii) rettifica o cancellazione incompleta, identificando relative misure di mitigazione.

Conclusioni

L'implementazione di sistemi di intelligenza artificiale che comportano il trattamento di dati personali configura rischi di rilevante entità per gli interessati, rispetto ai quali le IUE, operanti in qualità di titolari del trattamento, sono gravate da un obbligo di identificazione, valutazione e mitigazione.

Le Linee guida non si prefiggono di costituire un catalogo esaustivo dei rischi e delle relative strategie di mitigazione, bensì intendono fornire un quadro metodologico di carattere pratico, volto a supportare le IUE nella corretta impostazione di un approccio sistematico alla gestione del rischio, suscettibile di integrazione in considerazione di ulteriori profili di rischio e requisiti di conformità.

Il presidio dei rischi connessi ai sistemi di intelligenza artificiale da parte dei titolari del trattamento non costituisce un adempimento marginale, bensì un obbligo cruciale per le IUE: la conformità all'EUDPR, la salvaguardia dei diritti fondamentali e la preservazione della fiducia pubblica sono inscindibilmente correlate alla capacità dei titolari del trattamento di identificare, valutare e mitigare proattivamente i rischi lungo l'intero ciclo di vita dei sistemi di intelligenza artificiale. Tale imperativo trascende la dimensione di una valutazione meramente episodica, imponendo l'adozione di una cultura improntata alla responsabilizzazione, al monitoraggio e al miglioramento continuo.

BEATRICE GALLUCCI



https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2025-11-11-guidance-risk-management-artificial-intelligence-systems_en

| 1076

2025/4(16)AG

Gli orientamenti del 14.7.2025 della Commissione europea sulle misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online ai sensi dell'art. 28(4) del DSA (Comunicazione C/2025/5519)

Gli Orientamenti quali fonti del diritto: finalità. Il 14.7.2025, la Commissione europea (la **Commissione**) ha emanato un corpo di linee guida (gli **Orientamenti**) per rafforzare la privacy, la sicurezza e la protezione dei minori, in attuazione dell'art. 28(4) del regolamento (UE) 2022/2065 (Digital Services Act, **DSA**), ai sensi del quale alla Commissione è attribuito il potere, da esercitare previa consultazione del Comitato europeo per i servizi digitali (**EBDS**) (artt. 61 ss. DSA), di «emanare orientamenti per assistere i fornitori di piattaforme online nell'applicazione del paragrafo 1» del medesimo art. 28 DSA.

La finalità degli Orientamenti consiste quindi nell'esplicitare e specificare una serie di misure, da attuarsi anche *by design*, di buone pratiche e regole di *governance* della piattaforma, le quali, nel loro complesso, consentano ai fornitori di piattaforme online di adempiere al disposto del paragrafo 1 dell'art. 28 DSA, a tenore del quale: «[i] fornitori di piattaforme online accessibili ai minori adottano *misure adeguate e proporzionate* per garantire un elevato livello di tutela della *vita privata*, di *sicurezza* e di *protezione* dei minori sul loro servizio».

La vita privata, cioè la riservatezza, è un diritto fondamentale del minorenne, a cui si lega strettamente la capacità di autodeterminarsi, nel senso che più sono sconosciuti a terzi i dati e le attività online del minore e più quest'ultimo conserva uno spazio interiore libero dall'induzione e dalla manipolazione. Vedremo come diverse sono le prescrizioni rivolte dagli Orientamenti ai fornitori di piattaforme, finalizzate proprio a sostenere la libertà decisionale del minore e a proteggerne l'equilibrio psico-fisico. A ciò si aggiungono quelle indicazioni tecnologiche, sempre contenute negli Orientamenti, finalizzate ad evitare che il minore entri in contatto con contenuti e utenti pericolosi. Più esattamente, gli Orientamenti indicano 5 categorie di rischio denominate le 5C: **content, conduct, contact, consumer risks, cross-cutting risks**.

Se gli Orientamenti attuano l'art. 28(1) DSA, ne diventano una fonte del diritto integrativa, fondamentale per interpretarlo e attuarlo, cosicché le autorità indipendenti nazionali – in particolare l'Autorità per le garanzie nelle comunicazioni (**AGCOM**) nominato quale Coordinatore dei servizi digitali ai sensi dell'art. 15(1), d.l. 123/2023 conv. in l. n. 159/2023 (su cui v. in questa rubrica notizia n. 24 del [numero 2/2024](#) [2024/2(24)MVT], in *PeM* 2024, p. 732) – e la Commissione (art. 66 DSA) ad essi faranno riferimento nell'esercizio dei loro poteri di controllo e sanzionatori.

Sul piano delle fonti del diritto, è inevitabile che in ambiti altamente tecnologici il legislatore attribuisca a determinate istituzioni funzioni normative, essendo necessaria una regolamentazione dettagliata caratterizzata da una terminologia specialistica. Inoltre, va considerata la rapida obsolescenza di queste stesse regole, incompatibile con i tempi del procedimento legislativo, per cui, al fine di evitare uno scarto tra regolazione giuridica e realtà tecnologica, gli Orientamenti hanno previsto che la Commissione europea effettuerà un riesame dei medesimi ogni anno per valutare la necessità o meno di un loro adeguamento.

Accessibilità alla piattaforma e valutazione del rischio. Gli Orientamenti richiamano il considerando 71 DSA in cui si stabilisce quando la piattaforma online debba essere considerata accessibile al minore. Si indicano tre casi: 1) se le condizioni generali di contratto consentono ai minori di utilizzare il servizio; 2) se il servizio offerto dalla piattaforma «è rivolto o utilizzato prevalentemente da minori»; 3) se il fornitore della piattaforma «è altrimenti a conoscenza del fatto che alcuni dei destinatari del suo servizio sono minori perché egli già tratta i dati personali del suo servizio che rivelano la loro età per altri scopi» (ad es.: durante la creazione dell'account, gli utenti devono indicare la propria età, oppure la piattaforma monitora le interazioni e i contenuti condivisi, riconoscendo che alcuni utenti sono bambini o adolescenti).

Quando la piattaforma è accessibile ai minori, tutti i fornitori, anche se non si tratta di VLOP (*Very Large Online Platform*) o di VLOSE (*Very Large Online Search Engine*), devono effettuare la valutazione dei rischi, la quale impone di tenere conto dei seguenti elementi: a) probabilità che i minori accedano al servizio; b) impatto effettivo o potenziale sulla privacy, sicurezza e protezione dei minori che l'uso della piattaforma possa comportare sulla base della tipologia dei 5 rischi online per i minori sopra indicati, i quali rischi attengono esattamente: 1) al **contenuto** presente nell'ambiente digitale (ad es.: frasi/video incitanti all'odio, disinformazione); 2) al **comportamento** dell'utente online [ad es.: comportamenti incitanti all'odio, dannosi (video violenti/pornografici) o illegali (materiale pedopornografico/contenuti terroristici)]; 3) al **contatto** tra utenti potenzialmente pericoloso (ad es.: adescamento online, coercizione e estorsione sessuale online, cyberbullismo, furto di identità e altro ancora); 4) all'essere il minore un **consumatore** (vi sono rischi legati al marketing, alla profilazione commerciale, rischi finanziari o legati all'acquisto e al consumo di droghe, medicinali, alcool e altri prodotti pericolosi); 5) **rischi trasversali** che riguardano tutte le categorie di rischi e che possono influenzare negativamente la vita dei minori in diversi modi [ad es.: rischi da utilizzo di *chatbot*, rischi per la salute (obesità, anoressia, disturbi della concentrazione e del sonno per uso eccessivo delle piattaforme, depressione, isolamento sociale), rischi per la privacy e per la protezione dei dati (geolocalizzazione)].

La garanzia dell'età. La garanzia dell'età (age assurance) è il primo punto affrontato dagli Orientamenti nel segno dell'individuazione delle soluzioni più efficaci per impedire al minorenne di accedere a contenuti riservati ai maggiorenni. Se questo è l'obiettivo – precludere l'accesso – il fornitore di piattaforme online deve adottare misure adeguate e proporzionate idonee ad



assicurare che l'utilizzatore non abbia un'età inferiore a quella prevista nelle condizioni generali per l'utilizzo del servizio.

È evidente l'importanza apicale di tale garanzia, volta a salvaguardare soprattutto l'equilibrio psico-fisico del minore, il quale, se esposto prematuramente a contenuti inadeguati, rischia di pregiudicare il suo percorso formativo ed educativo.

Le soluzioni prospettate negli Orientamenti per assicurare la garanzia dell'età muovono dalla constatazione secondo cui gli sviluppi della tecnologia consentirebbero al fornitore di avere certezza dell'età di chi gli chieda l'accesso alla piattaforma. In ragione di ciò, viene scartato il metodo dell'autodichiarazione, ritenuto del tutto inadatto ad assicurare quell'elevato livello di protezione del minore preteso dall'art. 28(1) DSA.

Neppure il metodo - pure preso in considerazione dagli Orientamenti - della stima dell'età fornisce certezza degli anni del richiedente l'accesso alla piattaforma, poiché esso consente una valutazione soltanto probabilistica dell'età o dell'appartenenza a una certa fascia di età.

Le piattaforme devono, invece, pretendere il «token di età anonimizzato». Si tratta di uno strumento che prevede la partecipazione di un terzo, il quale fornisce all'utente un token, appunto, che potrà essere reso disponibile dallo stesso utente al fornitore di servizi, senza dover dimostrare nuovamente la propria età. Attraverso questo strumento, il fornitore avrà la certezza dell'età dell'utente e non incorrerà nel rischio di concedere l'accesso a chi non abbia ancora raggiunto l'età minima.

Questi sistemi tecnologici, al fine di rispettare il diritto alla privacy di chi voglia adoperarli, devono essere a «doppio cieco», ossia poter garantire un doppio anonimato: nei confronti del **fornitore della piattaforma**, il quale **non identifica il potenziale utente**, essendo sufficiente la garanzia dell'età di quest'ultimo, e nei confronti del **fornitore del servizio di verifica dell'età**, il quale **non viene a conoscenza dei servizi per i quali verrà utilizzata la prova dell'età**.

Il problema, dunque, della garanzia dell'età, di recente ancora gravemente eluso (cfr. la decisione del 10.4.2025 Garante per la protezione dei dati personali nel [caso Replika](#), su cui v. in questa rubrica la notizia n. 18 del [numero 2/2025](#) [2025/2(18)IG], in *PeM* 2025, p. 653), appare in via di soluzione, anche perché nell'Agenda dei consumatori 2030 (sul quale v. *supra* in questo numero di questa rubrica, il contributo n. 10 [2025/4(10)AA]) si afferma che nel quarto trimestre del 2026 verranno introdotti in tutti gli Stati membri i portafogli di identità digitale dell'UE ([EU digital identity wallets](#)). Il portafoglio europeo di identità digitale, previsto al capo II, sezione 1, del regolamento UE n. 910/2014 (regolamento **eIDAS**) come modificato dal regolamento (UE) 2024/1183 (regolamento **EUDI**), è un mezzo di identificazione digitale pensato per essere sicuro, affidabile e rispettoso della privacy per tutti i cittadini dell'Unione. In proposito, si ricorda la normativa nazionale (art. 13-*bis* d.l. 123/2023) con riguardo all'accesso a siti pornografici, pericolosi per «il benessere fisico e mentale» dei minori, unitamente alla [delibera AGCOM 96/25/CONS](#) (che ha dato attuazione al comma 3 dell'art. 13-*bis* d.l. 123/2023) che ha imposto ai fornitori di tali

piattaforme il ricorso a modalità tecniche e di processo che prevedano il ricorso a un soggetto terzo e indipendente.

Accesso: registrazione/non registrazione alla piattaforma. Gli Orientamenti distinguono due casi.

Il primo è caratterizzato dalla richiesta di registrazione del minore come condizione di accesso alla piattaforma online. Qui, nel richiamare alcune disposizioni del DSA, gli Orientamenti sintetizzano i diversi obblighi a carico dei fornitori delle piattaforme. Tra questi meritano una particolare sottolineatura i seguenti: i) spiegare tutti i vantaggi e i rischi della registrazione e, se del caso, la ragione di questa; ii) garantire che il processo di registrazione sia facilmente accessibile, navigabile da tutti i minori in base alle loro capacità in evoluzione, compresi i minori disabili e condotto in una lingua comprensibile; iii) evidenziare le caratteristiche di sicurezza della piattaforma o del servizio, le regole di condotta e le rispettive conseguenze in caso di violazione dei termini, oltre a porre in rilievo eventuali rischi previamente individuati (nella valutazione di cui si diceva innanzi) per la privacy, la sicurezza, l'incolumità dei minori e le risorse tecniche disponibili per assistere gli utenti.

L'individuazione e la comunicazione dei rischi in fase di registrazione sono funzionali a far maturare nel minorenne la consapevolezza della prudenza nelle attività in piattaforma. La prudenza interviene quando si è consapevoli dei pericoli presenti in un certo contesto o ingenerati da una determinata condotta. E allora, con i predetti doveri si intende promuovere nei più giovani la piena consapevolezza della pericolosità, anche per la propria incolumità fisica, dell'ambiente virtuale in cui l'utente ineducato, malvagio e le tecnologie manipolanti possono incidere sull'equilibrio psico-fisico ancor più rispetto a quanto possa verificarsi nel mondo fisico.

Su questo aspetto, si ricorda l'art. 24(2) lett. e), l. n. 132/2025, il quale, tra i principi e i criteri direttivi della delega legislativa al Governo, richiede la «previsione di percorsi di alfabetizzazione e formazione in materia di utilizzo di sistemi di intelligenza artificiale». Occorre avere piena contezza dei rischi dell'ambiente digitale, il che postula, al contempo, anche e soprattutto, la consapevolezza di quali siano le «vie maestre» per una crescita e una formazione adeguata del proprio essere. Solo con questo bagaglio conoscitivo il minorenne è più protetto da pregiudizi alla propria sfera interiore, dal crollo dell'autostima e della sicurezza di sé e dalla perdita della capacità di concentrazione e della tranquillità d'animo, essenziali per svolgere le proprie attività formative.

Per raggiungere questo fondamentale risultato protettivo e promozionale dell'esistenza del minore, accanto ai doveri di comunicazione e all'alfabetizzazione digitale si pongono, come si vedrà in seguito, altre misure operanti fin dalla progettazione della piattaforma.

Nel secondo caso cui si accennava sopra, non è richiesta la registrazione per accedere alla piattaforma. In tale eventualità, se vi è consapevolezza da parte del fornitore del fatto che qualsiasi utente non registrato possa essere un minore al di sotto della soglia stabilita per l'accesso, gli Orientamenti impongono al fornitore stesso di assicurare comunque protezione. Occorrerà, allora, configurare le impostazioni degli utenti non registrati in modo da



garantire il massimo livello di privacy, sicurezza e protezione, tenendo conto delle raccomandazioni di cui alle sezioni 6.3.1. (impostazioni predefinite) e 6.3.2. (disponibilità di impostazioni, caratteristiche e funzionalità) degli Orientamenti, su cui ci si soffermerà *infra* nei punti salienti.

Impostazione dell'account e salvaguardia della privacy e dell'autodeterminazione del minore. Le impostazioni predefinite incarnano la «misura adeguata» che i fornitori di piattaforme online devono assumere per garantire il massimo livello di privacy e l'autodeterminazione dei minorenni (sez. 6.3.1. Orientamenti). Esse, infatti, secondo le osservazioni empiriche, tendono a non essere modificate dall'utente. E allora i fornitori sono tenuti ad utilizzarle, onde assicurare il più ampio spazio possibile alla riservatezza e, di conseguenza, alla libertà delle scelte. C'è, infatti, un rapporto di proporzionalità inversa tra riservatezza e autodeterminazione: meno si conosce della personalità e degli interessi del minore e più quest'ultimo, non indotto da forze esterne, ha modo di riflettere sui suoi desideri e su ciò che vuole maggiormente.

Gli Orientamenti fissano, insomma, le condizioni affinché la persona possa conservare e rafforzare consapevolezza e possibilità di autodeterminazione. Ecco che il fornitore è tenuto ad abilitare le funzioni che consentono il controllo da parte degli utenti sulle loro interazioni; ad esempio poter richiedere il rallentamento della visualizzazione di certi contenuti. La finalità di questa misura tecnica specifica è di favorire la riflessione e la scelta di altri contenuti, spostando la propria attenzione su altro.

Va garantito altresì che i minori acquisiscano un controllo progressivo delle impostazioni, così da favorire la loro crescente autonomia, compresa la possibilità di ritornare alle impostazioni originarie. Occorre però che il fornitore valuti pure l'opportunità di rendere irreversibili alcune impostazioni, in particolare quando i rischi legati alla reversibilità appaiano superiori ai possibili benefici.

Oltre alle misure per favorire l'autonomia del minore, gli Orientamenti si occupano della protezione della sua integrità psico-fisica dal pericolo da contatti non previsti e inadeguati con altri utenti. Secondo gli Orientamenti, a prescindere dalle impostazioni dell'account scelte dai minori, il fornitore deve impedire che questi ultimi possano essere individuati o contattati da account non accettati in precedenza come propri contatti. A tali account, estranei al mondo online del minore, deve essere preclusa la visualizzazione delle informazioni del profilo, delle attività e della cronologia delle attività del minore stesso (sez. 6.3.2).

Progettazione dell'interfaccia e gestibilità dell'esperienza online da parte del minore. Gli Orientamenti sono netti nel richiedere ai fornitori di far funzionare le piattaforme in modo da non essere persuasive e da consentire ai minori di avere il controllo dell'esperienza online (sez. 6.4). Del resto, la manipolazione della mente fa leva anche sull'impossibilità di incidere sui contenuti osservabili, così da essere trasportati con facilità, passivamente, da una parte all'altra del mondo virtuale, dove il confine tra realtà e costruzione vuota di senso è impercettibile.

Da questo punto di vista, appaiono significative alcune prescrizioni contenute negli Orientamenti: a) la progettazione non deve essere persuasiva, perciò

essa non deve mirare prevalentemente a coinvolgere il minore, né a fargli utilizzare oltre misura la piattaforma. Ad es., andrebbero introdotte notifiche personalizzate sul tempo trascorso online, per indurre il minore a dedicarsi ad altro o a ritornare, se magari era dedito allo studio, su ciò che stava facendo in precedenza; b) è vietata l'attivazione automatica di chatbot e l'induzione all'utilizzo di questi "compagni di discussione", i quali possono influenzare e sviare il minore, il cui equilibrio psichico è delicato e la sua mente facilmente modellabile. Il dialogo con la macchina, la quale assurge ad amico, confidente, finanche partner romantico, presenta più rischi che benefici qualora l'interlocutore sia un minorenne. Si pensi anche solo al fatto che una delle dinamiche più significative della discussione tra il minore e i genitori è la scelta da parte di questi ultimi del silenzio o del contenimento di certe prospettazioni. Discutere con i figli certo è importante, ma ancora più efficace nell'educazione degli stessi, come affermato nella letteratura psicopedagogica, è l'esempio che i genitori offrono con i loro comportamenti nella quotidianità. La macchina, invece, oltre ad essere disincarnata, non sembra in grado di dosare e personalizzare i contenuti delle sue risposte e questo può risultare destabilizzante per il minorenne; c) i sistemi di raccomandazione, protesi ad amplificare i contenuti, già oggetto di una disciplina volta a promuovere la libertà di scelta (artt. 27 par. 1 e 38 DSA), devono imperniarsi, da un lato, sui «segnali impliciti basati sul coinvolgimento» del minorenne – *id est* su tutto ciò da cui dedurre le preferenze (ad es.: il tempo trascorso a visualizzare certi contenuti e i tassi di clic) – dall'altro, sui «segnali espliciti» forniti dall'utente minorenne – *id est* sui feedback e sulle interazioni che indicano le preferenze esplicite sia positive che negative, compresa la selezione dichiarata e deliberata di argomenti di interesse, sondaggi, segnalazioni e altri segnali basati sulla qualità (sez. 6.5.1) – . La bilancia dei sistemi di raccomandazione, quindi, in un sistema antropocentrico, deve pendere dal lato della valorizzazione della personalità del minore e non da quello dell'indirizzamento verso contenuti e realtà sponsorizzati dalla macchina.

Pratiche commerciali, acquisti online da parte del minore e influencer marketing. Nella sez. 6.6 degli Orientamenti, si rileva che i minori sono particolarmente esposti agli effetti persuasivi delle pratiche commerciali e devono essere protetti dalle pratiche di sfruttamento economico da parte delle piattaforme online, trovandosi ad affrontare tattiche persuasive diversificate, dinamiche e personalizzate, per esempio sotto forma di **pubblicità, inserimento di prodotti (product placement), uso di valute in-app, marketing da parte degli influencer, sponsorizzazioni e nudge potenziati dall'IA.**

In conseguenza di ciò, vengono individuate (nelle lettere a)-n) del punto 69 degli Orientamenti), ben **quattordici misure** che le piattaforme devono adottare per conformarsi al quadro giuridico orizzontale in vigore, in particolare per assicurare il rispetto delle disposizioni di cui alla **direttiva 2005/29/CE** relativa alle pratiche commerciali sleali (ritenuta pienamente applicabile a tutte le pratiche commerciali anche nei confronti dei minori), e alle norme del **DSA** in materia di pubblicità (artt. 26, 28(2) e 39 DSA) e di percorsi oscuri (art. 25 DSA).

Le misure previste dagli Orientamenti nella sezione 6.6 intendono contrastare quelle pratiche che sono idonee ad avere un effetto negativo sulla vita privata, sulla sicurezza e sulla protezione dei minori, comprese quelle pratiche idonee a ingenerare dipendenze che possano avere effetti negativi sulla privacy e sulla salute, determinando un circolo vizioso: più il minore acquista, più lascia segni di sé online e più viene indotto ad acquistare lo stesso prodotto o beni simili (effetto di trascinamento).

Tra le molte misure previste negli Orientamenti, il punto 69, lett. j) **vieta alle piattaforme di predisporre sistemi di acquisti «in app» o «in-game» che sono o sembrano necessari per accedere ad un servizio o per utilizzarlo, quando i minori accedono a piattaforme online o a parti e funzioni delle stesse che sono presentate o appaiono come gratuite.** Se i minori sono esposti a qualsiasi altro acquisto *in-app* o *in-game*, gli Orientamenti prescrivono che il prezzo debba sempre essere indicato nella valuta nazionale. Le «valute *in app*» consistono in valute virtuali sotto forma di crediti o denaro elettronico che permettono agli utenti di acquistare beni, servizi o oggetti virtuali. Queste valute virtuali possono essere acquistate con denaro reale e dunque il minorenni potrebbe essere indotto a spese eccessive, maturare dipendenze e assumere comportamenti compulsivi. Molte *app* offrono anche valute gratuite guadagnate tramite attività o premi che consentono di proseguire e di rimanere ulteriormente connessi (c.d. economia dell'attenzione).

In proposito, gli Orientamenti impongono alle piattaforme di garantire che i minori non siano esposti a tecniche che possono avere l'effetto di ridurre la trasparenza delle transazioni economiche e che possono essere fuorvianti per i minori, facendo proprio l'esempio di alcune valute virtuali e altri token o monete che possono essere scambiati con denaro reale (o, se del caso, per l'acquisto di un'altra valuta virtuale) e utilizzati per acquistare articoli virtuali, causando in tal modo anche spese indesiderate (punto 69, lett. i)).

Le valute a pagamento sono più pericolose per il minorenni, ecco perché sono state vietate anche nei giochi online (c.d. valute *in game*), soprattutto rispetto a quella pratica, palesemente in mala fede, consistente nel proporre all'utente micro-transazioni nei momenti decisivi del gioco. In particolare, negli Orientamenti, la Commissione ricorda che, nel caso dei giochi, a norma degli articoli 8 e 9 della direttiva 2005/29/CE (**pratiche commerciali aggressive**) i professionisti non devono sfruttare i pregiudizi comportamentali né introdurre elementi manipolativi relativi, ad esempio, alla tempistica delle offerte all'interno del gioco (offrendo ad es., come detto, microtransazioni nei momenti critici del gioco) o all'uso di effetti visivi e acustici per esercitare un'indebita pressione sul giocatore.

Quanto alle **pratiche di inserimento di prodotti da parte degli influencer marketing**, esse sono considerate nella lettera h) del punto 69 tra gli esempi di comunicazioni commerciali dissimulate che devono ritenersi vietate, insieme alle vetrine di prodotti e ad altre forme di promozione velata che possono ingannare o manipolare i minori inducendoli ad acquistare prodotti o servizi. Inoltre, nel punto 36 degli Orientamenti, si dice che le parti dei servizi dei social media con contenuti, sezioni o funzioni che possono rappresentare un rischio per i minori, come le sezioni per adulti di un social

media, o quelle che contengono comunicazioni commerciali o posizionamenti di prodotti per adulti da parte di influencer dovrebbero essere rese disponibili solo agli utenti adulti la cui età sia stata adeguatamente verificata.

Si tratta di divieti volti ad impedire che i minorenni siano esposti alle sollecitazioni degli influencer che, per finalità commerciali, presentano certi stili di vita come ideali creando strumentalmente uno standard di perfezione, con modalità idonee a generare un'ansia da raggiungimento ed effetti di perdita dell'autostima e di sviamento d'identità.

Nel medesimo punto (punto 69, lett. *h*)), gli Orientamenti impongono più generalmente alle piattaforme di garantire che i minori non siano esposti a pubblicità occulta o dissimulata, sia essa effettuata dal fornitore della piattaforma online o dagli utenti del servizio, ricordando che i fornitori di piattaforme online sono tenuti, a norma dell'articolo 26(2) DSA a mettere a disposizione dei destinatari del servizio una funzionalità che consente di dichiarare se i contenuti che forniscono siano o contengano comunicazioni commerciali.

Particolarmente significativa è la misura che impone alle piattaforme **di garantire che i minori non siano esposti a sistemi di IA integrati nella piattaforma che li influenzano o li incentivano a scopi commerciali, in particolare attraverso formati di conversazione o di consulenza quali i chatbot** (punto 69, lett. *e*)).

Inoltre, si prescrive alle piattaforme: di garantire che non venga sfruttata la mancanza di esperienza dei minori in ambito commerciale, tenendo conto della loro età, delle loro vulnerabilità e della loro limitata capacità di interagire in modo critico con le pratiche commerciali sulla piattaforma, fornendo loro un sostegno adeguato (punto 69, lett. *a*)); di garantire che i minori non siano esposti a pubblicità dannose, non etiche e illecite, valutando la loro adeguatezza relativamente alle loro varie fasce d'età (punto 69, lett. *b*)); di riesaminare periodicamente le misure di protezione pertinenti in consultazione con i minori, i tutori e altri portatori di interessi (punto 69, lett. *c*)); di garantire che i minori non siano esposti a una frequenza, a raccomandazioni e a volumi totali eccessivi di contenuti commerciali (punto 69, lett. *d*)); di garantire che le dichiarazioni sulla natura commerciale della comunicazione commerciale siano chiaramente visibili, a misura di minore, adeguate all'età e accessibili, come dettagliato anche nella sezione 8.4 degli Orientamenti dedicata alla trasparenza (punto 69, lett. *f*)); garantire che i minori non siano esposti alla commercializzazione e alla comunicazione di prodotti o servizi che possono avere un impatto negativo sulla loro vita privata e sulla loro sicurezza e protezione, come dettagliato anche nella sezione 5 degli Orientamenti dedicata all'analisi dei rischi (punto 69, lett. *g*)); di garantire che i minori non siano esposti a pratiche che possono portare a spese eccessive o indesiderate o a un uso eccessivo della piattaforma o a comportamenti compulsivi o che creano dipendenza, in particolare evitando di esporre i minori a oggetti virtuali quali scatole premio a pagamento, laddove offrano risultati casuali o imprevedibili o funzioni assimilabili al gioco d'azzardo, e introducendo una separazione o un punto di attrito tra i contenuti e l'acquisto di prodotti correlati (punto 69, lett. *k*)); di garantire che

i minori non siano esposti a tecniche di progettazione manipolative, quali la scarsità o premi intermittenti o casuali (punto 69, lett. l));

di considerare la possibilità di implementare strumenti efficaci per i tutori per controllare gli acquisti online, o di sottoporre qualsiasi impegno finanziario assunto da minori al di sotto di una certa età al riesame o al consenso dei tutori (punto 69, lett. m)); di rivedere la politica della piattaforma in relazione all'offerta di transazioni economiche, sulla base delle capacità in evoluzione dei minori, considerando che alcune fasce di età non dovrebbero essere esposte a transazioni economiche né essere autorizzate a effettuarle, in quanto non possiedono ancora la capacità di comprendere i concetti di spesa e denaro (punto 69, lett. n)).

Tecniche di intervento sui contenuti online illegittimi: orientamenti sulla moderazione dei contenuti. Nel contesto di un'articolata normativa, anche nazionale, che avversa i contenuti illeciti (v. contro il cyberbullismo, le leggi n. 71/2017, n. 70/2024 e d. lgs. n. 99/2025) gli Orientamenti prevedono un meccanismo di moderazione finalizzato a ridurre l'esposizione dei minori a contenuti e comportamenti dannosi per la loro privacy e sicurezza, che si avvale, tra l'altro, delle indicazioni contenute nell'[edizione rivisitata](#), pubblicata nel gennaio 2025 del codice di condotta per contrastare l'incitamento all'odio illegale online. Tale codice è stato valutato positivamente dalla Commissione e dall' EBDS ai sensi dell'art. 45(4) DSA; è rafforzativo del precedente codice del 2016 e ha individuato «impegni volontari volti a creare un quadro che faciliti il rispetto e l'efficace applicazione del DSA nel settore specifico dei contenuti illegali che incitano all'odio illegale, comprese nuove misure per affrontare le sfide e le minacce più recenti» (lett. f). Tra questi impegni spicca l'attività di monitoraggio che mira a valutare le prestazioni dei firmatari del codice nel contrasto ai contenuti di odio illegale (cfr. All. 1 al codice sulla «metodologia per le attività di monitoraggio» che codifica l'attività di monitoraggio da parte di soggetti qualificati iscritti in un apposito elenco).

Tornando agli Orientamenti, si prevede che i fornitori debbano, tra l'altro, stabilire procedure di moderazione, tenendo conto anche delle vulnerabilità specifiche del caso concreto. Inoltre, si impone al fornitore: a) di predisporre soluzioni tecniche efficaci per contrastare pratiche che potrebbero essere – non lo sono di per sé – illegali quali l'*hash matching* (confronto di dati sensibili, decriptazione di password e altro); b) di impedire *prompt* che il fornitore stesso abbia identificato come dannosi; di condividere i dati relativi alla moderazione dei contenuti.

Oltre al sistema di moderazione, i fornitori di piattaforme online devono istituire: 1) un meccanismo di segnalazione ai sensi dell'art. 16 DSA; 2) un sistema interno di trattamento dei reclami ai sensi dell'art. 20 DSA (se il minore se ne avvale, egli deve avere conferma della ricezione del reclamo); 3) una procedura di risoluzione stragiudiziale delle controversie ai sensi dell'art. 21 DSA; 4) misure di assistenza agli utenti. Queste ultime sono particolarmente significative in quanto assicurano un intervento protettivo immediato, onde evitare un danno maggiore. Si possono ad esempio prevedere collegamenti alle linee telefoniche di assistenza nazionali

competenti e fare in modo che i minori siano in grado di bloccare o silenziare qualsiasi utente o account o limitare i commenti altrui.

I fornitori devono altresì mettere a disposizione dei genitori o del tutore strumenti di controllo della piattaforma e dell'attività del minore [(ad es.: consentire la gestione delle impostazioni predefinite e l'impostazione di limiti di tempo), sul punto cfr. anche art. 13 d.l. n. 123/2023 conv. in l. n. 159/2023 cit.].

Governance della piattaforma online. In attuazione del DSA, gli Orientamenti impongono ai fornitori di assegnare a una persona o a un team dedicato la responsabilità di garantire privacy, sicurezza e protezione dei minori.

Accanto a questa misura strutturale, gli Orientamenti impongono ai fornitori, *inter alia*, le seguenti azioni: a) promuovere una cultura della partecipazione dei minori nella progettazione e nel funzionamento della piattaforma, prevedendo feedback da parte del fornitore per spiegare agli stessi minori come sono state prese in considerazione le loro opinioni; b) sensibilizzare l'opinione pubblica su *come il fornitore intenda difendere i diritti dei bambini* e sui *rischi* che i più giovani possono correre nelle loro attività sulla piattaforma con riguardo alla loro privacy e sicurezza; c) predisporre procedure per garantire il monitoraggio del rispetto dell'art. 28(1), DSA, le quali devono comprendere la raccolta e la registrazione dei dati relativi ai danni e ai rischi connessi alla privacy, sicurezza e protezione dei minori, al fine di poterli comunicare alla direzione del fornitore e alla persona o al team designato per la protezione dei minori stessi.

Termini e condizioni (buone pratiche) e trasparenza. Gli Orientamenti si soffermano particolarmente su questi due aspetti, legati tra loro, richiamando anzitutto l'art. 14 DSA dedicato proprio ai termini e alle condizioni generali di contratto, cui si aggiunge il dovere di trasparenza di quanto comunicato.

Com'è noto, mentre il paragrafo 1 dell'art. 14 DSA si appunta sul dovere dei prestatori di servizi intermediari di indicare le politiche e le tecniche di moderazione dei contenuti, di informare sul processo decisionale algoritmico e sulla verifica umana – l'intervento umano è uno dei principi fondamentali di governo dei sistemi di IA (v. anche art. 3(3) l. n. 132/2025 e art. 14 AI Act) – il paragrafo 3 stabilisce che «se un servizio intermediario è principalmente destinato a minori o è utilizzato in prevalenza da questi, il prestatore di tale servizio intermediario spiega in modo comprensibile per i minori le *condizioni* e le *restrizioni* che si applicano all'utilizzo del servizio». Condizioni e restrizioni del servizio devono, quindi, essere ben chiare al minore.

Le condizioni generali, da redigere «in un linguaggio chiaro, semplice, comprensibile, facilmente fruibile e privo di ambiguità» e da rendere disponibili «in un formato accessibile e leggibile meccanicamente» (art. 14(1) DSA), pongono le regole di accesso, spiegano il funzionamento della piattaforma, le sue finalità e le restrizioni, ossia ciò che non è consentito nella navigazione. Gli Orientamenti si concentrano in particolare sulle restrizioni d'uso, invitando i fornitori ad esplicitarle con accuratezza e altresì a spiegare come i minori saranno protetti dai contenuti illegali (ad esempio attraverso la moderazione).

Ebbene c'è un aspetto da tener presente, segnalato diffusamente nella letteratura specialistica: vi è una scarsissima propensione alla lettura delle condizioni generali di contratto. Chi vuole utilizzare una piattaforma per i contenuti e le possibilità da questa offerte, valuta solo l'aspetto del proprio interesse da realizzare nell'immediato. Se la piattaforma consente l'accesso a un determinato gioco (magari quello tra i più diffusi), se agevola i compiti scolastici o permette una certa esperienza, il minore che ne ravvisa l'utilità, anche in termini di riduzione del proprio impegno, tenderà ad attivarla subito, senza la lettura preventiva delle condizioni generali di utilizzo.

Senza nulla togliere all'importanza del principio di trasparenza, sul quale gli Orientamenti si soffermano attraverso il richiamo degli artt. 15 («obblighi in materia di relazioni di trasparenza per i prestatori di servizi intermediari») e 24 DSA («obblighi di comunicazione trasparente per i fornitori di piattaforme online») – i quali articoli indicano un complesso articolato di informazioni da fornire all'utilizzatore – ad esso deve affiancarsi un funzionamento virtuoso, eticamente orientato, della piattaforma stessa. In che senso? Gli Orientamenti valorizzano le buone pratiche. Si riporta, ad esempio, la soluzione adottata dalla piattaforma *HappyExplore*, in cui i minori giocano, creano ed esplorano creature e mondi di vario tipo che possono condividere tra loro. Qui gli utenti sono incoraggiati a sottoscrivere un *Kindness pledge* (un impegno alla gentilezza), utile per richiamare, con immediatezza e senza lo sforzo della lettura, il valore della correttezza e della continenza espositiva. Nella piattaforma opera un personaggio, *Pixel Pioneer*, che interagisce con gli utenti e spiega loro perché dovrebbero riflettere attentamente prima di condividere le loro creature e i loro mondi.

ANTONIO GORGONI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C_202505519

2025/4(17)BCo

Le attività conoscitive avviate dalla Commissione europea nell'ottobre 2025 nei confronti di Snapchat, YouTube, Apple e Google sulle misure di salvaguardia dei minori ai sensi del Digital Services Act

Con comunicato stampa del 10.10.2025, la Commissione europea (la **Commissione**) ha annunciato di aver avviato delle attività conoscitive nei confronti di Snapchat, YouTube, Apple e Google, al fine di valutare il rispetto degli obblighi di protezione a favore dei minori imposti dal regolamento (UE) 2022/2065 (Digital Services Act, **DSA**).

Il DSA com'è noto, mira a garantire uno spazio digitale sicuro e rispettoso dei diritti fondamentali attraverso una forte responsabilizzazione delle piattaforme, rafforzando gli oneri di queste ultime, specialmente delle Very Large Online Platforms (**VLOPs**), nel contrasto a contenuti illeciti e discriminatori, con una particolare attenzione alla tutela dei minori.

L'iniziativa segue la realizzazione del "DSA Transparency Database" (su cui v. in questa rubrica la notizia n. 11 del numero 4/2023 [2023/4(11)SO-SM] in *PeM* 2023, p. 770, e in *Atlante*, p. 438), attraverso il quale le piattaforme sono tenute a rendicontare l'attività di moderazione dei contenuti svolta, e, più di recente, l'adozione nel luglio 2025 degli orientamenti sulla protezione dei minori (su cui v. *supra* il contributo precedente in questo numero di questa rubrica, [2025/4(16)AG]) (gli **Orientamenti**), previsti dall'art. 28 DSA al fine di assistere le piattaforme nell'attuazione di misure appropriate e proporzionate per garantire un elevato livello di tutela della vita privata, sicurezza e protezione dei minori nell'ambito dei loro servizi. Gli Orientamenti confermano, inter alia, la necessità che, al fine di evitare l'accessibilità di certi siti ai minori, il fornitore di una piattaforma online non si possa limitare a una dichiarazione formale contenuta nelle condizioni generali, ma debba attuare misure concrete per impedire effettivamente ai minori di accedere al suo servizio. Riconoscendo l'eterogeneità delle piattaforme e la pluralità di misure adottabili, secondo le svariate esigenze che possono venire in gioco, la Commissione afferma la necessità che il fornitore vagli, tra l'altro: *i)* le probabilità che i minori accedano al suo servizio; *ii)* l'impatto effettivo o potenziale sulla protezione dei minori del servizio; *iii)* le misure già poste in essere per prevenire tali rischi; *iv)* le misure supplementari adottate sulla base di adeguatezza e proporzionalità e rispettose dei principi generali; dispone inoltre che il fornitore *a)* individui dei parametri per monitorare l'efficacia di tali misure; *b)* valuti i potenziali effetti positivi e negativi sui diritti dei minori o di altri utenti delle misure – anche di quelle supplementari se presenti – messe in atto. Tra le misure proposte vi è, per esempio, quella di impostare in maniera predefinita il profilo del minore come privato, rendendo inaccessibili le informazioni personali di quest'ultimo a coloro che non fanno parte della sua rete di contatti, ma anche l'impossibilità di acquisire screenshot di contenuti provenienti da minori per impedirne la circolazione e il rafforzamento delle misure di parental control.

Al fine di vagliare l'effettivo rispetto dei principi affermati, la Commissione ha quindi richiesto a **Snapchat, YouTube, Apple e Google** informazioni relative ai loro sistemi di verifica dell'età e, in particolare:

- a Snapchat di chiarire le modalità adottate per impedire ai minori di 13 anni di accedere ai suoi servizi e per inibire la vendita ai bambini di merci illegali;
- a Youtube approfondimenti relativi al suo sistema di assicurazione dell'età e a quello di raccomandazione conseguente alla segnalazione di contenuti dannosi diffusi ai minori;
- ad App Store e Google Play informazioni sulle modalità di gestione del rischio per gli utenti, soprattutto minori, di scaricare app illegali, o altrimenti dannose, e di applicazione delle classi di età per ogni applicazione del catalogo.

Per fare un esempio, un'informativa era stata recentemente richiesta nei confronti di **X** e aveva successivamente condotto la Commissione ad avviare una procedura formale di infrazione nei confronti della piattaforma per valutare - tra i vari profili - le misure di mitigazione adottate per contrastare la diffusione di contenuti illegali nell'Unione e, in particolare, per valutare se

vi fosse stata la manipolazione dell'informazione sulla piattaforma, con particolare riferimento ai c.d. dark patterns e alle spunte blu (blue checks), all'esito della quale il 5.12.2025 è stata disposta una multa di 120 milioni di euro a X per aver violato gli obblighi di trasparenza ai sensi del DSA (su questo provvedimento v. in questo numero di questa Rubrica il contributo n. 20 [2025/4(20)MVT]). Rimanendo al 2025 e alla protezione dei minori si può segnalare anche l'indagine aperta dalla Commissione (e annunciata con [comunicato stampa del 27 maggio 2025](#)) nei confronti delle piattaforme pornografiche **Pornhub**, **Stripchat**, **XNXX** e **XVideos**, individuando possibili violazioni in ragione della sospettata inefficacia delle misure di verifica dell'età adottate da tali siti. In generale si può ritenere che il tema dell'*age verification*, divenuto certamente una priorità politica nell'azione della Commissione, acquisirà sempre maggiore centralità nel tentativo di trovare un adeguato ma difficile bilanciamento tra la necessità di tutelare i minori e l'esigenza di evitare forme di sorveglianza di massa, con un approccio sempre più basato sulla proporzionalità tra il sistema dei controlli richiesti e i rischi previsti.

BRUNO CONCAS

<https://digital-strategy.ec.europa.eu/it/news/commission-scrutinises-safeguards-minors-snapchat-youtube-apple-app-store-and-google-play-under>

2025/4(18)RR

La seconda versione dell'*age verification blueprint* della Commissione europea del 10.10.2025

Il 10 ottobre 2025 la Commissione europea (la **Commissione**) ha pubblicato una [seconda versione del piano di verifica](#) dell'età (*age-verification blueprint*) la cui prima versione era stata pubblicata il 14 luglio dello stesso anno (la **Seconda versione**). La Seconda versione è volta all'ulteriore miglioramento delle soluzioni inizialmente adottate e ad aiutare le piattaforme online a implementare un metodo di verifica dell'età robusto, facile da usare e che preservi la *privacy* dei soggetti coinvolti. Ad una prima analisi, tra le migliorie della Seconda versione possono annoverarsi:

- i) metodi di *onboarding* ampliati
- ii) un metodo di presentazione della prova dell'età più *user-friendly* che sfrutta i moderni sistemi operativi e *browser* attraverso il supporto di *Digital Credentials API*
- iii) funzionalità *privacy* implementate
- iv) documentazione *family-friendly*.

Nello specifico, il piano della Commissione consiste in specifiche tecniche allineate a quelle dei [Digital Identity Wallets dell'UE](#) (i portafogli europei di identità digitale, definiti e previsti all'art. 3, n. 42 e al capo II, sezione 1, del regolamento UE n. 910/2014 – regolamento **eIDAS** - come modificato dal regolamento (UE) 2024/1183 – regolamento **EUDI**) e in un'implementazione

open source di queste nei termini di un app mobile personalizzabile nei diversi contesti nazionali, sia come app autonoma che integrata, come funzionalità di verifica dell'età, nei portafogli di identità digitali. È opportuno evidenziare, tuttavia, come gli operatori di mercato possono anche adottare una soluzione *software open source* e gratuita e svilupparla ulteriormente.

L'app di verifica dell'età è indirizzata a proteggere i minori dall'esposizione a contenuti online inappropriati e potenzialmente dannosi per la loro fascia d'età. Permette agli utenti maggiorenni di dimostrare facilmente la loro età per accedere a contenuti adulti riservati senza rivelare alcuna informazione personale, nemmeno la loro età esatta, la quale verrà comunque desunta nel corso del procedimento di verifica della stessa.

La soluzione di verifica dell'età è progettata per rispettare i più alti *standard* di *privacy*, impedendo, ad esempio, il tracciamento dell'identità dell'utente. Quest'ultima viene controllata solo una volta durante il rilascio della prova dell'età. In sostanza, il piano di verifica dell'età supporta l'efficace attuazione delle disposizioni per proteggere i minori online del reg. (UE) 2022/868 (Digital Services Act, **DSA**) e soddisfa i requisiti di una soluzione robusta e che preservi la *privacy* per la verifica dell'età stabilita nelle [linee guida DSA sulla protezione dei minori](#) del 14.7.2025 (sulle quali v. *supra* in questo numero di questa Rubrica il contributo n. 16 [2025/4(16)AG]). L'intero sistema fornirà un esempio di conformità e uno *standard* di riferimento per un metodo di verifica dell'età basato su un dispositivo. È opportuno evidenziare come, sebbene le funzionalità che preservano la *privacy* non possano essere modificate, gli Stati membri potranno personalizzare la soluzione di verifica dell'età in base alle loro esigenze nazionali, inclusi, ad esempio, il *branding* e la traduzione nella lingua nazionale.

La Seconda versione ha previsto una soluzione adatta alle famiglie nel rispetto delle sopra citate linee guida DSA sulla protezione dei minori. La Seconda versione consente l'uso di passaporti e carte d'identità come metodi di *onboarding*, oltre agli eID, per generare una prova dell'età. Inoltre, introduce il supporto per un metodo di presentazione delle prove più facile da usare, le *Digital Credentials API* (interfacce di programmazione per credenziali digitali), sempre più disponibili nei sistemi operativi e nei *browser* moderni.

Il piano è ora in fase di diversi test sperimentali ad opera degli Stati membri, delle piattaforme online, degli utenti finali e degli altri *stakeholder*. Nel comunicato stampa della Commissione del 10.10.2025, si dice che Danimarca, Francia, Grecia, Italia e Spagna sono stati primi Stati membri a sperimentare la soluzione tecnica prestabilita dal provvedimento europeo con l'intento di adattarla ai loro contesti nazionali. Questo avviene integrando una funzionalità compatibile di verifica dell'età nei loro portafogli digitali nazionali o predisponendo una app personalizzata per la verifica dell'età per la pubblicazione negli *store* digitali. Nel medesimo comunicato stampa del 10.10.2025, la Commissione ha previsto che le prime app personalizzate dovrebbero essere rilasciate all'inizio del 2026. Il modello di verifica dell'età può essere facilmente personalizzato dagli editori delle applicazioni, senza la possibilità, tuttavia, di modificare le funzionalità di protezione della *privacy*. Parallelamente, si stanno svolgendo test pilota con piattaforme online, inclusi

fornitori di contenuti per adulti, e quelle tra esse che non sono ancora state coinvolte sono però state invitate a partecipare al progetto pilota e alla fase di test. Anche gli esami per l'utente finale sono iniziati e stanno venendo ulteriormente ampliati con il supporto dei Centri Internet più Sicuri dell'UE. Durante il *Safer Internet Forum* (SIF) del 4 dicembre 2025, gli utenti finali hanno avuto, peraltro, l'opportunità di testare l'app di verifica dell'età e fornire il loro *feedback*.

La Commissione offre un supporto agli Stati membri per implementare il piano nelle loro soluzioni nazionali di verifica dell'età mediante un coordinamento con le autorità nazionali e i Coordinatori dei Servizi Digitali. Per concludere, si può affermare che il piano di verifica dell'età getta le basi per un futuro ampliamento di servizi adeguati all'età. Questo, infatti, è anche chiamato '*mini-wallet*' (ovvero 'mini-portafoglio'), poiché è costruito sulle stesse specifiche tecniche dei prossimi *European Digital Identity Wallets* (i portafogli europei di identità digitale previsti dal regolamento eIDAS, come modificato dal regolamento EUDI), garantendo la compatibilità a lungo termine, consentendo l'integrazione della funzionalità di verifica dell'età nei futuri portafogli e fornendo un trampolino di lancio dei *European Digital Identity Wallets* entro la fine del 2026.

RACHELE RANIERI

<https://digital-strategy.ec.europa.eu/en/news/commission-releases-enhanced-second-version-age-verification-blueprint#:~:text=To%20help%20online%20platforms%20implement,solution%20and%20further%20develop%20it>

2025/4(19)RMo

La bozza di raccomandazione delle clausole contrattuali tipo non vincolanti relative all'accesso ai dati e al relativo utilizzo e delle clausole contrattuali standard non vincolanti per i contratti di cloud computing elaborate dalla Commissione europea ai sensi dell'art. 41 del Data Act (Comunicazione C(2025) 7750 final del 19.11.2025)

Al fine di favorire l'accesso equo ai dati e il loro utilizzo, nonché la creazione di un mercato maggiormente competitivo per i servizi di trattamento dei dati, il regolamento (UE) 2023/2854 (**Data Act**) ha istituito, nei Capi da I a III, un quadro armonizzato volto a individuare i soggetti legittimati a utilizzare i dati generati dall'uso di un prodotto o di un servizio correlato, nonché le condizioni in base alle quali ciò può avvenire. Il Data Act si avvale, a tal fine, di contratti-tipo, con l'obiettivo è di creare certezza giuridica in ordine ai diritti e agli obblighi delle parti, promuovere la condivisione dei dati e assicurare un'equa distribuzione dei benefici lungo l'intera catena del valore dei dati.

Il Data Act stabilisce regole concernenti il diritto dei clienti di servizi di trattamento dei dati a migrare da un fornitore di tali servizi a un altro fornitore o a un'infrastruttura interna (*on-premises*), prevedendo condizioni e

procedure specifiche che garantiscano, tra l'altro, la sicurezza e la continuità operativa nel corso del processo di migrazione. La capacità dei clienti di migrare da un fornitore di servizi di trattamento dei dati a un altro, o di utilizzare simultaneamente i servizi di più fornitori, rappresenta una condizione imprescindibile per un mercato più competitivo e con minori barriere all'ingresso per nuovi operatori.

Il Data Act introduce un obbligo per i fornitori di trattamento dei dati di rimuovere gli ostacoli che possano impedire ai clienti di esercitare il diritto alla migrazione. I diritti e gli obblighi dei clienti e dei fornitori di servizi di elaborazione in relazione alla migrazione da un fornitore di tali servizi a un altro o, se del caso, a un'infrastruttura interna debbono essere definiti in modo chiaro in un contratto scritto (art. 25 Data Act). Il Data Act impone che tutte le parti coinvolte nella migrazione cooperino in buona fede per rendere efficace il processo di migrazione, al fine di consentire il trasferimento tempestivo dei dati e mantenere la continuità del servizio di trattamento dei dati (art. 27 Data Act).

Ai sensi dell'articolo 41 del Data Act, la Commissione europea è incaricata di elaborare e raccomandare condizioni contrattuali tipo non vincolanti sull'accesso e l'utilizzo dei dati, nonché clausole contrattuali standard non vincolanti per i contratti di servizi di trattamento dei dati, allo scopo di agevolare le parti nella conclusione di tali contratti.

Il 19 novembre 2025 la Commissione ha pubblicato un *draft Commission Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts* ([C\(2025\) 7750 final](#)), d'ora in poi "**draft Commission Recommendation**", che include una serie di Allegati contenenti: i) *model contractual terms* per i contratti relativi all'accesso e all'utilizzo dei dati (MCTs) e ii) *standard contractual clauses* per i contratti di servizi di trattamento dei dati (SCCs), quali strumenti di supporto per le parti nella negoziazione e conclusione dei rispettivi accordi. La raccomandazione sarà formalmente adottata dalla Commissione solo in un momento successivo, una volta disponibili le versioni nelle varie lingue.

Il Data Act introduce, inoltre, al Capo IV, un controllo sulle clausole contrattuali abusive riguardanti l'accesso e l'utilizzo dei dati, quando tali clausole siano imposte unilateralmente in contratti conclusi tra imprese. Questa forma di controllo concerne, tra l'altro, le clausole relative alla responsabilità della parte che ha imposto unilateralmente la clausola, nonché clausole che limitino i rimedi a disposizione della parte cui la clausola è imposta. I MCTs e le SCCs sono stati elaborati anche alla luce di tale disposizione.

I MCTs, contenuti negli Allegati II-V del *draft Commission Recommendation*, sono stati elaborati per assistere le parti nella redazione e negoziazione di contratti relativi all'accesso e all'utilizzo di dati (personali e non personali). Si mira a far sì che tali contratti stabiliscano diritti e obblighi contrattuali equi, ragionevoli e non discriminatori, prevedano un compenso adeguato e tutelino i segreti commerciali. I MCTs tengono conto, innanzitutto, dei tre tipi di rapporti contrattuali contemplati dalle previsioni del Data Act. Pertanto la *draft Commission Recommendation* distingue tra:

- i) MCTs dell'Allegato II destinati ai contratti tra un titolare dei dati e un utente di un prodotto connesso o di un servizio correlato, quando il titolare dei dati desidera utilizzare i dati generati tramite l'uso di tale prodotto o servizio ai sensi dell'art. 4 Data Act.
- ii) MCTs dell'Allegato III destinati ai contratti di cui all'art. 6 del Data Act intercorsi tra un utente di un prodotto connesso o servizio correlato e un terzo destinatario dei dati, quando l'utente richiede al titolare dei dati di rendere disponibili i dati al destinatario ai sensi dell'art. 5 del Data Act.
- iii) MCTs dell'Allegato IV destinati ai contratti tra un titolare dei dati e un terzo destinatario dei dati (art. 8 e 9 Data Act), qualora il titolare dei dati sia obbligato (ai sensi dell'art. 5 del Data Act) a rendere disponibili i dati su richiesta dell'utente. Essi possono essere utilizzati, con gli opportuni adattamenti, anche laddove l'obbligo di condivisione dei dati discenda da altre disposizioni del diritto dell'Unione o da normative nazionali adottate in conformità al diritto dell'Unione.

Invece, i MCTs dell'Allegato V riguardano i contratti tra un *data sharer* e un destinatario dei dati, quando il primo desidera mettere i dati a disposizione del destinatario su base volontaria, indipendentemente da richieste dell'utente o di altri soggetti. Il termine *data sharer* è stato scelto per riflettere la pluralità degli scenari possibili.

L'utilizzo di MCTs da parte dei contraenti non incide sui diritti e sugli obblighi loro spettanti ai sensi del Data Act o di altre normative dell'Unione o nazionali adottate conformemente al diritto dell'Unione, inclusi gli obblighi del titolare del trattamento e i diritti degli interessati ai sensi del Regolamento (UE) 2016/679 (d'ora in poi "GDPR"), nonché le norme in materia di concorrenza. Particolare attenzione deve essere prestata ai casi in cui la condivisione riguardi dati personali o insiemi di dati misti. In simili casi, i titolari dei dati sono tenuti a mettere a disposizione dati personali ai sensi del Data Act unicamente laddove esista una base giuridica conforme al GDPR.

La *draft Commission Recommendation* dà poi attuazione alle disposizioni del Capo VI del Data Act (relativo alla migrazione nei servizi di trattamento dei dati) mediante la previsione di alcune SCCs non vincolanti, da inserire nei contratti di servizi di trattamento dei dati. In particolare, sono state previste: 1) clausole sulla migrazione da un fornitore di servizi di trattamento dei dati ad un altro fornitore o a un'infrastruttura locale (*SCC on Switching & Exit*); 2) clausole sullo scioglimento del contratto di servizi di trattamento dei dati (*SCC on Termination*); e 3) clausole sulla sicurezza e sulla continuità operativa durante la migrazione, incluse le notifiche degli incidenti significativi da parte del fornitore (*SCC on Security & Business Continuity*). Ulteriori tre SCCs sono state predisposte al fine di promuovere equità, ragionevolezza e non discriminazione dei diritti e degli obblighi contrattuali, così da impedire squilibri idonei a compromettere l'effettività delle tutele previste dal Capo VI del Data Act. Si tratta, in particolare, di: 1) clausole per assicurare un ambiente contrattuale trasparente (*SCC on Non-Dispersion*); 2) clausole per evitare modifiche unilaterali ingiustificate (*SCC on Non-Amendment*); infine 3) clausole per garantire una ripartizione equilibrata della

responsabilità, evitando limitazioni ingiustificate in favore del fornitore di servizi di trattamento dei dati (*SCC on Liability*).

Le SCCs sono rivolte a tutti i clienti e fornitori di servizi di trattamento dei dati rientranti nell'ambito di applicazione del Data Act, indipendentemente dalla natura pubblica o privata del soggetto, o dalla sua dimensione.

Le SCCs del Data Act non contemplano gli adempimenti previsti dal GDPR. Le clausole necessarie per assicurare la conformità al GDPR dei contratti di servizi di trattamento dei dati devono essere inserite nel contratto. La Commissione ha già adottato il 21 giugno 2021 clausole contrattuali tipo per i titolari e responsabili del trattamento (https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en), sia ai fini della conformità al GDPR, sia per il trasferimento di dati personali verso Paesi terzi. Tali clausole non possono essere modificate dalle parti e possono essere incluse in un contratto più ampio o utilizzate come accordo autonomo.

ROBERTA MONTINARO

<https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding>

2025/4(20)MVT

La sanzione di 120 milioni di euro comminata della Commissione europea a X il 5.12.2025 per violazione del Digital Services Act

Il 5 dicembre 2025 la Commissione europea (la **Commissione**) ha irrogato una sanzione di 120 milioni di euro alla piattaforma X per la violazione di una serie di obblighi di trasparenza imposti dal [regolamento \(UE\) 2022/2065](#) (Digital Services Act, **DSA**).

La decisione ha avuto ad oggetto l'accertamento di violazioni dell'art. 25(1) DSA, che riguarda tutte le piattaforme, e degli articoli 39 e 40 DSA che riguardano solo le 'piattaforme online di dimensioni molto grandi' (**VLOPs**) e i 'motori di ricerca online di dimensioni molto grandi' (**VLOSEs**), applicabili alla piattaforma X (già chiamata Twitter) per essere essa stata designata come VLOP ai sensi del DSA in data 25.4.2023 (sulla designazione v. in questa Rubrica notizia n. 5 del [numero 2/2023](#) [2023/2(5)RA] in *PeM* 2023, p. 381 e in *Atlante*, p. 348).

La sanzione è stata comminata all'esito di un'istruttoria avviata dalla Commissione il 18 dicembre 2023 sia con riferimento alla diffusione di contenuti illegali, sia all'efficacia delle misure adottate per combattere la manipolazione delle informazioni. Al vaglio della Commissione sono stati sottoposti, altresì, l'uso di design e modelli ingannevoli, la mancanza di trasparenza pubblicitaria e l'accesso insufficiente ai dati per i ricercatori. In relazione a questi ultimi, dall'analisi dei documenti interni della società, dai colloqui con esperti e in seguito alla cooperazione con i Coordinatori dei Servizi Digitali Nazionali (**CSD**), la Commissione europea il 12 luglio 2024 ha formulato alcune constatazioni preliminari di non conformità della



piattaforma X al DSA in materia di *dark patterns*, trasparenza della pubblicità e accesso ai dati.

Dall'attività di indagine è emerso un primo elemento di non conformità al Regolamento, individuato nell'uso della cosiddetta «**spunta blu**», associata alla verifica dell'identità degli utenti e finalizzata a garantire l'identità del gestore, quale utente «verificato».

Si tratta di un sistema che, secondo la Commissione, inganna l'utente poiché la concessione del contrassegno blu non è subordinata ad alcun controllo di autenticità ma può essere ottenuta dietro il **pagamento di un corrispettivo**. Ne consegue che chiunque si abboni al servizio possa ottenere lo status di «utente verificato» e ottenere la c.d. spunta blu. Sebbene nel DSA non sia previsto alcun obbligo generale di verifica dell'identità degli utenti, l'**art. 25(1) DSA** vieta espressamente alle piattaforme online di progettare, organizzare o gestire le interfacce online in modo tale da ingannare o manipolare i destinatari dei loro servizi, ovvero da compromettere la loro capacità di assumere decisioni libere e informate. Per questo motivo, secondo la Commissione, la comunicazione di «account verificato», in assenza di alcun controllo, costituisce una pratica ingannevole, incompatibile con gli obblighi di trasparenza e correttezza informativa, idonea a compromettere la percezione dell'affidabilità dei profili e ostacolare la distinzione tra profili autentici e potenziali falsificazioni.

Un ulteriore profilo contestato alla piattaforma X concerne l'archivio pubblicitario e il mancato rispetto dell'obbligo di trasparenza imposto dal DSA. Ai sensi dell'**art. 39 DSA**, le piattaforme sono tenute a garantire un accesso agevole agli archivi contenenti informazioni complete sugli annunci pubblicitari, incluso il contenuto della comunicazione, il nome del prodotto, del servizio o del marchio pubblicizzato, l'oggetto della pubblicità, la persona fisica o giuridica per conto della quale viene presentata la pubblicità, ivi compreso il soggetto che l'ha finanziata, la finalità dell'annuncio, il periodo di presentazione della pubblicità e ogni informazione rilevante ad individuare i suoi destinatari. Le verifiche condotte dalla Commissione europea hanno evidenziato la **presenza di barriere tecniche, ritardi nell'accesso e lacune informative che ostacolano il monitoraggio delle attività pubblicitarie di X**, reputandolo un modello idoneo a compromettere la possibilità per i ricercatori e la società civile di accedere ai repertori di annunci e individuare fenomeni come truffe online, campagne di minacce ibride, operazioni coordinate di disinformazione e pubblicità ingannevole.

Il terzo elemento che la Commissione europea ha ritenuto non conforme al Regolamento riguarda la violazione dell'**art. 40 DSA** relativo all'accesso ai ricercatori ai dati pubblici della piattaforma. In particolare, si è osservato che **i termini di servizio di X impediscono ai ricercatori qualificati di accedere autonomamente ai dati pubblicamente disponibili**. Le procedure predisposte per l'accesso sono sproporzionate e tali da compromettere in modo significativo la possibilità di condurre ricerche indipendenti anche sui rischi sistemici derivanti dal funzionamento della piattaforma. Il processo elaborato dalla piattaforma X per concedere ai ricercatori di accedere alla sua interfaccia per programmi applicativi (API) dissuade i ricercatori dallo svolgimento di progetti di ricerca. Si tratta di limitazioni che impediscono alla

comunità scientifica di analizzare fenomeni come la diffusione di contenuti illegali, la disinformazione e la manipolazione del dibattito pubblico.

All'esito delle indagini preliminari, la Commissione europea ha concesso un termine ad X per analizzare i documenti di indagine e fornire un riscontro scritto alle conclusioni preliminari raggiunte dalla Commissione, avviando, parallelamente, la consultazione del Comitato europeo per i servizi digitali.

Il 5 dicembre 2025 la Commissione ha adottato la sua decisione. Ritenute confermate le osservazioni preliminari, in ragione di tutte le violazioni accertate, della gravità delle stesse e della potenziale platea di utenti raggiungibili nel territorio dell'Unione, la Commissione ha irrogato una sanzione di 120 milioni di euro **per la violazione degli obblighi di trasparenza, inclusa la progettazione ingannevole del «segno di spunta blu», la mancanza di trasparenza dell'archivio pubblicitario e i limiti imposti ai ricercatori per l'accesso ai dati pubblici.**

La decisione assume particolare rilievo, non solo per l'elevata entità della sanzione irrogata, ma anche per il suo valore di precedente applicativo del nuovo regime normativo europeo. Oltre alla sanzione pecuniaria, la piattaforma è stata sottoposta all'obbligo di comunicare, entro 60 giorni lavorativi dall'adozione del provvedimento, le misure adottate per porre fine alla violazione dell'art. 25(1) DSA, relativa all'uso del contrassegno blu. Entro 90 giorni lavorativi, X dovrà presentare un piano di azione per sanare le irregolarità concernenti la trasparenza dell'archivio e l'accesso dei ricercatori ai dati pubblici della piattaforma. Entro un mese dalla ricezione di tale piano, la Commissione adotterà la decisione finale. Il mancato adempimento di tali obblighi potrà comportare l'irrogazione di ulteriori sanzioni.

La decisione assunta dalla Commissione europea costituisce la prima applicazione formale del meccanismo sanzionatorio previsto dal Digital Services Act nei confronti di una piattaforma di dimensioni molto grandi e contribuisce a delineare i confini degli obblighi di cooperazione con la ricerca.

MARIA VITTORIA TRINCHERA

https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934

2025/4(21)GV

I preliminary findings della Commissione europea del 24.10.2025 sulla violazione dei doveri di trasparenza ai sensi del Digital Services Act da parte di TikTok e Meta e l'accettazione da parte della Commissione europea in data 5.12.2025 degli impegni assunti da TikTok in materia di trasparenza della pubblicità ai sensi del medesimo regolamento

Il 24 ottobre 2025 la Commissione europea (la **Commissione**) ha raggiunto alcuni risultati preliminari nell'ambito dei procedimenti formali avviati dalla stessa il 19 febbraio 2024 e il 30 aprile 2024, nei confronti rispettivamente di TikTok e Meta (quest'ultimo come fornitore di Facebook e Instagram), ai

sensi del reg. (UE) 2022/2065 (Digital Services Act, **DSA**). Com'è noto, l'art. 66 DSA attribuisce alla Commissione il potere di avviare un procedimento, in vista della possibile adozione di provvedimenti sanzionatori, in relazione alla condotta di piattaforme online di dimensioni molto grandi (**VLOPs**) o di motori di ricerca online di dimensioni molto grandi (**VLOSEs**), di cui si sospetti la violazione di una o più disposizioni del DSA. TikTok, Facebook e Instagram sono stati designati dalla Commissione europea, il 25 aprile 2023, come piattaforme online di dimensioni molto grandi (sulla designazione v. in questa Rubrica notizia n. 5 del [numero 2/2023](#) [2023/2(5)RA] in *PeM* 2023, p. 381 e in *Atlante*, p. 348).

I *preliminary findings* di cui ci si occupa in questa sede riguardano solo alcune delle violazioni contestate alle suddette piattaforme nei procedimenti formali di indagine sopra richiamati. Invero, un'altra violazione notificata a TikTok – relativamente alla mancanza delle dovute informazioni nell'archivio di annunci pubblicitari previsto dall'**art. 39 DSA** – è già stata constatata in via preliminare dalla Commissione il [15 maggio 2025](#).

In base alle nuove risultanze preliminari del mese di ottobre 2025, che coinvolgono sia la piattaforma cinese che le piattaforme statunitensi facenti capo a Meta in relazione alla presunta violazione dell'obbligo di rendere accessibili ai ricercatori i dati pubblici ai sensi dell'**art. 40(12) DSA**, la Commissione ritiene che l'accesso a tali dati non risulti agevole – come dovrebbe essere – a causa di procedure e strumenti onerosi che le piattaforme in questione potrebbero aver messo in atto. In particolare, i dati cui i ricercatori hanno accesso sono spesso parziali o inaffidabili. La difficoltà per i ricercatori di avere a disposizione i dati pubblici, in modo completo e attendibile, impedisce loro di verificare se gli utenti delle piattaforme, compresi i minori, siano esposti a contenuti illegali o dannosi. La Commissione sottolinea l'importanza di tale obbligo di trasparenza, in quanto è soprattutto grazie al lavoro dei ricercatori che può esercitarsi un controllo pubblico diffuso sul potenziale impatto delle piattaforme sulla nostra salute fisica e mentale. A riprova di ciò, dopo qualche giorno, il 29 ottobre 2025, la Commissione europea ha adottato il regolamento delegato (UE) 2025/2050, integrando l'art. 40(4) DSA con misure tecniche volte a garantire ai ricercatori abilitati l'accesso ai dati non pubblici delle piattaforme online di dimensioni molto grandi.

Vi sono, poi, alcuni risultati preliminari che riguardano solo Facebook e Instagram. Ad avviso della Commissione, entrambe le piattaforme di Meta non rispettano gli obblighi in merito ai meccanismi di segnalazione di contenuti illegali e ai mezzi di reclamo contro eventuali decisioni assunte dalle piattaforme, come la rimozione di contenuti o la sospensione degli *accounts*. In particolare, dovendo gli utenti compiere una serie di azioni prima di poter inviare una segnalazione, il meccanismo di cui all'**art. 16 DSA** non risulta di facile utilizzo, né facilmente accessibile per notificare contenuti – ad avviso degli utenti – illegali; in sostanza, la Commissione ravvisa l'esistenza di *dark patterns* nell'architettura dell'interfaccia online. Inoltre, per quanto riguarda il sistema interno di gestione dei reclami contro eventuali rimozioni di contenuti o sospensioni di *accounts* da parte dei fornitori dei servizi digitali, gli utenti non sembrano essere messi nelle condizioni di poter

fornire spiegazioni o prove a sostegno dei loro reclami. La Commissione è giunta a tali constatazioni preliminari anche grazie alla cooperazione con Coimisiún na Meán, coordinatore irlandese dei servizi digitali.

La Commissione conclude il comunicato stampa segnalando che, a seguito dei *preliminary findings* qui riassunti, TikTok, Facebook e Instagram possono rispondere per iscritto a tali risultanze, così come possono adottare misure per rimediare alle violazioni rilevate. Al contempo, la Commissione si prende carico di consultare il comitato europeo per i servizi digitali, previsto dall'art. 61 DSA, in vista della conclusione dell'indagine.

A proposito delle possibili iniziative che le piattaforme possono assumere per porre rimedio alle violazioni del DSA, merita segnalare che TikTok, dopo essere stato messo al corrente dei risultati preliminari del 15 maggio 2025 sopra citati, si è già impegnato con la Commissione – che ha accettato l'impegno il 5 dicembre 2025 – a fornire archivi pubblicitari che garantiscano la piena trasparenza in merito agli annunci sui suoi servizi. Tali impegni prevedono che TikTok: fornirà il contenuto completo dell'annuncio pubblicitario così come appare nei *feed* degli utenti, inclusi gli URL nel *link* fornito nell'annuncio; aggiornerà il suo archivio più rapidamente, assicurando che le informazioni siano disponibili entro un massimo di 24 ore; fornirà i criteri di *targeting* selezionati dagli inserzionisti, insieme ai dati aggregati degli utenti (tra cui sesso, fascia di età e Stato membro in cui si trovano gli utenti raggiunti), consentendo ai ricercatori di indagare su come gli annunci sono mirati e consegnati; introdurrà ulteriori opzioni di ricerca e filtri, consentendo agli utenti di trovare gli annunci pubblicitari più facilmente.

GIUSEPPE VERSACI

https://ec.europa.eu/commission/presscorner/detail/it/ip_25_2503

2025/4(22)VH

L'istruttoria annunciata il 4.12.2025 della Commissione europea per abuso di posizione dominante e il provvedimento cautelare dell'AGCM n. 31775 del 22.12.2025 aventi entrambi ad oggetto la nuova policy contrattuale di limitazione di accesso a WhatsApp applicata da Meta ai fornitori di IA

Il 4 dicembre 2025 la Commissione europea (la **Commissione**) ha [annunciato](#) di aver avviato un'indagine formale per valutare se le nuove condizioni contrattuali applicate da Meta dal 15 ottobre 2025, nell'ambito dei *Whatsapp Business Solution Terms* e relativamente alla fornitura di servizi e tecnologie IA da parte di imprese terze su WhatsApp, possano costituire un abuso di posizione dominante in violazione dell'art. 102 del Trattato sul funzionamento dell'Unione europea (TFUE).

Per effetto delle nuove condizioni contrattuali, Meta ha vietato alle imprese di fornitura di servizi e tecnologie IA di accedere alla piattaforma WhatsApp e, per questo tramite, di raggiungere gli utenti finali, ogni qual volta il servizio o la tecnologia IA costituisca il servizio principale offerto da queste imprese.



La Commissione ha, dunque, aperto un'istruttoria per esaminare il carattere potenzialmente anticoncorrenziale di suddetta condotta all'interno dello Spazio economico europeo (SEE). Meta ha consentito, fino al 15 ottobre 2025, a diversi fornitori di IA di offrire l'accesso ai propri *Chatbot* tramite WhatsApp, consentendo agli utenti di interagire direttamente con modelli di IA conversazionale all'interno dell'applicazione per attività quali rispondere a domande, generare contenuti o accedere all'assistenza clienti. Per effetto dell'aggiornamento dei *Whatsapp Business Solution Terms* da parte di Meta, la Commissione paventa la possibilità che l'esclusione delle imprese che forniscono servizi e tecnologie di servizi AI possa costituire un abuso di posizione dominante (art. 102 TFUE).

La decisione della Commissione si pone nel contesto della più ampia azione di monitoraggio da essa svolta nei mercati dell'IA, anche sulla base del [Competition Policy Brief in Generative AI and virtual worlds](#) del 19 settembre 2024, documento programmatico che orienta l'operato della Commissione europea nello svolgimento della sua funzione *antitrust* nei mercati dell'AI.

La decisione della Commissione si pone inoltre sulla scia dell'istruttoria già aperta dall'Autorità garante della concorrenza e del mercato (AGCM o l'Autorità) (provvedimento n. 31634 del 30 luglio 2025, su cui v. in questa Rubrica notizia n. 12 del [numero 3/2025](#) [2025/3(12)VH] in *PeM*, 2025, p. 1048), anch'essa relativa al mercato dei servizi IA sull'app di messaggistica WhatsApp.

Se in questa prima fase l'attenzione dell'Autorità si era concentrata sui profili anticoncorrenziali della condotta di Meta costituita nell'installazione automatica e nel posizionamento preminente del *Chatbot* Meta AI su WhatsApp, a far data dal 25 novembre 2025, e anticipando in questo senso le determinazioni della Commissione, l'AGCM ha esteso l'ambito oggettivo dell'istruttoria includendovi le modificazioni contrattuali di cui qui si tratta, contestualmente avviando un sub-procedimento cautelare, all'esito del quale, con il [provvedimento n. 31775 del 22 dicembre 2025](#) (il **Provvedimento cautelare**), l'AGCM ha disposto la sospensione dell'applicazione di queste stesse nuove condizioni contrattuali (nel territorio italiano) ora oggetto del procedimento aperto dalla Commissione europea. Di conseguenza, l'istruttoria aperta dalla Commissione europea riguarderà lo Spazio economico europeo, ad eccezione dell'Italia, al fine di evitare una sovrapposizione, in questa prima fase, con il procedimento avviato dall'AGCM.

Con il Provvedimento cautelare, adottato ai sensi dell'art. 14 *bis*, l. 287/1990, l'AGCM ha disposto nei confronti di Meta, in via cautelare, la sospensione immediata dell'applicazione delle nuove condizioni contrattuali previste dai *Whatsapp Business Solution Terms*, nella parte della sezione, denominata "*AI Providers*", in cui espressamente specificava che le imprese fornitrici di servizi e tecnologie di AI non possono accedere o utilizzare WhatsApp allo scopo di rendere disponibile agli utenti finali tali servizi e tecnologie di AI. L'Autorità, nello sviluppo dell'*iter* motivazionale, ai fini della definizione del procedimento cautelare, ha dapprima ricostruito le condotte di Meta, per quel che riguarda l'integrazione di servizi e tecnologie di AI *Chatbot* su

WhatsApp, prima delle modificazioni contrattuali del 15 ottobre 2025. In effetti, fino a quest'ultima data, WhatsApp risultava essere una piattaforma aperta alla implementazione di *AI Chatbot* forniti da soggetti terzi. In questo contesto si è rilevato come, fino alle intervenute modificazioni contrattuali, la presenza delle *AI Chatbot* fosse assolutamente significativa, dando la possibilità ai fornitori terzi di raggiungere gli utenti finale attraverso la piattaforma WhatsApp. Incidentalmente, è utile segnalare come proprio questa consolidata presenza di imprese che forniscono servizi e tecnologie di AI su WhatsApp ha contribuito alla decisione dell'Autorità di vagliare il carattere potenzialmente anticoncorrenziale dell'installazione automatica, a partire dal marzo 2025, del *Chatbot* Meta AI da parte di Meta.

Tanto premesso e dopo aver perimetrato il mercato rilevante entro il quale la condotta di Meta possa produrre effetti anticoncorrenziali, l'Autorità, ai fini dell'applicazione di una misura cautelare ai sensi dell'art. 14-*bis* l. 287/1990, ha proceduto ad esaminare la sussistenza del *fumus boni iuris* e del *periculum in mora*. Per quanto riguarda il primo presupposto, l'Autorità ha ritenuto che le modificazioni contrattuali di Meta, attraverso le quali è impedito l'accesso alla piattaforma WhatsApp per le imprese di fornitura di servizi e tecnologia *AI Chatbot*, appaiono costituire *prima facie* una possibile violazione dell'art. 102 TFUE. Infatti, la modifica delle condizioni di funzionamento di WhatsApp si colloca in un percorso che ha visto dapprima la presenza su WhatsApp solo di *AI Chatbot* terze, quindi l'ingresso, attraverso la preferenziale installazione automatica, della stessa Meta con il proprio servizio Meta AI e, infine, l'esclusione dei concorrenti, effettivi e potenziali, e il permanere della sola Meta AI, “con un'evidente preclusione concorrenziale e una drastica riduzione dell'offerta per gli utenti finali di tale piattaforma, non basata sui meriti”. Per quanto concerne la ricorrenza del *periculum in mora*, allo stesso modo l'Autorità si è pronunciata in ordine alla sua sussistenza; in questo senso, si è evidenziato che il mercato delle *AI Chatbot* è nascente e in evoluzione ed è, pertanto, necessario preservare il confronto competitivo anche su WhatsApp che rappresenta uno dei principali canali di acquisizione di utenti, soprattutto per gli operatori nuovi entranti che non dispongono già di punti di accesso consolidati e che, quindi, partono già da una condizione di svantaggio competitivo.

Infine, nella scelta della misura da adottare ad esito del procedimento cautelare, l'Autorità ha ritenuto di dover individuare una misura che consentisse, prima della conclusione del procedimento di merito (apertosi con il Provvedimento AGCM n. 31634 del 30 luglio 2025, come visto sopra), l'accesso e la piena operatività dell'*AI Chatbot* su WhatsApp, quale canale di accesso agli utenti finali. Alla luce di queste valutazioni, dunque, l'AGCM ha disposto la sospensione immediata dell'applicazione delle nuove condizioni contrattuali, adottate in data 15 ottobre 2025, previste *WhatsApp Business Solution Terms*, nella misura in cui tale condotta produca effetti sul territorio italiano.

VICTOR HARTL

https://ec.europa.eu/commission/presscorner/detail/it/ip_25_2896

<https://www.agcm.it/media/comunicati-stampa/2025/12/A576-->
<https://digital-strategy.ec.europa.eu/en/news/commission-publishes-policy-brief-competition-generative-ai-and-virtual-worlds>

| 1100

2025/4(23)AB

La sentenza della Corte di giustizia prima sezione nella causa C-413/23 P del 4 settembre 2025 sulla nozione di dati personali e di pseudonimizzazione (caso SRB (o CRU))

La recente decisione della Corte di Giustizia dell'Unione Europea (CGUE), [sentenza 4 settembre 2025, SRB c. EDPS, C-413/23 P](#), offre all'interprete importanti indicazioni sulle nozioni di *dato personale* e di *pseudonimizzazione* con riferimento al regolamento (UE) 2018/1725 (EUDPR) che riguarda il trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi europei, le cui regole, al fine di garantire un'applicazione uniforme e coerente del diritto eurounitario, devono essere interpretate alla luce del regolamento (UE) 2016/679 (GDPR).

La vicenda trae origine da una decisione del 7 giugno 2017 adottata dal Comitato di risoluzione unico (SRB) – agenzia governativa dell'Unione che ha il compito di garantire la risoluzione ordinata delle banche in difficoltà – nei confronti del *Banco Popular Español*, mediante la quale veniva stabilito di svalutare e convertire gli strumenti di capitale e di procedere alla vendita dell'attività d'impresa, in virtù del regolamento (UE) 2014/806. A seguito della risoluzione della banca, il SRB incaricava una società di revisione contabile e di consulenza esterna, *Deloitte*, di valutare se gli azionisti e i creditori del *Banco Popular* avessero in ipotesi potuto ricevere un trattamento migliore in presenza di una procedura ordinaria di insolvenza; ciò allo scopo di poter prendere una decisione definitiva sulla necessità o meno di concedere loro un indennizzo. In data 6 agosto 2018, il SRB pubblicava sul suo sito *Internet* l'avviso relativo alla sua decisione preliminare e l'avvio del procedimento relativo al diritto di essere ascoltati. Detto procedimento era articolato in due fasi: nella prima fase (c.d. iscrizione), gli azionisti e i creditori dovevano manifestare il loro interesse ad esercitare il loro diritto mediante un modulo di iscrizione *online* fornito dal SRB, corredato di un'informativa sulla protezione dei dati personali riguardante il trattamento nell'ambito di tale procedura; nella seconda fase (c.d. consultazione), le persone il cui status di azionisti e creditori interessati era stato verificato dal SRB potevano presentare, mediante un *link* unico personale ricevuto per posta elettronica, le proprie osservazioni sulla decisione preliminare, alla quale era allegata la versione non riservata della valutazione effettuata da *Deloitte*. Successivamente, il SRB chiedeva a quest'ultima di valutare le osservazioni pertinenti (1.104 osservazioni), trasferite attraverso un server dati virtuale sicuro dedicato.

Preme osservare che i membri del personale del SRB incaricati del trattamento delle osservazioni ricevute durante la fase di consultazione non avevano accesso né ai dati raccolti durante la (precedente) fase di iscrizione, né alla chiave dati o alle informazioni che consentivano di risalire all'identità

di un azionista o creditore interessato, posto che a ciascuna osservazione era assegnato un codice alfanumerico unico, generato in modo casuale al momento della ricezione delle risposte al link. Le osservazioni, quindi, trasmesse a *Deloitte* (responsabile del trattamento) recavano esclusivamente un codice alfanumerico, mentre il SRB (titolare del trattamento) era l'unico a poter collegare, mediante tale codice, le osservazioni con i dati identificativi dei loro autori, ricevuti durante la fase di iscrizione (conservati per eventuali future contestazioni o audit).

Alcuni azionisti e creditori interessati presentavano allo European Data Protection Supervisor (**EDPS**) diversi reclami, sostenendo la violazione dell'art. 15(1)(d) EUDPR, lamentando che il SRB non li avesse informati che i loro commenti sarebbero stati comunicati ad altri soggetti, fra cui *Deloitte*. L'EDPS, con decisione del 24 giugno 2020, accertava la violazione dell'obbligo di informazione, rivolgendo un ammonimento e, a seguito di una richiesta di revisione della decisione da parte del SRB, confermava la sua posizione in data 24 novembre 2020, considerando i dati condivisi con *Deloitte* alla stregua di dati pseudonimizzati e comunque dati personali, sebbene i dati identificativi non fossero stati comunicati.

Il SRB ricorreva allora al Tribunale dell'Unione Europea per chiedere l'annullamento della decisione, sostenendo che le informazioni trasmesse a *Deloitte* non costituivano dati personali. Il Tribunale accoglieva il ricorso con [sentenza del 26 aprile 2023, T-557/20](#), affermando che l'EDPS aveva erroneamente classificato le informazioni come dati personali senza un'adeguata analisi della loro riferibilità e identificabilità, specialmente dalla prospettiva della società di consulenza. Avverso tale decisione l'EDPS presentava appello in data 5 luglio 2023, con due motivi di impugnazione, di cui il primo sostanzialmente suddiviso in due parti: la prima parte riguardante la condizione, prevista dall'art. 3(1) EUDPR, secondo cui l'informazione «concerne» una persona fisica e la seconda parte sulla condizione relativa al carattere «identificabile» di tale persona.

Anzitutto, la Corte ricorda che nell'art. 3(1) EUDPR, al pari di quanto stabilito nell'identica definizione di «dato personale» di cui all'art. 4(1) GDPR, l'uso dell'espressione «qualsiasi informazione» riflette l'obiettivo di attribuire un'accezione estesa a tale nozione, che comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse «riguardino» la persona interessata (§ 54 della decisione in rassegna). È vero che un'informazione riguarda una persona fisica qualora, in ragione del suo contenuto, della sua finalità o del suo effetto, essa sia connessa a una persona identificabile – valutazione che il Tribunale contestava all'EDPS di non aver svolto, ma che la Corte non condivide – ma è pacifico che le osservazioni degli interessati sulla valutazione di *Deloitte* riflettevano le opinioni o i punti di vista e, in quanto espressione del pensiero di una persona (v. CGUE, sentenza 20 dicembre 2017, *Nowak*, C-434/16), non possono che essere necessariamente e strettamente connessi a quest'ultima (§ 60).

Quanto al fatto che le informazioni risultanti dalle osservazioni trasmesse a *Deloitte* concernessero una persona fisica «identificabile», il motivo di impugnazione si articola in due censure distinte.

La prima dolenza riguarda l'asserzione del EDPS che i dati pseudonimizzati costituiscono, in ogni caso, dati personali in ragione della sola esistenza di informazioni che consentono di identificare l'interessato, senza che sia necessario esaminare concretamente se, nonostante la pseudonimizzazione, la persona alla quale si riferiscono tali dati sia identificabile da parte del destinatario.

Va ricordato che la pseudonimizzazione non costituisce un elemento della definizione dei «dati personali», ma si riferisce all'attuazione di misure tecniche e organizzative dirette a ridurre il rischio di mettere in correlazione un insieme di dati con l'identità degli interessati, in modo tale che «i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile», come affermato dall'art. 3(6) EUDPR. La Corte ha cura di sottolineare che detto requisito ha, in sostanza, «l'obiettivo di evitare che l'interessato possa essere identificato mediante i soli dati pseudonimizzati» (§ 74).

Se è certo allora che per il SRB le osservazioni degli interessati conservano, nonostante la pseudonimizzazione, il loro carattere personale, avendo altresì la disponibilità delle informazioni identificative aggiuntive, non si può negare che per quanto riguarda *Deloitte*, alla quale sono state comunicate osservazioni pseudonimizzate, le misure tecniche e organizzative possono avere l'effetto di trasmettere tali dati in modo tale che non rivestano natura personale. Ma ciò presuppone, osserva la Corte (§ 77), che *Deloitte* non sia in grado di revocare tali misure in occasione di qualsiasi trattamento effettuato sotto il suo controllo e che queste misure possano effettivamente impedire di attribuire le stesse osservazioni all'interessato anche mediante il ricorso ad altri mezzi di identificazione (come ad esempio la sovrapposizione con altri elementi), in modo tale che, per la società di consulenza esterna, l'interessato non sia o non sia più identificabile.

Un passaggio decisivo nelle argomentazioni della Corte sta nell'analisi del *considerando* 16 del EUDPR (analogo al *considerando* 26 GDPR): se, per un verso, i dati personali sottoposti a pseudonimizzazione, in quanto potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni relative a una persona fisica identificabile, per altro verso, allo scopo di stabilire detta identificabilità è opportuno considerare «tutti i mezzi» di cui il titolare del trattamento o «un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente» e, specificamente, si deve prendere in considerazione «l'insieme dei fattori oggettivi, tra cui i costi e il tempo necessari per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento sia degli sviluppi tecnologici». Così, tali precisazioni sarebbero private di qualsiasi effetto utile – come rilevato nelle [conclusioni dell'Avvocato Generale Spielmann](#), ma per certi versi anche nelle [Linee guida EDPB 1/2025 in tema di pseudonimizzazione](#) – qualora i dati pseudonimizzati dovessero essere considerati, in ogni caso e per qualsiasi persona, alla stregua di dati personali (§ 80).

Dunque, dati che sono di per sé impersonali possono ben acquisire carattere «personale», qualora il titolare del trattamento li metta a disposizione di altre persone che dispongono di mezzi che consentano con ragionevole probabilità l'identificazione dell'interessato, tanto per tali persone quanto, indirettamente, per il titolare del trattamento (v. CGUE, sentenza 9 novembre 2023, *Gesamtverband Autoteile-Handel*, C-319/22) ovvero il titolare del trattamento disponga di strumenti giuridici per ottenere da altri le informazioni aggiuntive che consentano di identificare tale persona (v. CGUE, sentenza 19 ottobre 2016, *Breyer*, causa C-582/14). Epperò, tali affermazioni sono vere fino a quando ci si possa avvalere ragionevolmente di un mezzo per identificare la persona interessata; ciò non vale, per esempio, quando l'identificazione di tale persona è vietata dalla legge o praticamente irrealizzabile perché, ad esempio, implicherebbe un dispendio sproporzionato di tempo, costi e manodopera (v. CGUE, sentenza 7 marzo 2024, *OC*, causa C-479/22). Contrariamente a quanto sostenuto dal EDPS, quindi, «la pseudonimizzazione può, a seconda delle circostanze del caso di specie, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato in modo tale che, per esse, quest'ultimo non sia o non sia più identificabile» (§ 86), nei limiti in cui è escluso cioè che tali soggetti siano ragionevolmente in grado di attribuire i dati pseudonimizzati all'interessato.

Per quanto riguarda la seconda censura, l'EDPS ritiene che il Tribunale avrebbe comunque travisato la natura oggettiva della condizione di identificabilità, ritenendo che il Garante avrebbe dovuto esaminare specificamente se le osservazioni trasmesse a *Deloitte* costituissero, dal punto di vista di quest'ultima, dati personali.

In realtà, la Corte osserva che l'obbligo di informazione incombe sul titolare del trattamento sin dal momento della raccolta dei dati personali presso l'interessato proprio al fine permettere a quest'ultimo di avere una preventiva conoscenza delle varie operazioni compiute con i suoi dati. Nel caso di specie, «l'obbligo di informazione incombente al SRB si applicava nella fattispecie a monte del trasferimento delle osservazioni in questione e a prescindere dal fatto che fossero o meno dati personali, dal punto di vista di *Deloitte*, dopo la loro eventuale pseudonimizzazione» (§ 112). In altre parole, se il titolare del trattamento abbia rispettato o meno i suoi obblighi informativi non può dipendere dalle possibilità di identificazione dell'interessato, di cui disporrebbe, eventualmente, un eventuale destinatario dopo un ulteriore trasferimento dei dati, dal momento che l'oggetto dell'obbligo di informazione si inserisce nel rapporto giuridico fra l'interessato e il titolare del trattamento e integra, per quest'ultimo, una responsabilità che prescinde da successivi trattamenti. Sicché non ha errato l'EDPS a non valutare se le osservazioni trasmesse a *Deloitte* costituissero, dal punto di vista di quest'ultima, dati personali, posto che l'identificabilità dell'interessato va esaminata al momento della raccolta dei dati e dal punto di vista del titolare del trattamento.

Anche questa censura viene accolta, decidendo così la Corte per l'annullamento della sentenza impugnata e rinviando la controversia nuovamente al Tribunale, anche per le valutazioni in ordine ai restanti motivi



di impugnazione (assorbiti), fra cui la violazione del principio di *accountability* del titolare del trattamento (artt. 4, par. 2 e 26, par. 1, EUDPR), in relazione al mancato adempimento dei suoi obblighi di informazione.

ALESSANDRO BERNES

| 1104

[CGUE, sentenza 4 settembre 2025, causa C-413/23 P, SRB c. EDPS](#)

2025/4(24)EG

La sentenza della Corte di giustizia del 2.12.2025 nella causa C-492/23 (caso Russmedia) sul principio di responsabilizzazione del GDPR e il rapporto con la direttiva e-commerce a proposito del trattamento dei dati personali contenuti in annunci pubblicati sulla piattaforma di un mercato online

Con sentenza del 2 dicembre 2025, nella causa C-492/23 (la **Sentenza**), la Corte di giustizia dell'Unione europea (la **Corte**) ha chiarito il ruolo del gestore di un mercato online ai fini del reg. (UE) 2016/679 (**GDPR o Regolamento**), individuando, in chiave di *accountability*, gli obblighi che gli incombono in relazione ai dati personali – anche appartenenti a categorie particolari – contenuti negli annunci pubblicati sulla sua piattaforma.

Il procedimento origina dalla pubblicazione, su un portale di annunci gestito da Russmedia in Romania, di un'inserzione anonima che presentava la ricorrente come persona disponibile a prestazioni sessuali, accompagnata da sue fotografie e dal numero di telefono, in assenza di relativo consenso. L'annuncio è stato rimosso dopo la segnalazione dell'interessata, ma il contenuto era già stato replicato da altri siti di inserzioni, che indicavano il marketplace come fonte.

La ricorrente ha agito nei confronti di Russmedia per ottenere il risarcimento del danno, deducendo anche la violazione della disciplina in materia di protezione dei dati personali; il giudice rumeno ha sospeso il procedimento e ha investito la Corte di questioni pregiudiziali dirette, da un lato, a chiarire la qualificazione del gestore del marketplace ai sensi del Regolamento e, dall'altro, a definire l'estensione degli obblighi discendenti dagli artt. 5(2), 24–26 e 32 GDPR quando gli annunci contengono dati rientranti nell'art. 9(1) GDPR.

Qualificazione del ruolo del gestore del marketplace

Nella sentenza la Corte affronta, in primo luogo, il tema della qualificazione del gestore del marketplace. Ai sensi dell'art. 4 n. 7 GDPR, è titolare del trattamento il soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; secondo giurisprudenza costante della Corte, si ha contitolarità quando più soggetti, mediante decisioni autonome ma convergenti, partecipano alla determinazione di tali finalità o degli elementi essenziali delle modalità del trattamento. Richiamate tali definizioni, la Corte distingue il ruolo dell'utente inserzionista da quello del gestore della piattaforma. L'inserzionista definisce il contenuto dell'annuncio e lo scopo immediato della sua pubblicazione. Il gestore,

invece, fissa i parametri di diffusione degli annunci, ne determina presentazione, durata e collocazione nelle varie rubriche, organizza la classificazione che ne condiziona la visibilità, e, in base alle condizioni generali di utilizzo, si riserva il diritto di distribuire, trasmettere, pubblicare, rimuovere o riprodurre le informazioni ivi contenute, inclusi i dati personali. In sostanza, partecipa alla determinazione dei mezzi essenziali della pubblicazione e della diffusione dei dati personali che figurano negli annunci, influenzando in modo decisivo sulla loro circolazione complessiva. Ne deriva che il gestore del marketplace non può essere escluso dalla nozione di titolare per il solo fatto di non determinare il contenuto dell'annuncio: una lettura siffatta contrasterebbe tanto con la formulazione quanto con la finalità dell'art. 4 n. 7 GDPR, che è quella di assicurare un'ampia protezione agli interessati. La Corte conclude quindi che, in una situazione come quella di specie, il gestore del mercato online è titolare del trattamento dei dati personali contenuti negli annunci pubblicati sul proprio sito ai sensi dell'art. 4 n. 7 GDPR.

Il principio di accountability previsto dal GDPR

Successivamente, la Corte analizza come il principio di responsabilizzazione del titolare del marketplace operi quando il trattamento riguarda dati sensibili, muovendo dalla natura delle informazioni oggetto di causa. L'annuncio controverso conteneva, infatti, informazioni relative alla vita sessuale della ricorrente; si trattava, dunque, di dati rientranti nella definizione dell'art. 9(1) GDPR, il cui trattamento è in linea di principio vietato, salvo il ricorrere di una delle eccezioni tassative previste dal paragrafo 2, tra cui il consenso esplicito dell'interessato.

In questa prospettiva, la Corte richiama l'art. 5(2) GDPR, che consacra il principio di *accountability* quale obbligo in capo al titolare del trattamento di garantire – e di saper dimostrare in ogni momento – la conformità del trattamento stesso ai principi di cui all'art. 5(1) GDPR (liceità, correttezza, trasparenza, esattezza, integrità e sicurezza). Tale obbligo trova attuazione operativa negli artt. 24 e 25 GDPR, che impongono al titolare di progettare e gestire il servizio mediante misure tecniche e organizzative adeguate, integrate nel servizio sin dalla fase di ideazione e per impostazione predefinita, tenendo conto della natura dei dati trattati, del contesto e delle specifiche tipologie di rischio per i diritti e le libertà degli interessati. Quando, poi, vengono in rilievo dati rientranti nell'art. 9(1) GDPR, la valutazione deve assumere un carattere particolarmente puntuale e calibrato sull'elevato impatto potenziale che il trattamento può produrre sui diritti fondamentali alla vita privata e alla protezione dei dati personali.

Su questo sfondo, la Corte chiarisce (parr. 92 e ss. della Sentenza) che, quando un annuncio contenente dati sensibili viene pubblicato sul marketplace, il gestore della piattaforma e l'utente inserzionista assumono la qualità di contitolari, ai sensi dell'art. 26 GDPR, con riferimento al trattamento costituito dalla pubblicazione dell'annuncio sul mercato online. La contitolarità, così ricostruita, non resta sul piano definitorio: comporta che entrambi siano chiamati a presidiare gli obblighi di cui all'art. 5, par. 2, e agli artt. 24 e 25 e a poter comprovare, ciascuno per la propria sfera di intervento, che il trattamento è lecito; che, ove siano in gioco dati rientranti nell'art. 9,

par. 1, ricorre una delle condizioni derogatorie del paragrafo 2 (in particolare il consenso esplicito); e che i dati siano esatti ai sensi dell'art. 5, par. 1, lett. d), GDPR.

Per il gestore, il principio di *accountability* – inquadrato nel contesto di contitolarità – si traduce in una sequenza di obblighi che la Corte enuncia in forma sintetica nel dispositivo e rimette poi al giudice del rinvio per la verifica in concreto. In particolare, il gestore del marketplace, quale titolare del trattamento dei dati personali contenuti negli annunci pubblicati sul proprio sito e contitolare, insieme all'utente inserzionista, del trattamento costituito dalla pubblicazione dell'annuncio sensibile, è tenuto, prima della messa online e mediante misure tecniche e organizzative adeguate, a:

- (i.) individuare gli annunci che contengono dati sensibili, a norma dell'art. 9(1) GDPR;
- (ii.) verificare se l'utente inserzionista che si appresta a collocare un annuncio contenente dati sensibili sia la persona cui i dati figurano in tale annuncio e, in caso contrario,
- (iii.) rifiutare la pubblicazione dell'annuncio, a meno che tale utente inserzionista possa dimostrare che la persona interessata ha prestato il proprio consenso esplicito affinché i dati in questione siano pubblicati in tale mercato online, ai sensi di detto art. 9(2)(a) GDPR, o che sia soddisfatta una delle altre eccezioni previste da tale art. 9(2) alle lettere da b) a j).

Misure di sicurezza

Quanto alla quarta questione, il giudice dell'Unione è stato chiamato a stabilire se il gestore di un mercato online, in quanto titolare del trattamento, debba adottare – ai sensi dell'art. 32 GDPR – misure di sicurezza idonee a impedire o contenere la copia e la successiva ripubblicazione, su altri siti Internet, di annunci che contengono dati sensibili e che sono stati originariamente messi online sul marketplace. Dalle premesse del giudice del rinvio risultava, infatti, che l'annuncio lesivo era stato ripreso da altri portali di annunci che indicavano il marketplace come fonte, senza che fosse chiarito se la diffusione ulteriore dipendesse da accordi di condivisione conclusi da Russmedia o, invece, da iniziative autonome di terzi. In proposito, la Corte precisa che la questione deve essere analizzata come riferita al solo caso in cui il gestore non abbia a sua volta comunicato a terzi il contenuto dell'inserzione, sicché le pubblicazioni successive derivano da copie non autorizzate dell'annuncio originario.

Assunto questo presupposto, la Corte ricostruisce la portata dell'art. 32 GDPR in connessione con l'art. 24 GDPR. Quest'ultimo fissa l'obbligo generale del titolare di predisporre misure tecniche e organizzative adeguate a garantire la conformità del trattamento al Regolamento; l'art. 32 GDPR ne costituisce la declinazione sul piano della sicurezza, imponendo un livello di protezione “adeguato al rischio”, valutato tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche. La Corte sottolinea, inoltre, che l'art. 32 GDPR si innesta su una logica di *risk management*, per cui al titolare è richiesto di

adottare misure idonee a prevenire, per quanto possibile, violazioni dei dati personali, senza che ciò equivalga a pretendere l'azzeramento del rischio.

Nel caso di specie, la Corte richiama il rischio intrinseco della pubblicazione online di dati personali e, a maggior ragione, di dati sensibili. La condivisione online rende i dati potenzialmente accessibili a un numero indeterminato di soggetti e ne agevola la duplicazione e la riproduzione su altri siti, con conseguente difficoltà – se non impossibilità – di assicurare un'effettiva cancellazione. Una volta che un annuncio è stato reso pubblico, la circolazione ulteriore può determinare una perdita di controllo diffusa, incidendo anche sull'effettività delle tutele predisposte dal Regolamento, incluso il diritto alla cancellazione di cui all'art. 17 GDPR.

Su queste basi, nella pronuncia in esame viene affermato che, quando dati sensibili sono oggetto di pubblicazione online, il titolare del trattamento è tenuto, ai sensi dell'art. 32 GDPR, ad adottare misure tecniche e organizzative capaci di garantire un livello di sicurezza adeguato al rischio e, in particolare, idonee a prevenire in modo efficace la perdita di controllo sui dati. Nel contesto di un marketplace, ciò implica la necessità di valutare – in funzione dello stato delle conoscenze tecniche e dei costi di implementazione – quali misure possano ridurre la probabilità che annunci contenenti dati sensibili vengano copiati e illecitamente ripubblicati su altri siti (ad esempio, limitazioni tecniche alla copiatura o all'esportazione dei contenuti, presidi contrattuali nei rapporti con eventuali partner, procedure di rimozione coordinata).

Rapporto con le esenzioni di responsabilità della direttiva e-commerce

Da ultimo, la Corte si pronuncia sul rapporto tra gli obblighi del gestore del marketplace derivanti dal GDPR e le limitazioni di responsabilità previste dalla direttiva 2000/31/CE (**direttiva e-commerce**) per i prestatori intermediari di servizi della società dell'informazione.

La direttiva e-commerce, agli artt. 12–15, disciplina i regimi di esenzione per *mere conduit*, *caching* e *hosting* e, all'art. 15, vieta l'imposizione di un obbligo generale di sorveglianza sui contenuti trasmessi o memorizzati. Il ragionamento viene tuttavia ricondotto al perimetro tracciato dall'art. 1(5)(b) della stessa direttiva, che esclude dal suo ambito le questioni disciplinate dal diritto dell'Unione in materia di protezione dei dati personali, nonché dall'art. 2(4) GDPR, che conferma l'applicazione del Regolamento senza pregiudizio per la direttiva, ma senza che ciò consenta a quest'ultima di incidere sul regime di tutela dei dati personali.

Su questa base, si precisa che la qualificazione di un operatore come titolare del trattamento ai sensi del GDPR non determina, di per sé, l'irrelevanza delle esenzioni della direttiva e-commerce per profili estranei alla protezione dei dati; tuttavia, con riguardo agli obblighi imposti dal Regolamento, le limitazioni di responsabilità degli artt. 12–15 della direttiva e-commerce non sono invocabili per eludere il regime proprio del titolare. In particolare, le esenzioni previste per i prestatori intermediari non possono essere opposte a fronte di violazioni degli obblighi derivanti dall'art. 5(2), e dagli artt. 24–26 e 32 GDPR, relativi al trattamento dei dati personali contenuti negli annunci pubblicati sul marketplace.

Nel dispositivo, si afferma quindi che l'art. 1(5)(b) della direttiva e-commerce e l'art. 2(4) GDPR devono essere interpretati nel senso che il gestore di un mercato online, quale titolare ex art. 4 punto 7 GDPR del trattamento dei dati personali contenuti negli annunci pubblicati sul proprio sito, non può invocare, in caso di violazione degli obblighi derivanti dall'art. 5(2) GDPR e dagli artt. 24–26 e 32 GDPR, le esenzioni di responsabilità previste dagli artt. 12–15 della direttiva e-commerce per i prestatori intermediari di servizi della società dell'informazione.

ELISA GROSSI

<https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=306764&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=15183137>

2025/4(25)ST

Il primo report dell'*Appeals Centre Europe*: potenzialità e ostacoli della risoluzione extragiudiziale delle controversie sulle decisioni delle piattaforme

Il primo ottobre 2025, l'[Appeals Centre Europe](#) (ACE o il Centro) ha pubblicato il suo primo '[Transparency Report](#)' (il Report) sull'attività svolta nel periodo novembre 2024-agosto 2025. ACE è un organismo certificato per la risoluzione extragiudiziale delle controversie ai sensi dell'art. 21 del [regolamento \(UE\) 2022/2065](#) (Digital Services Act, DSA). Il Centro è stato fondato nel 2024 grazie a una sovvenzione iniziale dell'Oversight Board Trust di Meta e attualmente dichiara di autofinanziarsi attraverso le commissioni pagate dalle piattaforme di social media per ogni controversia gestita.

Prima di illustrare i contenuti del Report, ricordiamo brevemente il contesto normativo di riferimento.

L'art. 21 DSA

L'art. 21 DSA prevede il diritto di accesso alla risoluzione extragiudiziale delle controversie relative alle decisioni delle piattaforme online, stabilendone le regole, e così offrendo agli utenti delle piattaforme online una via alternativa e più snella rispetto ai tribunali per contestare le decisioni dei gestori.

Ai sensi dell'art. 21 DSA, gli utenti che non sono soddisfatti di come una piattaforma abbia gestito un loro reclamo (ad esempio, la rimozione di un post o la sospensione di un account) hanno **il diritto di rivolgersi a un organismo di risoluzione delle controversie certificato**. Tale scelta non impedisce all'utente di presentare ricorso alla piattaforma o rivolgersi, in qualunque momento, a un tribunale ordinario, ma semplicemente **si aggiunge alle opzioni a disposizione** per contestare la decisione delle piattaforme. Si tratta di un'opzione particolarmente interessante almeno da due punti di vista, uno relativo ai costi, l'altro relativo ai tempi.

Quanto ai **costi**, è sicuramente incentivante la previsione del paragrafo 5 dell'art. 21 DSA, in base al quale se l'organismo dà ragione all'utente, la piattaforma deve pagare i costi della procedura e rimborsare le spese ragionevoli sostenute dall'utente. Se, viceversa, vince la piattaforma, l'utente non deve pagare nulla, a meno che non abbia agito palesemente in malafede. Quanto ai **tempi**, gli organismi di risoluzione extragiudiziale delle controversie certificati devono mettere le loro decisioni a disposizione delle parti entro un periodo di tempo ragionevole e non oltre 90 giorni dal ricevimento del reclamo. In caso di controversie molto complesse, detto periodo può essere prorogato per una durata massima complessiva di 180 giorni. Si tratta di un tempo che garantisce un minimo di ponderazione e che, sebbene non breve, non è paragonabile a quelli dei tribunali.

L'art. 21 DSA, inoltre, evidenzia degli aspetti importanti e riassumibili come segue:

- le piattaforme devono rendere l'opzione relativa alla risoluzione extragiudiziale delle controversie chiaramente **visibile e facile da usare** sui loro siti;
- gli organismi di risoluzione delle controversie devono essere **certificati dal Coordinatore dei servizi digitali** nazionale per un massimo di 5 anni e devono collaborare al sistema di monitoraggio inviando annualmente una relazione.

Sono previsti ulteriori e specifici requisiti che gli organismi di risoluzione delle controversie devono soddisfare. Il riferimento è, in particolare, all'**indipendenza e imparzialità**: non devono avere legami finanziari o di altro tipo con le piattaforme o con i segnalatori; alla **competenza**: devono avere esperti in contenuti illegali e termini di servizio delle piattaforme; alla **accessibilità**: devono operare online e in almeno una lingua ufficiale dell'UE. Le decisioni di questi organismi **non sono vincolanti**, funzionano come una mediazione autorevole, ma non come una sentenza definitiva.

Il Report.

Lo scopo del Report è diffondere la consapevolezza delle persone riguardo al diritto di contestare le decisioni di una piattaforma. Esso è diviso in quattro parti relative rispettivamente alle statistiche generali, alle schede informative (con una parte dedicata alle informazioni relative ai singoli paesi) e ai piani per il futuro.

Quanto alle statistiche, si legge che nel periodo considerato (novembre 2024-agosto 2025) il Centro ha ricevuto quasi 10.000 ricorsi, e si è ritenuto competente a trattarne oltre 3.300, con una prevalenza di casi contro Facebook, seguito da Instagram, TikTok e YouTube.

Nel Report si delinea una sorta di «mappa termica» degli errori più comuni delle piattaforme e si rileva che sono state ribaltate dal Centro nel 65% dei casi le decisioni delle piattaforme relative a beni e servizi soggetti a restrizioni, nel 57% delle ipotesi le decisioni delle piattaforme relative alla nudità e all'attività sessuale degli adulti e il 50% delle volte le decisioni su discorsi di incitamento all'odio e comportamenti odiosi.

Il dato non è di poco conto se si considera che lo stesso Report si apre con l'affermazione che «le storie degli utenti dei social media che hanno

presentato reclami dimostrano che quando le piattaforme commettono errori, sono le persone a pagarne il prezzo».

Nonostante i progressi compiuti, il Report dichiara che la **cooperazione con le piattaforme è stata discontinua**, sia perché le piattaforme «mantengono il segreto» sugli organismi di risoluzione delle controversie, sia a causa del fatto che spesso le piattaforme non inviano a tali organismi i contenuti oggetto di contestazione. In quest'ultimo caso, il Centro ha emesso «decisione di default» a favore dell'utente oppure, accertata la presenza del contenuto, online ha emesso una decisione utilizzando il link fornito dall'utente. Dal Report risulta che allorché è stata ribaltata la decisione della piattaforma, è stato raccomandato di ripristinare i contenuti o gli account non violatori nel 75% dei casi e di rimuovere i contenuti violatori nel 25% dei casi.

Le decisioni hanno riguardato in particolare:

- post legittimi sull'adozione di animali che sono stati erroneamente rimossi;
- discorsi politici, comprese critiche e satira, rimossi nonostante non violassero le regole della piattaforma;
- bulling e molestie lasciati sulla piattaforma;
- discorsi di incitamento all'odio contro gruppi protetti e comunità vulnerabili lasciati online nonostante violassero le politiche della piattaforma. Ben oltre un terzo delle controversie ammissibili ha riguardato questo aspetto;
- immagini di nudità rimosse nonostante fossero state pubblicate in un contesto medico. La nudità e l'attività sessuale degli adulti è stata la seconda area politica più contestata delle controversie ammissibili ricevute. In particolare, le persone hanno affermato che i loro contenuti erano stati rimossi in modo errato. In diversi casi, le persone ritenevano che i loro contenuti avrebbero dovuto essere coperti da eccezioni quali la nudità per contenuti artistici o per sensibilizzare l'opinione pubblica su condizioni mediche.

Il Report illustra a titolo esemplificativo alcuni casi studio esaminati:

Caso di studio 1. Nudità in un contesto medico: in relazione a un ricorso del marzo 2025 avverso la rimozione da parte di Facebook di un'immagine relativa a un autoesame per il cancro ai testicoli, ACE ha riformato la decisione originaria. Il contenuto rientrava nelle deroghe previste per finalità diagnostico-sanitarie ed è stato disposto il ripristino previo inserimento di un'avvertenza (*warning screen*).

Caso di studio 2. Account TikTok ReZored: nel marzo 2025, il Centro è stato adito da un utente rumeno per il ripristino di un profilo *TikTok*, sospeso a seguito della pubblicazione di un contenuto video ritenuto dalla piattaforma in violazione delle proprie policy. All'esito della fase istruttoria, è emersa l'insussistenza di condotte denigratorie o discriminatorie ai danni di categorie protette. Conseguentemente, ACE ha raccomandato la revoca del provvedimento sanzionatorio, alla quale la piattaforma ha dato esecuzione ripristinando l'operatività dell'account.

Caso di studio 3. Gruppo Facebook Rexored: un utente di Cipro ha presentato un reclamo relativo a un gruppo *Facebook* che era stato sospeso per presunta violazione delle norme di Meta sui beni e servizi soggetti a restrizioni. ACE ha riscontrato che il caso sarebbe dovuto rientrare in un'eccezione che consente alle persone di discutere dei meriti medici dei

farmaci soggetti a prescrizione medica. Facebook, dopo l'intervento dell'*Appeals Centre Europe* ha quindi ripristinato il gruppo in questione.

Caso di studio 4. incitamento all'odio contro le comunità rom: un'organizzazione slovacca ha inviato una contestazione contro la decisione di TikTok di lasciare online un commento che utilizzava un linguaggio offensivo e degradante nei confronti dei rom. ACE ha riscontrato che il contenuto violava le regole di TikTok in materia di incitamento all'odio e comportamenti offensivi e ne ha raccomandato la rimozione. Comunicata la decisione a TikTok, il contenuto è stato rimosso.

Caso di studio 5. Decisione della piattaforma ribaltata sulla base dei suoi valori: un utente francese ha inviato una contestazione richiedendo la rimozione di un post da Facebook. Il post sosteneva che le persone che non si identificano rigorosamente come maschi o femmine dovrebbero consultare uno psichiatra. Meta aveva esaminato il post, non aveva riscontrato violazioni e non lo aveva rimosso, nonostante, come rilevato da ACE, la posizione di Meta contro gli stereotipi dannosi risulti nella motivazione della sua politica sui comportamenti che incitano all'odio e nei principi dell'azienda in materia di voce, dignità e sicurezza. Il post è stato poi rimosso.

Nella parte finale del Report, si trovano indicate le **azioni** che secondo il Centro potrebbero migliorare in futuro il quadro relativo agli errori nelle decisioni prese dalle piattaforme.

Secondo ACE, potrebbe essere utile che le piattaforme:

- garantiscano un coinvolgimento regolare con gli organismi di risoluzione delle controversie, attraverso punti di contatto chiari;
- condividano il contenuto originale contestato con gli organismi di risoluzione delle controversie;
- forniscano agli utenti un numero di riferimento univoco da comunicare all'organismo di risoluzione delle controversie. Ciò consente alle piattaforme di individuare il contenuto in modo rapido e sicuro;
- attuino le decisioni degli organismi di risoluzione delle controversie e informino gli utenti quando lo hanno fatto.

Il Report auspica che gli organismi di risoluzione extragiudiziale delle controversie certificati possano avere un ruolo più incisivo e a tal fine si propone di espandere la competenza di tali organismi a nuovi settori e di aggiungere il controllo su nuove piattaforme rispetto a Facebook, TikTok e YouTube, Instagram, Threads, Pinterest.

SARA TOMMASI

<https://www.appealscentre.eu/wp-content/uploads/2025/09/Appeals-Centre-Europe-Transparency-Report.pdf>

2025/4(26)RA

La sentenza del 19.11.2025 del Tribunale dell'Unione europea di rigetto del ricorso di Amazon per l'annullamento della decisione della Commissione europea di designazione di Amazon Store come VLOP ai



sensi del Digital Services Act e le inerenti statuizioni di conformità del DSA alla CDFUE

| 1112

Con ricorso del 5 luglio 2023, Amazon Services Europe Sàrl, cui è successivamente subentrata Amazon EU Sàrl (**Amazon**), ha chiesto l'annullamento della decisione C(2023) 2746 final della Commissione, del 25 aprile 2023, che ha designato 'Amazon Store' come piattaforma *online* di dimensioni molto grandi (**VLOP**), ai sensi dell'art. 33(4) del regolamento (UE) 2022/2065 (Digital Services Act, **DSA**) (v. in questa rubrica la notizia n. 5 nel numero [2/2023](#) [2023/2(5)RA], in *PeM* 2023, p. 381 e in *Atlante*, p. 348).

La decisione risulta particolarmente significativa, perché Amazon nel suo ricorso non ha lamentato una non corretta applicazione del DSA ma ha contestato lo stesso DSA, sostenendo che il medesimo regolamento violerebbe la Carta dei diritti fondamentali dell'Unione europea (**CDFUE**).

In particolare, con il proprio ricorso, Amazon ha contestato la legittimità dell'art. 33 DSA – in virtù del quale, ai VLOP e ai motori di ricerca *online* di dimensioni molto grandi (**VLOSE**), è imposto di rispettare taluni obblighi supplementari, contenuti agli artt. 34 e seguenti del DSA – sul presupposto che tale disposizione contrasterebbe con alcuni principi e diritti sanciti dalla CDFUE.

Con decisione del 19 novembre 2025, il Tribunale dell'Unione europea (il **Tribunale**) ha tuttavia respinto il ricorso presentato da Amazon.

Segnatamente, premessa la ricevibilità del ricorso, il Tribunale ha anzitutto escluso la violazione dell'art. 16 CDFUE, in virtù del quale è riconosciuta ai consociati la libertà d'impresa. In proposito, il Tribunale ha osservato che gli obblighi imposti dagli artt. 34 ss. DSA costituiscono bensì, effettivamente, un'ingerenza del diritto dell'Unione rispetto a tale libertà, poiché impongono ai fornitori di VLOP di adottare misure che possono rappresentare, per loro, un costo notevole, avere un impatto considerevole sull'organizzazione delle loro attività o richiedere soluzioni tecniche difficili e complesse. Tuttavia - ha proseguito il Tribunale - tale ingerenza non inficia il contenuto essenziale della libertà, e deve anche reputarsi giustificata, tenuto conto che essa è preordinata a prevenire o, comunque, limitare rischi sistemici derivanti dalla diffusione di contenuti illeciti o dalla violazione di diritti fondamentali, che possono trovare diffusione nell'ambito di VLOP e VLOSE.

In secondo luogo, il Tribunale ha escluso che sussista una violazione del diritto di proprietà, garantito ai sensi dell'art. 17 CDFUE. Sul punto, i giudici hanno osservato, per un verso, che la ricorrente non ha sviluppato alcun argomento a sostegno della propria affermazione secondo cui gli obblighi previsti agli artt. 34 ss. DSA costituiscono un'ingerenza nel suo diritto di proprietà; per altro verso, che le richiamate disposizioni impongono certamente oneri amministrativi ai fornitori di VLOP, ma non li privano della proprietà di tali piattaforme e, in ogni caso, che, anche supponendo che i predetti obblighi possano essere considerati ingerenze nel diritto di proprietà, tali ingerenze sarebbero comunque giustificate da motivi analoghi a quelli poc'anzi richiamati con riguardo all'asserita violazione dell'art. 16 CDFUE.

In terzo luogo, il Tribunale ha escluso la sussistenza di una violazione, dedotta da Amazon, dell'art. 20 CDFUE, il quale sancisce il principio di uguaglianza. In proposito, il Tribunale ha rilevato che il legislatore europeo, nell'ambito del proprio ampio margine di discrezionalità, ha deciso in modo non arbitrario né manifestamente inadeguato di trattare VLOP e VLOSE, da un lato, in maniera differenziata rispetto alla generalità delle altre piattaforme *online*, anche tenuto conto del fatto che le prime raggiungono un maggior numero di utenti rispetto alle seconde e, dunque, possono esporre molte più persone a contenuti illeciti, presentando perciò rischi sistemici per la società.

Ancora, il Tribunale ha respinto il rilievo di Amazon secondo cui gli obblighi imposti dagli artt. 34 ss. DSA contrasterebbero con l'art. 11(1) CDFUE, secondo cui ogni persona ha diritto alla libertà di espressione e d'informazione. A tale riguardo, il Tribunale ha osservato, da un lato, che la ricorrente non ha spiegato la ragione per cui le richiamate norme del DSA costituirebbero un'ingerenza nella predetta libertà. Dall'altro, che, sebbene l'art. 38 DSA – laddove obbliga i fornitori di VLOP ad assicurare almeno un'opzione per ciascuno dei loro sistemi di raccomandazione, non basata sulla profilazione – possa considerarsi un'ingerenza nella libertà di espressione e d'informazione, limitando il modo in cui i predetti fornitori possono presentare i prodotti commercializzati sulle loro piattaforme, tale ingerenza è tuttavia giustificata, risultando prevista dalla legge, non incidendo sul contenuto essenziale delle libertà e perseguendo, in modo proporzionato, l'obiettivo legittimo di tutela dei consumatori.

Da ultimo, il Tribunale ha escluso pure la violazione dell'art. 7 CDFUE, che – al pari dell'art. 8 CEDU – garantisce il diritto al rispetto della vita privata e alla protezione delle informazioni riservate, rilevando che gli obblighi di trasparenza pubblicitaria e di accesso a determinati dati imposti dal DSA costituiscono sì un'ingerenza in tale diritto, ma che essi sono previsti dalla legge, proporzionati e finalizzati al perseguimento di un obiettivo di interesse generale (vale a dire, la prevenzione di rischi sistemici e, in particolare, assicurare la tutela dei consumatori), che li giustifica.

La decisione del Tribunale potrà essere impugnata da Amazon dinnanzi alla Corte di giustizia dell'Unione europea, limitatamente a motivi di diritto.

RICCARDO ALFONSI

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=306323&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=14408142>

2025/4(27)GD

I rimedi comportamentali e strutturali imposti a Google con sentenza del 2.9.2025 a proposito della proprietà di Chrome, dei dati di ricerca e dei contratti in esclusiva nella causa Stati Uniti d'America c. Google LLC, 2024 WL 3647498

Con una pronuncia del 2.9.2025 (la **Seconda sentenza**), la Corte degli Stati Uniti d’America per il Distretto della Columbia, nella persona del giudice Amit P. Mehta (la **Corte**), ha chiuso la seconda fase di uno storico processo, apertasi dopo la clamorosa sentenza del 5.8.2024, che aveva accertato l’abuso di posizione dominante di Google LLC (**Google**) nelle ricerche online e nella pubblicità degli annunci di testo (v. in questa Rubrica, la notizia n. 12 del numero 3/2024 [[2024/3\(12\)GD](#)], in *PeM* 2024, p. 1073).

La seconda fase del processo ha avuto ad oggetto la definizione della sanzione da irrogare a Google e i c.d. rimedi comportamentali e strutturali.

La Seconda sentenza (di ben 230 pagine) ha disposto che Google

- dovrà condividere parte dei propri dati di ricerca con i concorrenti
- non potrà più firmare contratti di esclusiva per la distribuzione del suo motore di ricerca sui dispositivi e browser
- potrà mantenere la proprietà del browser Chrome.

La Corte ha, quindi, rigettato la proposta del Dipartimento di Giustizia degli USA (**DoJ**) che prevedeva (1) di imporre a Google la cessione a terzi del suo motore di ricerca Chrome e (2) a seguire, l’impossibilità per Google, per almeno cinque anni, di possedere un proprio browser e di rientrare nel mercato dei browser anche tramite quote in motori di ricerca concorrenti, prodotti concorrenti basati sull’intelligenza artificiale (AI) o tecnologie pubblicitarie (su cui v. in questa Rubrica, la notizia n. 52 del numero 4/2024 [[2024/4\(52\)GD](#)], in *PeM* 2024, p. 1567).

Nella Seconda sentenza, si afferma che la cessione di Chrome a terzi sarebbe incredibilmente complicata e altamente rischiosa (citando testualmente la pronuncia: *“It would be incredibly messy and highly risky. (...) Chrome does not run as a standalone business. At the most basic level, it depends on Google for a host of administrative functions, such as finance, marketing, and human resources”*).

In altri termini, secondo la Corte, la cessione di Chrome a terzi avrebbe potuto comportare un sostanziale peggioramento del prodotto (Chrome) e un danno per i consumatori – citando testualmente la pronuncia *“substantial product degradation and a loss of consumer welfare”*.

Inoltre, la Corte sostiene che il DoJ non abbia soddisfatto l’onere della prova per giustificare un così gravoso rimedio “strutturale radicale” implicante la cessione forzata di Chrome.

Tuttavia, la Seconda sentenza non rappresenta una vittoria “piena” per Google, in quanto la Corte ha parzialmente accolto altri rimedi proposti dal DoJ.

In primo luogo, la Corte ha stabilito che Google dovrà condividere con i concorrenti qualificati (come **Bing**, **DuckDuckGo** e aziende di intelligenza artificiale come **OpenAI**) un set limitato di dati dell’indice di ricerca che Google crea scansionando il web e informazioni sulle interazioni degli utenti. L’obiettivo è aiutare i concorrenti qualificati a sviluppare prodotti competitivi. La condivisione di tali dati rilevanti contenuti nell’indice di ricerca di Google dovrà avvenire *una tantum* (e non periodicamente, come aveva richiesto il DoJ).

In secondo luogo, la Corte ha specificato che sebbene Google possa continuare a pagare terzi, come **Apple** e **Mozilla**, per rendere Google Search

il motore di ricerca predefinito, non potrà più stipulare accordi di esclusiva che escludono la concorrenza.

La Corte ha altresì nominato un Comitato tecnico per monitorare l'implementazione dei rimedi da parte di Google e garantire che quest'ultima non eluda la decisione finale del Tribunale.

Infine, la Corte ha stabilito che i rimedi resteranno in vigore per sei anni (rigettando sia la proposta del DoJ che prevedeva una durata di 10 anni, sia la proposta di Google che prevedeva una durata di 3 anni).

Google ha già annunciato che intende impugnare la pronuncia in commento. Ciò significa che la battaglia legale è ben lontana dall'essere definitivamente conclusa.

GIORGIA DIOTALLEVI

https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2020cv3010-1436

2025/4(28)FF

La sanzione di 255,7 milioni di euro irrogata dall'AGCM a Ryanair il 19.12.2025 per abuso di posizione dominante nei confronti delle agenzie di viaggio fisiche e *online* per i servizi aerei nazionali ed europei da e/o verso l'Italia

L'Autorità garante della concorrenza e del mercato (AGCM o l'Autorità), con il [provvedimento](#) adottato nella sua adunanza del 19 dicembre 2025, ha concluso il procedimento avviato con propria [delibera del 14 settembre 2023, n. 30772](#), nei confronti di Ryanair DAC – successivamente esteso sul piano soggettivo alla società Ryanair Holdings Plc con [delibera del 16 gennaio 2024, n. 31027](#) (collettivamente **Ryanair**) – accertando un abuso di posizione dominante di natura escludente, in violazione dell'art. 3 della l. n. 287/1990 e dell'art. 102 del Trattato sul funzionamento dell'Unione europea (TFUE).

Il procedimento trae origine da segnalazioni presentate dall'*Associazione Italiana Agenti di Viaggio* (AIAV) e dalla *Federazione del Turismo Organizzato* (FTO), nonché dalle associazioni dei consumatori *Associazione Codici Lombardia* e *Associazione Codici Nazionale*. Nel corso dell'istruttoria, l'Autorità ha ammesso l'intervento di altri soggetti rappresentativi della filiera dell'intermediazione turistica, tra cui le associazioni di categoria AdvUnite, FIAVET ed euTravelTech, nonché diverse *Online Travel Agencies* (OTA) come *Vacaciones eDreams*, *Kiwi.com*, *BravoNext* (*Lastminute.com*), *Fru.PL* e *Booking.com*.

L'oggetto della contestazione riguardava una serie di condotte attraverso le quali Ryanair, in qualità di vettore dominante nel mercato a monte del trasporto aereo, avrebbe bloccato, ostacolato o comunque reso più difficoltosa l'offerta, da parte delle agenzie di viaggio, dei propri voli in combinazione con voli di altri vettori o con ulteriori servizi, necessari alla composizione di "pacchetti turistici".

Ritenute sussistenti le violazioni contestate, l'Autorità ha irrogato alle due società, in solido, una sanzione amministrativa pecuniaria pari a oltre 255,7



milioni di euro, imponendo altresì la cessazione delle condotte e l'adozione di misure idonee a garantire condizioni eque di accesso ai voli Ryanair per le agenzie di viaggio, da comunicarsi con apposita relazione entro 90 giorni dalla notifica del provvedimento.

La decisione si colloca all'esito di un'articolata attività istruttoria, protrattasi per oltre due anni, nel corso della quale è stato avviato anche un sub-procedimento cautelare, svoltosi tra aprile e maggio 2024, concluso senza l'adozione di misure. In questo complesso *iter* procedimentale appare utile soffermarsi sui passaggi centrali del percorso argomentativo seguito dall'AGCM:

- (i) l'individuazione del mercato rilevante a monte;
- (ii) la sussistenza della posizione dominante in capo a Ryanair;
- (iii) il rapporto di concorrenza con le agenzie *online* nel mercato a valle;
- (iv) la qualificazione abusiva delle condotte contestate; e
- (v) i riflessi di tale assetto sul benessere dei consumatori (v).

(i) La definizione di “**mercato rilevante**” assume rilievo centrale ai fini della verifica della sussistenza di una posizione dominante e della capacità dell'impresa di incidere sul mantenimento di una concorrenza effettiva (§ 293-394; cfr. [Corte giust., 14 febbraio 1978, c. 27/76](#), United Brands c. Commissione), nel caso di specie limitatamente alla dimensione territoriale nazionale (§ 353-358). In tale prospettiva, l'AGCM qualifica i servizi di trasporto aereo come un *input* essenziale per l'attività delle agenzie di viaggio, ponendo al centro dell'analisi il rapporto tra queste e i vettori aerei, anche in ragione del ruolo svolto dalle esigenze dei consumatori nella strutturazione dell'offerta degli intermediari, in termini di varietà delle destinazioni, combinazioni di servizi e pluralità di soluzioni. Per tale ragione, l'AGCM respinge la tesi di Ryanair secondo cui il rapporto con le agenzie dovrebbe essere qualificato esclusivamente come relazione *business-to-business*, con la conseguenza di escludere qualsiasi rilievo del versante della domanda finale. Un simile approccio non consentirebbe di cogliere le dinamiche concorrenziali che caratterizzano la vendita dei servizi turistici, trascurando il ruolo centrale svolto dalle preferenze dei consumatori nella strutturazione dell'offerta degli intermediari. Alla luce di tali considerazioni, il **mercato rilevante a monte** è rappresentato dai servizi di trasporto aereo di linea, nazionali ed europei, da e/o verso l'Italia, quali *input* per l'attività delle agenzie di viaggio, fisiche e *online* (§ 309).

(ii) Il secondo passaggio dell'analisi riguarda la verifica della sussistenza di una posizione dominante in capo a Ryanair, che l'AGCM ritiene integrata, sulla base di una pluralità di elementi convergenti emersi in istruttoria. (§ 322). In particolare, l'Autorità valorizza le elevate **quote di mercato** detenute dal vettore nei collegamenti nazionali ed europei da e verso l'Italia, stabilmente superiori al 40%, caratterizzate da un significativo distacco rispetto ai principali concorrenti e con un andamento stabile nel tempo (§ 312-313); nonché la **capillarità** della rete di collegamenti offerta, che consente a Ryanair di raggiungere la maggioranza delle destinazioni rilevanti (oltre il 60% e, per alcuni aeroporti, fino all'81% delle destinazioni di maggiori dimensioni) (§ 314-315).

A tali elementi si affiancano il ruolo di principale, e in molti casi unico, vettore operante nelle città aeroportuali italiane e la posizione di *leadership* a livello europeo, in un contesto segnato dalla contrazione dell'offerta e da limiti strutturali all'espansione dei concorrenti (§ 319-321). Il quadro risulta ulteriormente rafforzato dal dato secondo cui Ryanair è il vettore più frequentemente scelto dai consumatori italiani, con una quota di preferenza pari a circa il 46% nel 2024.

In questo contesto, l'AGCM conclude che Ryanair rappresenti un partner commerciale imprescindibile per le agenzie di viaggio che intendano operare nel mercato nazionale offrendo servizi turistici comprensivi di un volo aereo, secondo una logica che richiama quella dell'*essential facility*, in termini di accesso competitivo al mercato intermediato attraverso canali digitali (v. [Corte giust., 25 febbraio 2025, c. 233/23](#), Alphabet Inc. e a. c. AGCM).

(iii) La qualifica di Ryanair come titolare di una posizione dominante nel mercato a monte costituisce il presupposto per esaminare l'incidenza della sua condotta nel mercato a valle, relativo all'attività di prenotazione e vendita di servizi turistici, al fine di comprendere come la forza del vettore si rifletta sulle successive fasi della filiera. In tale prospettiva, l'AGCM osserva che la prenotazione dei servizi turistici avviene oggi prevalentemente attraverso canali digitali: il sito del vettore (*Travel Service Provider* – TSP) rappresenta il principale canale di acquisto dei biglietti aerei (71%), seguito dalle agenzie *online* (22%), mentre il ricorso alle agenzie fisiche assume un ruolo residuale (7%).

Questa premessa è necessaria per delimitare con più esattezza i confini del mercato rilevante: difatti l'AGCM opera una prima **distinzione tra canali di vendita offline e online**, evidenziando come le agenzie di viaggio fisiche e le OTA rispondano a esigenze differenti e presentino caratteristiche non sovrapponibili (§ 339-345). Le prime sono scelte prevalentemente per funzioni di consulenza e assistenza all'acquisto, mentre i canali *online* risultano preferiti per ragioni di semplicità d'uso, convenienza e possibilità di comparazione delle offerte. In linea con l'approccio seguito dalla Commissione europea in precedenti operazioni di concentrazione, ([M.8046, TUI/Transat France](#), 20 ottobre 2016; [M.6163, AXA/Permira / Opodo/Go Voyages/eDreams](#), 30 maggio 2011), l'AGCM non esclude tuttavia che le condotte di Ryanair possano produrre effetti pregiudizievoli anche nei confronti delle agenzie fisiche, nella misura in cui queste, nell'esercizio della propria attività, facciano ricorso a strumenti digitali. In tal senso, l'ostacolo all'operatività delle OTA appare produrre effetti indiretti anche sulle agenzie fisiche: a conferma di ciò, il 67% di queste ha registrato un impatto negativo sulla domanda già a seguito dell'introduzione della prima condotta restrittiva adottata da Ryanair, relativa alle procedure di identificazione dei passeggeri (§ 448-454).

In secondo luogo, sotto il profilo merceologico, l'Autorità esclude dal perimetro del mercato rilevante l'**intermediazione dei servizi alberghieri e para-alberghieri** (§ 54-57; § 346-352) qualificandola come appartenente ad un segmento di mercato distinto, in ragione di differenze tecnologiche e organizzative, nonché di modelli di remunerazione, titoli abilitativi e garanzie offerte ai consumatori. Tale impostazione si allinea all'orientamento più

recente della Commissione europea ([M.10615, Booking Holdings/eTraveli Group](#), 25 settembre 2023), pur a fronte di precedenti più risalenti di segno diverso ([M.8416, The Priceline Group/Momondo Group Holdings](#), 17 luglio 2017).

Individuato il mercato rilevante a valle nell'intermediazione *online* dei voli, venduti singolarmente o in combinazione con altri servizi turistici, l'Autorità si sofferma sul rapporto economico tra Ryanair e le agenzie *online*, chiarendo come il vettore non possa essere considerato un mero fornitore, bensì un operatore che, attraverso il proprio canale diretto di vendita, entra in rapporto concorrenziale con le OTA (§ 359-373). Queste ultime non si limitano a riprodurre l'offerta dei singoli vettori, ma svolgono una funzione di intermediazione che consente ai consumatori di accedere a soluzioni di viaggio alternative, anche mediante la combinazione di voli operati da vettori differenti, con vantaggi in termini di prezzo, orari e flessibilità. Parallelamente, Ryanair affianca alla vendita diretta dei propri voli una gamma articolata di servizi turistici accessori, quali alloggio, noleggio auto e ulteriori servizi ancillari, remunerati secondo un modello commissionale analogo a quello tipico delle OTA. Il vettore si colloca così, per una parte della propria attività, in una posizione funzionalmente assimilabile a quella di un intermediario *online*, competendo con le OTA sia direttamente, quando l'offerta riguarda esclusivamente voli Ryanair, sia indirettamente, quando tali voli sono combinati con quelli di altri vettori, per l'attrazione della domanda finale. (§ 396).

In tale contesto, centrale è il ruolo del traffico *web* quale risorsa strategica per la competizione nel mercato a valle. Dalle evidenze istruttorie emerge come Ryanair e le OTA competano per intercettare l'attenzione dei consumatori e indirizzarne le scelte di acquisto verso il proprio canale digitale, in un contesto in cui il punto di accesso iniziale tende a coincidere con il punto di acquisto. Alla luce di tali elementi, l'Autorità conclude che tra Ryanair e le agenzie *online* sussiste un **rapporto concorrenziale effettivo nel mercato a valle** dell'intermediazione *online* dei voli, con la conseguenza che le condotte del vettore non si risolvono in mere scelte distributive, ma risultano idonee a incidere sulla struttura concorrenziale del mercato.

(iv) Dopo aver delineato il contesto, l'AGCM ricostruisce le **condotte contestate** a Ryanair come una serie di comportamenti di ostacolo progressivamente intensificatisi nel tempo, idonei a incidere sull'operatività delle agenzie di viaggio, in particolare *online*, e sulla loro capacità di offrire voli Ryanair ai consumatori finali. Tali condotte si sviluppano secondo un *climax* ascendente, avviatosi a partire dall'aprile 2023.

In una prima fase, Ryanair ha introdotto specifiche procedure di verifica dell'identità applicabili ai passeggeri che avevano acquistato il titolo di viaggio tramite agenzie di viaggio. Quando l'acquisto era ricondotto a un account riconducibile a un'agenzia, la compagnia bloccava la prenotazione, comunicando al passeggero l'impossibilità di effettuare il *check-in online* e richiedendo la creazione di un account Ryanair, la fornitura dei dati personali e la verifica dell'identità. Quest'ultima poteva avvenire attraverso una procedura *online*, in forma "rapida" (basata su tecnologia di riconoscimento facciale) o "standard" (mediante invio della firma e di copia del documento),

ovvero presso la biglietteria Ryanair in aeroporto entro 60 minuti dalla partenza, con applicazione di un supplemento fino a 75 euro per il *check-in* in aeroporto (§ 98-104).

Nel corso di una seconda fase, da novembre 2023, Ryanair ha adottato ulteriori accorgimenti tecnici idonei a impedire o rendere estremamente difficoltosa la vendita dei propri voli da parte delle OTA. In particolare, ha introdotto il sistema denominato “Shield”, finalizzato all’individuazione e al blocco “a monte” delle prenotazioni provenienti dalle OTA. Secondo quanto emerge dalla documentazione istruttoria, il sistema era volto a impedire il perfezionamento degli acquisti mediante il blocco dei pagamenti effettuati con carte di credito categorizzate come B2B, con un effetto di sostanziale preclusione della finalizzazione della transazione. A ciò si era affiancata la cancellazione massiva dei soli *account* riconducibili alle OTA (§ 105-111).

Durante la terza fase, le condotte di ostacolo sono state accompagnate da una pressione commerciale e reputazionale esercitata da Ryanair nei confronti delle OTA, per indurle a sottoscrivere specifici accordi di *partnership*. Tale pressione si è manifestata non solo attraverso il persistente blocco delle prenotazioni, ma anche mediante una campagna stampa critica rivolta alle singole OTA non allineate (cd. OTA pirata) protrattasi sino alla sottoscrizione degli accordi. I contratti proposti, denominati *Direct Distribution Agreement* o *Direct Sale Agreement*, prevedevano, tra l’altro, che le OTA potessero utilizzare i dati dei voli Ryanair esclusivamente ai fini della visualizzazione, ma non della vendita diretta, imponendo che la prenotazione fosse finalizzata sul sito del vettore e che i consumatori accettassero i termini e le condizioni, incluse quelle in materia di *privacy*, predisposte da Ryanair (§ 112-125). Tali accordi, presentati dalla compagnia come funzionali a garantire che le tariffe più basse dei voli Ryanair fossero disponibili esclusivamente sul proprio sito, si inserivano in una logica di *self-preferencing*, configurando il canale diretto del vettore come punto privilegiato per la finalizzazione dell’acquisto ([Corte giust., 10 settembre 2024, c. 48/22](#), Google e Alphabet c. Commissione (Google Shopping); in argomento, v. in questa Rubrica la notizia n. 8 del [numero 3/2025](#) [2025/3(8)FZ], in *PeM* 2025, p. 1036).

Le condotte descritte si sono protratte almeno fino al 22 aprile 2025 – ad istruttoria già ampiamente avviata – data in cui Ryanair ha modificato le modalità di integrazione delle proprie *Application Programming Interfaces* (API), ossia interfacce che consentono l’integrazione tecnica tra i sistemi informatici di operatori diversi, includendo nella soluzione *whitelabel iFrame* ulteriori specifiche tecniche relative ai servizi da offrire ai consumatori. Le API così sviluppate hanno consentito alle agenzie *online* di combinare i voli Ryanair con servizi ulteriori, permettendo la creazione di offerte più articolate sotto il profilo qualitativo e quantitativo, favorendo il riavvio della dinamica concorrenziale nei mercati a valle. Resta tuttavia impregiudicata la verifica, da parte dell’autorità, della idoneità di tale soluzione a rimuovere in modo stabile gli effetti escludenti delle condotte accertate (§ 476; 490).

Alla luce di tale ricostruzione, l’Autorità ritiene integrati i presupposti per l’adozione sia della sanzione amministrativa pecuniaria sia delle misure inibitorie, in quanto le condotte accertate – qualificate come **abuso di**

posizione dominante – risultano idonee a incidere in modo significativo sulla struttura concorrenziale del mercato a valle.

(v) Tale passaggio offre altresì lo spunto per alcune considerazioni sugli effetti indiretti dei comportamenti sanzionati sul benessere dei consumatori, inteso quale risultato del corretto funzionamento del processo competitivo (§ 454). Pur muovendo da una valutazione propriamente *antitrust*, centrata sulla struttura dei mercati interessati, l'analisi dell'Autorità consente di apprezzare come le condotte escludenti contestate a Ryanair siano idonee a riflettersi anche sulla posizione dei consumatori finali.

In tale prospettiva sistematica, il rigetto delle istanze fondate sulla violazione del Codice del consumo promosse da alcune associazioni (§ 21) non ha impedito all'Autorità di valorizzare, in chiave propriamente *antitrust*, una pluralità di pregiudizi indiretti per i consumatori, quali la riduzione delle possibilità di scelta effettiva (ad esempio, l'accesso a soluzioni di viaggio alternative e a combinazioni multi-vettore), il peggioramento della qualità dell'esperienza di acquisto – derivante da procedure aggiuntive, blocchi delle prenotazioni e costi accessori – nonché i rischi di incremento dei prezzi connessi alla concentrazione del traffico sul canale diretto del vettore dominante. Tale impostazione si inserisce nel solco di una concezione del consumatore non come mero destinatario passivo della tutela, bensì come protagonista del mercato concorrenziale, la cui centralità è confermata dal riconoscimento della legittimazione ad attivare direttamente rimedi *antitrust* in sede civile, nel quadro del cd. *private enforcement antitrust*. Questo approccio, affermatosi inizialmente nella giurisprudenza europea ([Corte giust., 20 settembre 2001, c. 453/99](#), *Courage*; [Corte giust., 13 luglio 2006, da c. 295/04 a c. 298/04](#), *Manfredi*) e nazionale ([Cass., Sez. Unite, 4 febbraio 2005, n. 2207](#), ma già [Cass., 1° febbraio 1999, n. 827](#)), è stato successivamente codificato dalla [dir. 2014/104/UE](#), recepita con [d.lgs. 3/2017](#).

Nel provvedimento in esame, la tutela del consumatore rileva non già come autonomo parametro di valutazione, bensì quale criterio di apprezzamento dell'idoneità dei rimedi imposti, chiamati non solo a porre fine alle condotte accertate, ma anche a ristabilire condizioni di mercato tali da garantire un'offerta più ampia, trasparente e qualitativamente migliore per i consumatori finali.

È opportuno, infine, sottolineare che il quadro delineato dal provvedimento presenta carattere provvisorio, atteso che Ryanair, in un [comunicato](#) del 23 dicembre 2025, ha annunciato l'intenzione di impugnare il provvedimento dinanzi alle competenti autorità giurisdizionali. La compagnia ha infatti contestato la decisione e la sanzione irrogata, ritenendole prive di fondamento giuridico, e ha dichiarato di voler far valere, in sede contenziosa, alcuni precedenti giurisprudenziali che hanno valorizzato i benefici per i consumatori del modello di vendita diretta.

FRANCESCA FERRETTI

https://www.agcm.it/dotcmsdoc/allegati-news/A568_chius_omi%20x%20pubb..pdf

2025/4(29)GG

Il Codice di condotta per gli influencer e le modifiche alle Linee guida per gli influencer approvati dall'AGCOM con delibera n. 197/25/CONS del 23.7.2025

| 1121

Il 23 luglio 2025 l'Autorità per le garanzie nelle comunicazioni (**AGCOM** o l'**Autorità**) ha approvato la versione definitiva delle *Linee guida volte a garantire il rispetto delle disposizioni del testo unico da parte degli influencer* (le **Linee guida**), nonché il *Codice di condotta per gli influencer* (il **Codice di condotta**): allegati A e B alla [delibera n. 197/25/CONS](#). Con i provvedimenti in commento, l'Autorità ha equiparato gli influencer cd. "rilevanti" ai fornitori di servizi media audiovisivi, rendendo di conseguenza applicabili anche a loro le norme del Testo unico dei servizi di media audiovisivi e radiofonici (d. lgs. 8 novembre 2021, n. 208, **TUSMA**).

La versione definitiva delle Linee guida ed il Codice di condotta sono il risultato di un complesso percorso di co-regolamentazione, durato più di due anni ed articolato su due consultazioni pubbliche (avviate dalle delibere nn. [178/23/CONS](#) e [472/24/CONS](#)) ed un Tavolo tecnico ([delibera n. 7/24/CONS](#)), alle quali hanno partecipato attivamente anche le associazioni di categoria e gli stakeholder del settore digitale (v. in questa Rubrica, notizia n. 29 nel numero 2/2024 [2024/2(29)VP], in *PeM*, 2024, p. 754).

In particolare, dal confronto con gli operatori è emersa la necessità di introdurre alcune modifiche rispetto alla prima versione delle Linee guida (vedi sotto). La medesima delibera ha, inoltre, approvato il Codice di condotta per affiancare le Linee guida tenendo conto della peculiarità e novità del fenomeno.

Definizione di Influencer e ambito di applicazione

Le Linee guida ed il Codice di condotta si applicano esclusivamente agli influencer rilevanti, ovvero le persone fisiche o giuridiche che, anche tramite personaggi virtuali, diffondono contenuti al pubblico attraverso piattaforme digitali, in particolare i social media, e che possono avere un impatto significativo sul comportamento e sulle scelte di tale pubblico, in modalità analoga o comunque assimilabile a quella dei fornitori di servizi di media audiovisivi sotto la giurisdizione nazionale, laddove risultino possedere cumulativamente i seguenti requisiti:

- lo scopo principale del servizio offerto è la fornitura di contenuti digitali, ivi compresi i contenuti audiovisivi, creati, prodotti o selezionati dall'influencer e diffusi al pubblico – tramite un servizio di piattaforma di condivisione di video, di social media o di altro media che ne consenta la pubblicazione – che informano, intrattengono o istruiscono a fronte del pagamento di un corrispettivo in denaro (ivi compresi, a mero titolo esplicativo e non esaustivo, eventuali ricavi dai prodotti e/o servizi venduti) o in prodotti, servizi, benefici o qualsiasi altra utilità, o lucro;
- l'influencer ha la responsabilità editoriale sui contenuti stessi;



- il servizio raggiunge un numero significativo di utenti in Italia ed ha un impatto rilevante sul pubblico;
- il servizio offerto costituisce attività economica ai sensi degli articoli 56 e 57 del Trattato sul funzionamento dell'Unione Europea (TFUE) ed è caratterizzato da un legame stabile ed effettivo con l'economia italiana;
- raggiungono almeno 500.000 follower complessivi (dato rilevato nel trentesimo giorno antecedente all'invio del modulo di iscrizione all'elenco AGCOM – vedi sotto) o un numero di visualizzazioni medie mensili pari a un milione (dato riferito ai sei mesi antecedenti il giorno dell'invio del modulo) su almeno una delle piattaforme di social media o di condivisione video utilizzate.

Rispetto alla versione 2024 delle Linee guida, l'Autorità ha precisato la definizione di influencer ed ha modificato le metriche. Originariamente, infatti, l'influencer era rilevante se raggiungeva un milione di follower su tutte le piattaforme, pubblicava almeno 24 contenuti nell'anno precedente ed aveva un *engagement rate* del 2% negli ultimi sei mesi. Poiché tali requisiti rischiavano di non tener conto degli algoritmi di visualizzazione e circolazione dei contenuti di specifiche piattaforme, se ne è proposto un aggiornamento.

Se l'influencer non raggiunge la soglia di rilevanza, AGCOM presume un'attività meno strutturata e applica solo alcune regole generali: protezione dei minori da contenuti dannosi e del pubblico da materiale che inciti violenza, odio o costituisca reato.

L'elenco degli influencer rilevanti.

La delibera n. 197/25/CONS istituisce un "*Elenco degli influencer rilevanti*" tenuto dall'Autorità, al quale gli influencer rilevanti dovranno registrarsi entro il mese di febbraio 2026, comunicando in un [modulo telematico](#) le proprie generalità (nome e cognome, ragione sociale e nickname), il link al proprio sito/pagina/piattaforma/account, il valore delle metriche su ciascuna piattaforma o social media ed un proprio recapito. L'elenco sarà pubblicato entro il mese di luglio 2026 ed aggiornato dall'Autorità ogni sei mesi. I soggetti interessati hanno quindici giorni dalla data di pubblicazione dell'elenco per presentare obiezione al proprio inserimento, per formulare richiesta di inserimento nello stesso o per chiedere la rettifica di informazioni inesatte. Trascorso tale intervallo di tempo, l'elenco è ritenuto definitivo.

Il modulo va inviato non appena si acquisisce lo status di influencer rilevante. Inoltre, gli influencer sono tenuti a notificare all'Autorità qualsiasi cambiamento di stato, così da permettere l'aggiornamento semestrale dell'elenco. Il mancato invio del modulo è sanzionato con una somma compresa fra 516 e 103.200 euro.

Si noti il valore dichiarativo dell'iscrizione all'elenco: gli influencer qualificabili come rilevanti sono tenuti al rispetto delle Linee guida e del Codice di condotta, a prescindere dal loro inserimento nell'elenco.

L'inserimento nell'elenco Agcom obbliga l'influencer rilevante ad indicare le generalità sul proprio profilo, nonché ad inserire la dicitura "*in elenco AGCOM*" o, nel caso di influencer virtuale, "*soggetto virtuale in elenco AGCOM*" nel proprio contenuto (cd. "*riconoscibilità degli influencer*").

Obblighi e principi fondamentali.

I contenuti diffusi dagli influencer rilevanti devono rispettare principi e obblighi contenuti nel TUSMA, quali:

- i principi generali del sistema dei servizi di media audiovisivi e della radiofonia ex art. 4(1) TUSMA, quali:
 - a) libertà e pluralismo dei mezzi di comunicazione radiotelevisiva;
 - b) libertà di espressione di ogni individuo, inclusa la libertà di opinione e quella di ricevere o di comunicare informazioni o idee senza limiti di frontiere, nel rispetto della dignità umana, del principio di non discriminazione e di contrasto ai discorsi d'odio;
 - c) obiettività, completezza, lealtà e imparzialità dell'informazione;
 - d) contrasto alle strategie di disinformazione;
 - e) tutela dei diritti d'autore e di proprietà intellettuale;
 - f) apertura alle diverse opinioni e tendenze politiche, sociali, culturali e religiose;
 - g) salvaguardia delle diversità etniche e del patrimonio culturale, artistico e ambientale, in ambito nazionale e locale, nel rispetto delle libertà e dei diritti, in particolare della dignità della persona e della protezione dei dati personali, della promozione e tutela del benessere, della salute e dell'armonico sviluppo fisico, psichico e morale del minore, garantiti dalla Costituzione, dal diritto dell'Unione europea, dalle norme internazionali vigenti nell'ordinamento italiano e dalle leggi statali e regionali;
 - h) contrasto alla tendenza contemporanea di distruggere o comunque ridimensionare gli elementi o simboli della storia e della tradizione della Nazione (*cancel culture*);
- l'art. 6(2)(a) TUSMA, sulla presentazione veritiera dei fatti e degli avvenimenti, in modo tale da favorire la libera formazione delle opinioni;
- le disposizioni a tutela del diritto d'autore richiamate nell'art. 32 TUSMA;
- le disposizioni a tutela dei diritti fondamentali della persona, dei minori e dei valori dello sport di cui agli articoli 30, 37, 38 e 39 TUSMA;
- le disposizioni in materia di comunicazioni commerciali di cui agli articoli 43, 46, 47 e 48 TUSMA.
- tutte le delibere AGCOM attuative delle disposizioni di cui sopra.

Le Linee guida, inoltre, dispongono esplicitamente che i contenuti prodotti dagli influencer:

- non devono contenere alcuna istigazione o provocazione a commettere reati ovvero apologia degli stessi;
- devono garantire il rispetto della dignità umana;
- non devono pubblicare contenuti o espressioni suscettibili di diffondere, incitare, propagandare oppure giustificare, minimizzare o in altro modo legittimare la violenza, l'odio o la discriminazione e offendere la dignità umana (cd. "*hate speech*");
- non devono contenere elementi suscettibili di determinare la deresponsabilizzazione dell'autore o la corresponsabilizzazione della



vittima di violenza, odio, di discriminazione o di lesione della dignità umana o di qualsiasi altra forma di vittimizzazione secondaria.

Ulteriori prescrizioni sono contenute nel Codice di condotta; tra le più importanti si ricordano:

- il divieto di sfruttamento di inesperienza o credulità o fiducia del pubblico (par. 3.2 Codice di condotta);
- il caso di filtri e altri meccanismi di modifica dei contenuti (par. 3.3 Codice di condotta). Se i contenuti social sono modificati tramite utilizzo di filtri e/o applicazioni software in misura tale da incidere potenzialmente sullo sviluppo dei minori, diffondendo modelli irrealistici e/o promuovendo prodotti e servizi che fanno ipotizzare prestazioni ed effetti non coerenti con le loro caratteristiche, l'influencer è tenuto a segnalarlo con una specifica dicitura, eventualmente da inserire come *hashtag*.

Norme particolari sulla tutela dei minori

I contenuti diffusi dagli influencer devono rispettare le norme in tema di tutela dei minori assicurando di non pubblicare contenuti gravemente nocivi al loro sviluppo fisico, psichico o morale. Il Codice di condotta:

- prevede che l'influencer non arrechi pregiudizio al decoro o alla reputazione dei minori esposti nei contenuti distribuiti dagli influencer;
- individua i criteri per la classificazione dei contenuti gravemente nocivi per i minori sulla base di aree tematiche di classificazione quali violenza, sesso, diritti fondamentali e incolumità della persona;
- prevede che la pubblicità di bevande alcoliche non sia specificamente rivolta ai minori e non ne incoraggi un consumo smodato. In particolare, gli influencer si impegnano ad utilizzare tutti gli strumenti ad oggi messi a disposizione dalle piattaforme di condivisione di video e dai social media per limitare l'accesso a tali contenuti da parte dei minori almeno per il periodo immediatamente successivo alla pubblicazione, dovendosi con ciò intendere almeno sette giorni dalla fine della campagna.

Le disposizioni sulla comunicazione commerciale

Le Linee guida ed il Codice di condotta prevedono che gli influencer rilevanti applichino le regole contenute nel [Regolamento Digital Chart](#) dell'Istituto di Autodisciplina Pubblicitaria (IAP) sulla riconoscibilità della comunicazione commerciale (**Regolamento IAP Digital Chart**).

Nel caso di rapporto di committenza tra brand e influencer (*Endorsement*) per il quale l'influencer riceve un corrispettivo, il Regolamento prevede l'obbligo di inserire nei contenuti diciture di agevole leggibilità (anche *hashtag*) come “pubblicità” o “advertising” (o, in alternativa, “promosso da ... brand” o “promoted by ... brand”, “sponsorizzato da ... brand” o “sponsored by ... brand”, “adv/ad+ brand”) in ogni contenuto commerciale. Nei video, la dicitura deve essere presente sia nella descrizione sia in sovrimpressione nelle scene iniziali, mentre nei contenuti a scadenza (*Stories*) deve essere ben visibile sugli elementi visivi. Così, anche in caso di invio di prodotti o inviti a eventi senza rapporto di committenza, è necessario inserire disclaimer specifici (“prodotto inviato da ... brand”, “product gifted by ... brand”,

“product sent by ... brand”, “invitato/a da ... brand”/“invited by ... brand”). Regole analoghe sono previste anche per i casi di “Tool”, Codici sconto, Autopromozioni, “In-feed Units”, “Paid search units”, “Recommendation widgets”, “In-App advertising”, “Advergame”, su cui si rimanda al Regolamento IAP Digital Chart. Anche agli influencer si applicano le regole riguardanti le sponsorizzazioni e televendite, al fine di rendere sempre chiara la natura commerciale dei contenuti proposti.

Gli influencer sono tenuti al rispetto del divieto assoluto di comunicazione commerciale per:

- sigarette ed altri prodotti a base di tabacco o contenenti nicotina, inclusi i prodotti di nuova generazione;
- gioco d'azzardo;
- medicinali e cure mediche che, nel territorio italiano, si possono ottenere unicamente su prescrizione medica.

Vigilanza e sanzioni.

La delibera n. 197/25/CONS ha ritenuto di confermare l'operatività del Tavolo tecnico istituito dalla delibera n. 7/24/CONS, che ora avrà la funzione di monitorare il fenomeno dell'*Influencer marketing*, valutare l'adeguatezza delle soglie e metriche previste nelle Linee guida, pianificare ed organizzare campagne formative e di informazione, elaborare proposte di revisione del Codice di condotta.

Parallelamente, l'Autorità svolgerà una funzione di vigilanza e sanzione per verificare l'osservanza delle condotte degli influencer al Tusma, alle Linee guida, al Codice di condotta e alle delibere attuative dell'Autorità. Il relativo procedimento sanzionatorio può essere avviato d'ufficio o su segnalazione dei soggetti interessati e delle associazioni od organizzazioni rappresentative dei loro interessi, trasmettendo apposita istanza per via telematica. Nel corso del procedimento l'Autorità può anche acquisire ogni elemento necessario, attraverso ispezioni, richieste di informazioni e documenti, audizioni e segnalazioni. Le sanzioni per la violazione delle disposizioni possono variare da 10.329 a 258.228 euro, con importi fino a 600.000 euro in caso di violazione delle disposizioni a tutela dei minori.

GIORGIO GIULIANO*

Funzionario AGCOM

*Le opinioni o i punti di vista espressi sono esclusivamente dell'autore e non dell'istituzione

2025/4(30)RMa-MCG

Le “Linee guida per l'implementazione dell'Intelligenza Artificiale nel mondo del lavoro” adottate con decreto del Ministro del lavoro e delle politiche sociali n. 180 del 17.12.2025

Con il decreto ministeriale n. 180 del 17 dicembre 2025 (il **Decreto**) il Ministro del Lavoro e delle Politiche Sociali (il **Ministro**) ha adottato le “Linee guida per l'implementazione dell'Intelligenza Artificiale nel mondo del lavoro” (le **Linee guida**), al fine di corrispondere ad alcune necessità di

chiarimento avvertite dalle imprese e dai lavoratori in una fase di profonda trasformazione del mercato occupazionale in conseguenza della diffusione di sistemi di IA nel mondo del lavoro. Il Decreto si inserisce nel solco tracciato dal regolamento (UE) 2024/1689 (**AI Act**) e dalla legge 132/2025 e promuove un utilizzo dell'intelligenza artificiale consapevole, responsabile e antropocentrico.

Le Linee guida non introducono nuovi obblighi giuridici, ma offrono un quadro di riferimento pratico e operativo. In particolare, nelle Linee guida vengono individuate tre aree di intervento prioritarie per governare l'impatto dell'intelligenza artificiale nei luoghi di lavoro:

- formazione e sviluppo delle competenze, attraverso percorsi di *upskilling* e *reskilling*;
- tutela dei lavoratori, con particolare attenzione alla prevenzione delle discriminazioni algoritmiche, alla protezione dei dati personali e alla supervisione umana dei sistemi automatizzati;
- riduzione del divario digitale, per evitare che l'intelligenza artificiale amplifichi disuguaglianze territoriali, generazionali o sociali.

Particolare attenzione è riservata alle piccole e medie imprese, per le quali le Linee guida delineano un percorso graduale di adozione dell'intelligenza artificiale. Si parte dalla valutazione preliminare della maturità digitale dell'organizzazione (AI Readiness), per poi passare alla pianificazione strategica e alla definizione di una *governance* conforme al quadro normativo. Seguono la sperimentazione attraverso progetti pilota per testare le soluzioni in ambienti controllati, l'implementazione progressiva delle soluzioni nelle organizzazioni aziendali, il monitoraggio continuo dei rischi e, come filo conduttore di tutto il processo, la valorizzazione del capitale umano attraverso investimenti continui nella formazione.

Orbene, proprio la formazione rappresenta uno dei pilastri del documento. La diffusione dell'intelligenza artificiale rende infatti sempre più necessario il ricorso a percorsi di aggiornamento costanti, al fine di prevenire il rischio di esclusione tecnologica e ridurre il divario tra chi è in grado di utilizzare efficacemente le nuove tecnologie e chi incontra maggiori difficoltà di adattamento. Secondo il World Economic Forum, entro il 2030 quattro lavoratori su dieci dovranno rafforzare le proprie competenze per rimanere occupabili. In questo scenario, le imprese sono chiamate a investire nell'*upskilling* e nel *reskilling* del personale, mentre i lavoratori devono essere sostenuti con percorsi formativi accessibili e mirati.

A sostegno della transizione digitale, le Linee guida richiamano diversi incentivi e strumenti di finanziamento, tra cui il Fondo Nuove Competenze, il Piano Transizione 5.0 e programmi europei come InvestAI, Horizon Europe e il Fondo Sociale Europeo Plus (FSE+).

Un altro principio cardine delle Linee guida è quello della supervisione umana. L'intelligenza artificiale non può, infatti, trasformarsi in una "scatola nera" che incide in modo opaco su decisioni cruciali come assunzioni, valutazioni, promozioni o licenziamenti. I sistemi automatizzati devono essere trasparenti, comprensibili e verificabili, e le decisioni devono poter essere contestate. Inoltre, le Linee guida richiamano espressamente il rischio

di discriminazioni algoritmiche, che possono derivare da *dataset* distorti o da modelli non adeguatamente supervisionati.

Viene dedicata attenzione anche ai lavoratori autonomi, per i quali l'IA rappresenta al tempo stesso un'opportunità e una sfida. Se da un lato, infatti, l'automazione può aumentare l'efficienza e ridurre i carichi amministrativi, dall'altro emergono criticità legate alla dipendenza dalle piattaforme digitali e alla tutela della proprietà intellettuale. In quest'ottica, le Linee guida suggeriscono di favorire l'accesso a soluzioni *open source* e la creazione di reti di supporto tra lavoratori autonomi, per rendere l'innovazione più inclusiva.

Le Linee guida sono concepite come un testo dinamico, destinato a essere aggiornato nel tempo dall'[Osservatorio sull'adozione dei sistemi di IA nel mondo del lavoro](#), previsto dalla legge 132/2025. L'Osservatorio avrà il compito di monitorare l'impatto dell'IA su occupazione, diritti e organizzazione del lavoro, assicurando che lo sviluppo tecnologico resti coerente con un modello di *governance* partecipato e realmente incentrato sulla persona.

RICCARDO MARAGA-MARIA CHIARA GAROFALO

<https://www.lavoro.gov.it/documenti-e-norme/normativa/decreto-ministeriale-n-180-del-17122025>

<https://www.lavoro.gov.it/osservatorio-adozione-sistemi-intelligenza-artificiale/pagine/normative>

2025/4(31)FDA

La sentenza del TAR Lombardia, Sez. V, 21 ottobre 2025, n. 3348 e la segnalazione al Consiglio dell'Ordine degli Avvocati competente per l'accertamento della responsabilità disciplinare del professionista che si avvale dell'attività di collaboratori o di applicazioni di intelligenza artificiale senza verificare l'esito delle ricerche

La sentenza del TAR Lombardia, Sez. V, 21 ottobre 2025, n. 3348 è degna di nota non tanto per la questione sostanziale decisa dal collegio (conferma del giudizio di non ammissione di un studentessa liceale alla classe successiva), quanto per la delineazione di una possibile responsabilità disciplinare per violazione dei doveri deontologici incombenti sul legale della parte ricorrente (deferimento al consiglio locale dell'Ordine degli Avvocati ai sensi dell'art. 88 c.p.c.) colpevole di aver utilizzato un programma d'intelligenza artificiale per redigere l'atto difensivo senza aver poi verificato la correttezza delle citazioni giurisprudenziali trascritte nel documento elaborato dal calcolatore informatico.

Nello specifico la pronuncia ha preso atto che nel «ricorso tutte le sentenze citate a sostegno dell'affermazione dell'illegittimità dei provvedimenti impugnati richiamano estremi di pronunce non pertinenti e le massime indicate in molti casi sono riferibili ad orientamenti giurisprudenziali non noti»; e a nulla può valere la giustificazione orale addotta dallo stesso legale



in udienza e poi verbalizzata di «aver citato nel ricorso della giurisprudenza reperita mediante strumenti di ricerca basati sull'intelligenza artificiale che hanno generato risultati errati».

Secondo il giudice milanese tale condotta processuale costituisce una chiara «violazione del dovere del difensore di comportarsi in giudizio con lealtà e probità, in quanto introduce elementi potenzialmente idonei ad influenzare il contraddittorio processuale e la fase decisoria verso un percorso non corretto»; e poi «rende inutilmente gravosa, da parte del giudice e delle controparti, l'attività di controllo della giurisprudenza citata e dei principi dalla stessa apparentemente affermati».

Un simile comportamento dell'avvocato non può essere scusato in quanto la «sottoscrizione degli atti processuali ha la funzione di attribuire la responsabilità degli esiti degli scritti difensivi al sottoscrittore indipendentemente dalla circostanza che questi li abbia redatti personalmente o avvalendosi dell'attività di propri collaboratori o di strumenti di intelligenza artificiale»; e ciò tanto più dinanzi a possibili «risultati errati» del sistema esperto «comunemente qualificati come “allucinazioni da intelligenza artificiale”, che si verificano quando tali sistemi inventano risultati inesistenti ma apparentemente coerenti con il tema trattato».

A imporlo, secondo il giudice amministrativo, è il «principio della centralità della decisione umana» (ora espressamente sancito anche per l'attività forense dall'art. 13(1) della legge 23 settembre 2025, n. 132: «l'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera») che intesta all'avvocato un «onere di verifica e controllo dell'esito delle ricerche effettuate con i sistemi di intelligenza artificiale».

Per tutti questi motivi, la sentenza, tra le altre statuizioni, ha ordinato alla Segreteria della Sezione di trasmettere copia della medesima sentenza all'Ordine degli Avvocati di Milano per le valutazioni di competenza indicate in motivazione.

FILIPPO D'ANGELO

<https://www.giustizia-amministrativa.it/web/guest/dcsnpr>

2025/4(32)DI

Pubblicato lo studio dell'agenzia ministeriale francese ANSES sugli effetti dell'uso dei social network sulla salute degli adolescenti

Il 13 gennaio 2026 è stato pubblicato il lavoro di expertise dell'agenzia ministeriale francese ANSES (*Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail*) circa gli effetti dell'uso dei social network sulla salute degli adolescenti: *rapport sur les usages des réseaux sociaux numériques et santé des adolescents* (il **rapport**). Il *rapport* è stato condotto da un gruppo multidisciplinare di esperti (epidemiologi, biologi, psichiatri infantili, psicologi, giuristi e ricercatori nel campo delle

scienze dell'informazione e della comunicazione) e si basa sull'esame di una elevata quantità (oltre mille) di studi scientifici sugli effetti dei social network sulla salute.

Dopo avere dimostrato come il modello di funzionamento dei social network si basi sulla raccolta di dati prodotti dalla navigazione dell'utente e dunque cerchi di massimizzare il tempo che ciascuno trascorre su quello schermo, il *rapport* mette in luce i numerosi fattori di rischio per la salute che un massiccio utilizzo di social media può determinare per gli adolescenti nel campo della salute mentale. Innanzitutto, si registra come una prolungata navigazione su social network ritardi l'addormentamento, determini delle alterazioni del sonno e in generale ne peggiori la qualità. Ciò comporta a sua volta sonnolenza, irritabilità, tristezza durante il giorno e può favorire sintomi depressivi. In secondo luogo, il *rapport* ha esaminato un secondo effetto causato dall'utilizzo eccessivo di social network e che è costituito dalla devalorizzazione di sé e della propria immagine corporea. Per un verso, l'anonimato e la facilità di diffusione delle minacce amplificano il coinvolgimento e, per altro verso, l'esposizione alla violenza (come nel caso di cyberbullismo, insulti, voci, esclusione, ricatti o diffusione di immagini intime senza consenso) costituisce un terreno fertile per l'insorgenza di sintomi depressivi. Inoltre, l'analisi della letteratura scientifica prodotta in questi anni mostra come l'utilizzo massiccio dei social network abbia un impatto maggiore sulle ragazze rispetto ai ragazzi. Le prime vi passano più tempo, sono più spesso vittime di violenza on-line, condividono con maggiore frequenza contenuti che le rappresentano e sembrano risultare maggiormente vulnerabili allo scambio di contenuti visivi incentrati sull'aspetto fisico. Tale utilizzo dei social network può alterare l'immagine che si ha del proprio corpo e, considerate anche i *bias* di genere e la pressione sociale che spinge a conformarsi a ideali fisici, può esacerbare i disturbi alimentari.

Il *rapport* contiene anche una analisi del dato normativo esistente e suggerisce delle linee d'azione per proteggere gli adolescenti dagli effetti della sovraesposizione ai social network. Innanzitutto, si raccomanda che i minori possano accedere solo a social network progettati e configurati al fine di proteggere la loro salute. In tal senso si sottolinea l'importanza dell'applicazione del limite di età previsto dal GDPR per impedire l'accesso ai social network ai minori di 13 anni, con sistemi affidabili di verifica dell'età e di raccolta del consenso dei genitori nonché l'opportunità di una revisione approfondita dei principi di funzionamento dei social network. Mediante un puntuale richiamo ai dati normativi esistenti, il *rapport* ribadisce il divieto di ricorrere a tecniche di interfaccia manipolative, di diffusione di contenuti dannosi per la salute (comportamenti a rischio, giochi d'azzardo, diete estreme, contenuti violenti, pornografici, che incitano all'odio, molestie, ecc.), nonché la necessità di regolamentare e limitare gli strumenti destinati ad aumentare, mantenere o estendere l'utilizzo del servizio da parte dell'utente.

DANIELE IMBRUGLIA

Report: <https://shorturl.at/opEEj>

2025/4(33)CI

La sanzione di oltre 98 milioni di euro irrogata dall'AGCM ad Apple il 16.12.2025 per abuso di posizione dominante in relazione alla policy App Tracking Transparency

| 1130

Con il [provvedimento n. 31772 del 16 dicembre 2025](#), l'Autorità Garante della Concorrenza e del Mercato (AGCM) ha irrogato alle società Apple Inc., Apple Distribution International Ltd e Apple Italia S.r.l. (collettivamente **Apple**) una sanzione pari a 98.635.416,67 euro per abuso di posizione dominante, in violazione dell'art. 102 del Trattato sul Funzionamento dell'Unione Europea (TFUE), nel mercato della fornitura agli sviluppatori di piattaforme per la distribuzione online di applicazioni destinate agli utenti del sistema operativo iOS.

La decisione è stata adottata al termine di un procedimento istruttorio complesso, avviato il 2 maggio 2023, volto ad accertare la compatibilità con le norme in materia di concorrenza della policy *App Tracking Transparency* (ATT), introdotta da Apple a partire dal 2021. Tale policy consiste in un insieme di regole che disciplinano le condizioni di accesso all'*Identifier for Advertisers* (IDFA), una funzionalità del sistema operativo iOS che, attraverso l'attribuzione di un codice univoco a ciascun dispositivo Apple, consente di riconoscere lo stesso dispositivo all'interno di applicazioni diverse e di collegarne le attività. In particolare, Apple ha strutturato l'ATT in modo da subordinare l'accesso all>IDFA, da parte degli sviluppatori terzi, alla previa acquisizione del consenso degli utenti al tracciamento a fini pubblicitari, mediante una schermata standardizzata predisposta unilateralmente dalla società (c.d. *ATT prompt*) e imposta come condizione tecnica per l'utilizzo della funzionalità. Apple ha giustificato l'introduzione dell'ATT richiamando l'esigenza di rafforzare la tutela della privacy degli utenti, sostenendo che la policy rispondeva a una crescente domanda di trasparenza e di controllo sull'utilizzo dei dati personali e che la richiesta di un consenso espresso tramite l'ATT prompt fosse funzionale ad assicurare che il collegamento dei dati a fini pubblicitari avvenisse in modo libero, specifico e informato, in linea con i principi del GDPR e della Direttiva ePrivacy.

Con il provvedimento in commento, l'AGCM ha tuttavia ritenuto che tale condotta integrasse un abuso di posizione dominante ai sensi dell'art. 102 lett. a) TFUE, disposizione che vieta all'impresa in posizione dominante di imporre condizioni non eque nei rapporti commerciali, anche in assenza di effetti escludenti sul mercato («imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque»). Il nucleo dell'illiceità è stato individuato nell'imposizione, agli sviluppatori terzi, di oneri aggiuntivi e non giustificati, consistenti nella duplicazione della richiesta di consenso degli utenti al trattamento dei dati personali quale condizione per l'accesso all>IDFA.

Nel corso del procedimento è emerso che gli sviluppatori erano già tenuti, in forza del regolamento (UE) 2016/679 (GDPR), a raccogliere un valido consenso mediante propri strumenti di raccolta, anche per i trattamenti

effettuati a fini pubblicitari, e che l'*ATT prompt* non risultava, da solo, idoneo a soddisfare i requisiti di validità del consenso richiesti dalla disciplina applicabile. Gli sviluppatori restavano pertanto obbligati a mantenere i propri strumenti, con la conseguenza di sottoporre gli utenti a una duplice richiesta di consenso nel solo ambiente iOS.

Tale assetto ha prodotto effetti negativi sia in termini di complessità operativa sia in termini di riduzione dei tassi di accettazione del tracciamento, incidendo direttamente sulle condizioni economiche e operative dell'attività degli sviluppatori e, in particolare, sulla loro capacità di accedere ai dati necessari alla monetizzazione delle applicazioni.

L'impatto economico dell'ATT risulta particolarmente evidente alla luce della funzione svolta dall'IDFA nell'ecosistema delle applicazioni distribuite online. Una parte significativa di tali applicazioni è infatti offerta gratuitamente agli utenti e si fonda su modelli di business incentrati sulla vendita di spazi pubblicitari. Nel mercato del *mobile advertising*, gli inserzionisti privilegiano forme di pubblicità *in-app* mirata, idonee a raggiungere specifici segmenti di utenti e a consentire una misurazione affidabile delle performance delle campagne. In tale contesto, la possibilità di identificare lo stesso utente su più applicazioni mediante l'IDFA assume un ruolo centrale, se non addirittura un presupposto, per la sostenibilità economica di tali modelli di business.

Ai fini della valutazione della giustificazione addotta da Apple, l'AGCM ha richiamato il principio, consolidato nella giurisprudenza relativa all'art. 102 TFUE, secondo cui un'impresa in posizione dominante è gravata da una speciale responsabilità di non compromettere il corretto funzionamento del mercato, anche quando persegua obiettivi in sé legittimi. Su tale base, la condotta è stata sottoposta a un test di proporzionalità, volto a verificare se le modalità concretamente adottate per rafforzare la tutela della privacy, obiettivo non contestato in quanto tale, fossero necessarie e adeguate rispetto agli effetti prodotti.

L'Autorità è giunta a una conclusione negativa, ritenendo che l'imposizione unilaterale dell'ATT e la conseguente duplicazione della richiesta di consenso eccedessero quanto strettamente necessario per la protezione dei dati personali. A sostegno di tale conclusione, il provvedimento ha valorizzato il parere del Garante per la protezione dei dati personali del 4 agosto 2025, secondo cui la policy adottata da Apple non costituiva l'adempimento di specifici obblighi normativi gravanti sulla società e la duplicazione del consenso risultava "non necessaria" alla luce della normativa vigente, in quanto riconducibile a una scelta imprenditoriale discrezionale. La duplicazione della richiesta di consenso è stata pertanto qualificata come una condizione non equa, in quanto trasferiva sugli sviluppatori il costo economico e funzionale di tale scelta, senza un'adeguata giustificazione rispetto all'obiettivo perseguito.

Quanto al profilo probatorio, l'Autorità ha ribadito che, ai fini della configurabilità dell'abuso, non era necessario dimostrare l'esistenza di un danno attuale e quantificabile, essendo sufficiente l'idoneità della condotta a produrre un pregiudizio concorrenziale. Ciò nondimeno, il provvedimento ha ricostruito anche una serie di effetti concreti riconducibili all'ATT, tra cui la

riduzione dei tassi di consenso alla profilazione per gli sviluppatori terzi, la conseguente minore disponibilità di dati utilizzabili per il targeting, la perdita di valore degli spazi pubblicitari e l'aumento dei costi per gli inserzionisti, effetti risultati particolarmente marcati per gli operatori di minori dimensioni. Parallelamente, l'AGCM ha evidenziato come l'assetto delineato dall'ATT fosse idoneo a produrre vantaggi competitivi indiretti per Apple nei mercati collegati, in particolare con riferimento alle proprie attività pubblicitarie e ai servizi integrati nell'App Store. In un contesto caratterizzato da una forte asimmetria regolatoria e informativa, la compressione della capacità di monetizzazione degli sviluppatori terzi è stata ritenuta suscettibile di rafforzare la posizione dell'impresa dominante lungo la catena del valore della pubblicità in-app.

Su tali basi, l'Autorità ha ordinato ad Apple di cessare immediatamente i comportamenti ritenuti distorsivi della concorrenza e di astenersi, per il futuro, dal porre in essere condotte analoghe o comunque idonee a produrre effetti equivalenti a quelli oggetto dell'infrazione accertata. Le società sono state altresì tenute a trasmettere all'Autorità, entro novanta giorni dalla notifica del provvedimento, una relazione dettagliata sulle misure adottate per conformarsi agli obblighi imposti. In ragione della gravità e della durata dell'infrazione, l'AGCM ha infine irrogato alle medesime società, in solido tra loro, una sanzione amministrativa pecuniaria complessiva pari a euro 98.635.416,67.

CECILIA ISOLA

https://www.agcm.it/dotcmsdoc/allegati-news/A561_chiusura.pdf

2025/4(34)FZ

Il primo provvedimento AGCOM del 6.11.2025 di diffida ai sensi del regolamento UE Platform-to-business (caso Refurbed)

La recente iniziativa dell'Autorità per le garanzie nelle comunicazioni (**AGCOM** o l'**Autorità**) nei confronti di Refurbed Marketplace GmbH (**Refurbed**), segna un passaggio di rilievo nell'attuazione del regolamento (UE) 2019/1150 (**regolamento P2B**) sul rapporto tra piattaforme digitali e business, rappresentando la prima applicazione formale in Italia del regolamento P2B e offrendo un'interessante chiave di lettura sull'evoluzione dei principi di trasparenza nel mercato digitale.

La [delibera AGCOM n. 263/25/CONS](#) del 6 novembre 2025, con cui l'Autorità ha intimato a Refurbed, società attiva nel settore della vendita di dispositivi ricondizionati, di **adeguare le proprie condizioni generali d'uso** – giudicate non conformi agli obblighi di trasparenza previsti dal regolamento P2B – muove dalla constatazione di una persistente asimmetria strutturale tra piattaforme online/intermediari digitali, normalmente dotati di un potere contrattuale elevato e di capacità tecnologiche avanzate, e imprese (tendenzialmente PMI), in un contesto economico in cui la visibilità *online* e

l'accesso ai dati assumono un valore competitivo spesso superiore al prezzo o alla qualità del prodotto.

A seguito di una scrupolosa istruttoria, l'AGCOM ha constatato che Refurbed non rispettava una serie di obblighi fondamentali previsti dal sopracitato regolamento P2B.

In particolare, l'Autorità ha rilevato una prima criticità significativa nella comunicazione dei **criteri di posizionamento dei prodotti e delle offerte**, giudicata insufficiente a consentire ai venditori di comprendere se, e in che misura, il *ranking* dipendesse da fattori quali (i) la qualità delle recensioni, (ii) le *performance* logistiche, (iii) la competitività del prezzo o (iv) eventuali accordi commerciali, con il rischio di generare effetti distorsivi e potenzialmente discriminatori.

Ulteriori profili problematici sono emersi in relazione alla **gestione dei dati generati dall'attività degli utenti business**, rispetto ai quali la piattaforma non forniva indicazioni chiare né sulle modalità di raccolta, né sulle possibilità di accesso e riutilizzo, in contrasto con l'obiettivo del regolamento P2B di impedire un uso unilateralmente vantaggioso delle informazioni da parte delle piattaforme.

A ciò si aggiunge la carenza di procedure strutturate e trasparenti per la **gestione dei reclami**, elemento che, specie nei casi di penalizzazioni o sospensioni algoritmiche delle offerte, accentua l'incertezza operativa delle imprese e rafforza l'asimmetria di potere contrattuale.

La vicenda si inserisce in un contesto già interessato da [segnalazioni di associazioni di consumatori](#) e da iniziative avviate innanzi all'Autorità garante della concorrenza e del mercato (AGCM), confermando come le pratiche delle piattaforme siano sempre più oggetto di scrutinio incrociato sotto il profilo della correttezza commerciale e della trasparenza informativa. Sul piano sistemico, la diffida assume un valore che va ben oltre il caso concreto, chiarendo l'approccio interpretativo dell'Autorità al regolamento P2B, e ribadisce che gli obblighi informativi non possono esaurirsi in documenti formalmente completi ma sostanzialmente opachi, dovendo invece necessariamente tradursi in informazioni effettivamente disponibili e comprensibili. In tale prospettiva, la trasparenza cessa di essere un adempimento marginale e si configura, altresì, quale requisito strutturale per il corretto funzionamento del mercato digitale, in linea con il più ampio processo di riforma europea che, attraverso il reg. (UE) 2022/1925 (Digital Markets Act, **DMA**) e il reg. (UE) 2022/2065 (Digital Services Act, **DSA**), mira a rendere intelligibili e controllabili le dinamiche algoritmiche anche al di fuori dei soli grandi *gatekeeper*.

Le prospettive aperte dalla delibera sono, pertanto, rilevanti: da un lato, l'avvio di un percorso di monitoraggio che potrebbe incidere sull'operato di numerose piattaforme attive nel mercato italiano; dall'altro, la conferma che la reale prova di conformità non risiede nella mera revisione delle condizioni contrattuali, bensì nella **modifica concreta dei processi interni e dei meccanismi decisionali**.

In un ecosistema digitale in cui dati e visibilità costituiscono *asset* economici primari, il rispetto delle regole di trasparenza diventa condizione imprescindibile per garantire livelli adeguati di concorrenza e fiducia,



favorendo al contempo un maggiore coordinamento tra autorità nazionali ed europee e contribuendo alla costruzione di un quadro regolatorio più coerente e meno frammentato.

La diffida nei confronti di Refurbed appare, dunque, come il segnale di una nuova fase, nella quale le piattaforme non possono più rivendicare un potere regolatorio unilaterale, ma sono chiamate a operare sotto un controllo più rigoroso e sistemico, capace di incidere concretamente sulla vita quotidiana delle imprese e sulla loro capacità di competere in modo equo nel mercato digitale.

FRANCESCA ZAMPONE

<https://www.agcom.it/provvedimenti/delibera-263-25-cons>

2025/4(35)ES

Pubblicato il d.lgs. n. 212 del 31.12.2025 di recepimento della direttiva (UE) 2023/2225 del relativa ai contratti di credito ai consumatori

Il 9 gennaio 2026 è stato pubblicato sulla Gazzetta Ufficiale il D. Lgs. 212 del 31 dicembre 2025 (il **Decreto**) che adegua l'ordinamento italiano alla dir. (UE) 2023/2225 relativa ai contratti di credito ai consumatori (la **Direttiva**). Il Decreto, in attuazione della Direttiva, contiene, tra le tante disposizioni, una serie di importanti norme in materia di trattamento di dati personali e di trattamento automatizzato (v. infra). Esso apporta diverse modifiche al d.lgs. 385/1993 (**Testo Unico Bancario** o **TUB**) e, in misura minore, al d.lgs. 141/2010, che aveva dato attuazione alla precedente direttiva in materia, la dir. 2008/48/CE. Il Decreto mira a incrementare la tutela del consumatore ampliando il novero delle fattispecie assoggettabili alla propria disciplina, rafforzando l'informativa precontrattuale, migliorando la qualità della normativa sul credito al consumo, intervenendo sul punto del trattamento dei dati personali del consumatore, e implementando l'educazione finanziaria e il finanziamento responsabile. Il fine ultimo è prevenire situazioni di difficoltà economico finanziaria del consumatore.

Come detto, il Decreto **amplia l'ambito di applicazione** della normativa sul credito al consumo modificando l'art. 122(1) TUB. In particolare, stabilisce che essa si applichi a tutti i finanziamenti fino a 100.000,00 €, e non più fino a 75.000,00 €, ed abroga le lett. c) e d) del medesimo art. 122(1) TUB che escludevano l'applicabilità della disciplina sul credito al consumo ai contratti di finanziamento di breve durata con costi bassi o nulli. In tali casi, piuttosto che non applicare nessuna disciplina, il legislatore ha ritenuto opportuno prevedere un regime di tutele semplificato e proporzionale al valore del credito concesso che sarà disciplinato nella normativa di rango secondario emanata dalla Banca d'Italia.

Il Decreto, poi, stabilisce che nell'ambito applicativo della normativa sul credito al consumo rientrano anche i pagamenti rateali, assai diffusi nella prassi commerciale, **i** “senza interessi o altre spese” eseguiti direttamente dal fornitore di beni o servizi senza l'intermediazione di terzi (art. 122(1)(i-

bis) TUB); ovvero ii) quelli in cui si prevede la cessione del credito contestuale alla dilazione di pagamento (art. 122(1)(i-ter) TUB).

La disciplina in commento, inoltre, stabilisce che non configura attività di intermediazione la mera presentazione di un consumatore ad un finanziatore svolta quale attività accessoria rispetto a quella principale esercitata da chi presenta il cliente.

Per quanto riguarda gli **obblighi di comportamento degli intermediari**, è inserito nel TUB l'art. 122-bis il quale prevede che l'operatore economico agisca con diligenza, correttezza e trasparenza *“tenendo conto dei diritti e degli interessi dei consumatori”*.

Il Decreto modifica anche l'art. 123(1) prevedendo che gli **annunci pubblicitari** non possano indurre in inganno i consumatori creando false aspettative; anzi, devono includere un avvertimento agli individui che prendere in prestito del denaro comporta dei costi. Non a caso, l'art. 123(2) TUB come modificato **vieta** la pubblicità che *“a) incoraggia i consumatori a chiedere credito suggerendo che il credito migliorerebbe la loro situazione finanziaria; b) precisa che i contratti di credito in essere o i crediti registrati nelle banche dati hanno un'influenza minima o nulla sulla valutazione di una richiesta di credito; c) suggerisce falsamente che il credito comporta un aumento delle risorse finanziarie, costituisce un sostituto del risparmio o può migliorare il tenore di vita del consumatore”*.

Viene modificato anche l'art. 124 TUB rafforzando l'informativa precontrattuale al fine di offrire al consumatore un quadro quanto più completo possibile prima di concludere un accordo. In particolare, il comma 1-bis specifica che il consumatore deve ricevere *“in tempo utile”* prima del perfezionamento del contratto, anche se concluso a distanza, un'informativa adeguata e, laddove tali informazioni siano fornite con poco preavviso rispetto alla conclusione del contratto, il finanziatore deve inviare al consumatore un promemoria sulla possibilità di recedere dal contratto di credito e sulla procedura da seguire. Le informazioni devono sempre essere chiare, complete, gratuite e su supporto durevole; in particolare, il promemoria deve essere inviato tra uno e sette giorni dopo la conclusione del contratto.

Il neo inserito art. 124.1 TUB ribadisce che *“è vietata ogni concessione di credito al consumatore senza **previa richiesta ed esplicito consenso** di questo”*; il consenso non può essere in alcun modo desunto, nemmeno *“tramite l'utilizzo di opzioni predefinite, incluse le caselle preselezionate”* e deve essere espresso in maniera libera, specifica, informata, inequivocabile.

L'art. 124.2 TUB, anch'esso inserito dal Decreto, stabilisce che nello svolgimento del servizio di **consulenza** gli intermediari non devono solo acquisire tutte le informazioni necessarie e aggiornate sulla situazione finanziaria, sugli obiettivi e sulle preferenze del consumatore, ma devono anche agire nel suo miglior interesse fornendogli le raccomandazioni di investimento più adeguate rispetto alla situazione finanziaria e ai bisogni di quest'ultimi; a tal fine, il Legislatore richiede all'intermediario di fornire indicazioni basandosi su un numero sufficientemente ampio di contratti di credito.



Ferme le esigenze di corretta gestione degli intermediari, la *ratio* della norma è svolgere una valutazione approfondita del merito creditizio del consumatore evitando situazioni di sovraindebitamento.

Particolarmente importanti sono le disposizioni in materia di **trattamento di dati personali e di trattamento automatizzato**.

Innanzitutto, è previsto (nuovo comma 6-bis dell'art. 24 TUB) che i finanziatori e gli intermediari del credito debbano informare i consumatori quando presentano loro un'offerta personalizzata basata sul trattamento dei dati personali (cfr. in termini analoghi, art. 49(1)(e-bis) codice del consumo, d.lgs. 206/2005).

In secondo luogo, la valutazione del merito creditizio deve essere eseguita prima dell'instaurazione del rapporto contrattuale, deve essere costantemente aggiornata e **non deve avvalersi dei dati di cui all'art. 9, par. 1 Reg. 2016/679/UE e delle informazioni reperibili sui social network**. Laddove essa avvenga, anche solo in parte, attraverso il **trattamento automatizzato** di dati personali del consumatore, l'art. 124-bis(2bis) TUB stabilisce che questi ha diritto di esprimere la propria opinione, e di ottenere una spiegazione e il c.d. intervento umano, ossia: *“a) una spiegazione chiara e comprensibile della valutazione del merito creditizio, compresi la logica e i rischi derivanti dal trattamento automatizzato dei dati personali nonché la rilevanza e gli effetti sulla decisione; b) esprimere la propria opinione al finanziatore; c) chiedere un riesame della valutazione del merito creditizio e della decisione relativa alla concessione del credito da parte del finanziatore”*. Il finanziatore, inoltre, deve comunicare tempestivamente e gratuitamente al consumatore la banca dati da cui sono state estratte le informazioni su cui è stata elaborata la decisione (art. 120 undecies.1 TUB). Coerentemente con il considerando n. 81 della Direttiva, il Decreto modifica anche l'art. 121 TUB istituendo un servizio di consulenza sul debito che consiste nel fornire assistenza personalizzata tecnica, giuridica o psicologica da parte di operatori professionali indipendenti.

Il Decreto, infine, introduce le seguenti ulteriori novità:

- accogliendo il principio di diritto di cui alla nota sentenza della Corte di Giustizia del 11 settembre 2019, C-383/18, c.d. “Lexitor”, si stabilisce che il consumatore può **rimborsare anticipatamente** in ogni momento, in tutto o in parte, l'importo del finanziamento e, in tal caso, ha diritto a una riduzione del costo totale del credito per la restante durata del contratto. In particolare, nel calcolare tale riduzione *“devono essere presi in considerazione tutti i costi posti a carico del consumatore dal finanziatore”* (art. 120 sexies, commi 1 e 1 bis);
- in caso di **recesso** da un contratto di fornitura di beni o servizi da parte del consumatore, si risolve anche il contratto di credito collegato (art. 125 ter, comma 2, let. a));
- coerentemente con quanto previsto dal considerando 63 della Direttiva, sono modificate alcune disposizioni sulla **riduzione o cancellazione di aperture in conto corrente e sconfinamento** (art. 120 octies.1);

- si implementa sia il ruolo dell'**Organismo Agenti e Mediatori** ("OAM"), sia la disciplina sui requisiti di professionalità e onorabilità dei finanziatori, modificando altresì il quadro sanzionatorio in materia di intermediazione finanziaria.

Il Decreto prevede che i finanziatori e gli intermediari del credito si adeguino alle suddette novità entro il 20 novembre 2026.

EMANUELE STABILE

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2026-01-09&atto.codiceRedazionale=26G00009&elenco30giorni=false

2025/4(36)TB

La nuova versione dello standard ISO/IEC 27701:2025 per la privacy

Nel mese di ottobre 2025 l'International Standard Organization (ISO) ha pubblicato la seconda edizione dello *standard* ISO/IEC 27701, relativo ai sistemi di gestione delle informazioni privacy (privacy information management system, **PIMS**).

Il principale cambiamento apportato dalla nuova edizione, che sostituisce la precedente versione pubblicata nel 2019, consiste nell'impostazione dello standard in questione come sistema autonomo di gestione delle informazioni, con un superamento della struttura che lo vedeva dipendere necessariamente dallo standard ISO/IEC 27001 sui sistemi di gestione delle informazioni.

L'edizione 2025 si propone quindi l'obiettivo di consentire alle organizzazioni di strutturare e certificare in modo autonomo il PIMS, integrandolo ed allineandolo solo eventualmente con altri standard come l'ISO/IEC 27001.

Il documento è caratterizzato da un approccio olistico - per molti versi simile a quello che ispira il regolamento (UE) 2016/679 (**GDPR**) - improntato alla progettazione degli aspetti rilevanti da un punto di vista organizzativo e tecnico prima che documentale, in una prospettiva di responsabilizzazione (accountability) che ciascuna organizzazione è chiamata a mettere a fuoco a seconda delle sue specifiche caratteristiche, onde poter dimostrare la propria conformità alle disposizioni normative applicabili e garantire il rispetto dei diritti degli interessati.

Il punto di partenza per l'adozione di un PIMS consiste nella comprensione del contesto operativo e dei ruoli che l'organizzazione assume in relazione ai trattamenti di dati personali in cui è coinvolta (titolare, contitolare, responsabile), nell'individuazione dei bisogni e delle necessità dei portatori di interessi rilevanti e nella determinazione del perimetro di applicazione del PIMS.

A questo scopo, la funzione chiave è rivestita dal top management, che è chiamato a definire una politica e degli obiettivi privacy in maniera coerente con le peculiarità dell'organizzazione, ripartendo in modo chiaro ruoli e responsabilità al suo interno tra soggetti in possesso delle necessarie



competenze, nonché garantendo la messa a disposizione di risorse adeguate a consentire l'efficace implementazione e la continua revisione in chiave migliorativa del PIMS.

Tra i pilastri portanti dello standard ISO/IEC 27701-2025 spiccano la progettazione di processi di valutazione dei rischi privacy e di mitigazione degli stessi a seconda dell'esito della valutazione; il mantenimento e l'aggiornamento della documentazione rilevante; la determinazione di metodi di monitoraggio, analisi, revisione e miglioramento; e la conduzione periodica di audit interni sulla conformità e sull'effettivo aggiornamento del PIMS.

Lo standard include degli allegati di natura normativa che riepilogano dei principali aspetti che le organizzazioni devono tenere in considerazione per le operazioni di trattamento dei dati personali a seconda che operino come titolari, contitolari o responsabili (Allegato A) e delle linee guida di implementazione degli stessi (Allegato B).

Sono inoltre inseriti ulteriori allegati di stampo informativo che si propongono di fornire una mappatura tra le indicazioni fornite nel documento ed i riferimenti rilevanti – ove presenti - all'interno dello standard ISO/IEC 29100 (Allegato C), del GDPR (Allegato D), degli standard ISO/IEC 27018 e ISO/IEC 29151 (Allegato E) e della precedente versione dello *standard* ISO/IEC 27701 (Allegato F).

Il documento non fornisce indicazioni pratiche sulle modalità e le tempistiche della transizione del meccanismo di certificazione rispetto alla versione precedente, che verranno verosimilmente fornite prossimamente dall'*International Accreditation Forum*.

TIMOTEO BUCCI

<https://www.iso.org/standard/27701>

2025/4(37)LC

Il provvedimento del Garante privacy italiano del 1.10.2025 di limitazione provvisoria del trattamento di dati personali relativi al servizio di IA generativa “Clothoff”

Il Garante per la protezione dei dati personali (**GPDP** o il **Garante**), con provvedimento n. 10174164 del 1° ottobre 2025, ha disposto in via d'urgenza e con effetto immediato (ai sensi dell'art. 5(8) del regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante) la limitazione provvisoria del trattamento dei dati personali degli utenti italiani nei confronti dell'app *Clothoff*, la cui società holding (la *AI/Robotics Venture Strategy 3 Ltd.*), titolare del trattamento dei dati, ha sede nelle Isole Vergini Britanniche. Tale applicazione offre un servizio di IA generativa che rende possibile, gratuitamente o a pagamento, la generazione di deep fake (creazione di immagini, audio e video attraverso strumenti di intelligenza artificiale, in modo da apparire falsamente autentici o veritieri) e, nella specie, di “deep nude”, ovvero la creazione artificiale di foto e video falsi di persone

ritratte in pose sessualmente esplicite o, addirittura, pornografiche, basandosi su immagini reali. Lo stesso sito esplicitamente dichiara: «*ClothOff offers a wide range of customization settings, including body shape, pose, and style adjustments*». Questo artificio consente a chiunque, compresi i minorenni (quali soggetti attivi), di creare immagini e realizzare video di questo tenore partendo da immagini, anche ritraenti minori (quali soggetti passivi), in assenza di qualsiasi previo accertamento che consenta di verificare il consenso eventualmente prestato della persona ritratta e senza apporre alcuna segnalazione o etichetta circa il carattere artificiale di foto e video in questione. L'azione del Garante, che ha avviato un'attività istruttoria più approfondita volta a contrastare tutte le applicazioni di nudificazione (c.d. nudifier), si è resa necessaria a causa degli elevati rischi che tali servizi possono comportare per i diritti e le libertà fondamentali, in particolare con riguardo alla tutela della dignità della persona, ai diritti di riservatezza e di protezione dei dati personali dei soggetti coinvolti in queste tipologie di trattamenti, specialmente laddove ad essere coinvolti siano minori e, dunque, soggetti vulnerabili. Le notizie di cronaca si moltiplicano e restituiscono un fenomeno che ha ormai i contorni di un vero e proprio allarme sociale. Prova ne è il moltiplicarsi oltreoceano dei “nudify tools”, che consentono all'utente di creare immagini esplicite a carattere pornografico, a partire da immagini di vita reale. Per contrastare tale fenomeno nell'ordinamento eurounitario vengono riconosciuti ampi poteri di *enforcement* alle *authorities* nazionali. In particolare, nel provvedimento in commento l'autorità competente italiana (il GPDP) ha fatto applicazione di due fondamentali plessi normativi del diritto europeo dei dati, segnatamente, il regolamento (UE) 2016/679 (GDPR) e il regolamento (UE) 2024/1689 (AI Act), del quale richiama in particolare i considerando 133 e 134 laddove stabiliscono che «i fornitori di sistemi di intelligenza artificiale devono integrare soluzioni tecniche che, attraverso strumenti affidabili, interoperabili ed efficaci, tenuto conto dello stato dell'arte, marchino gli *output* di tal che si comprenda chiaramente che si tratta di contenuti generati o manipolati da un sistema di IA e non da esseri umani». Ed aggiunge «[i]n particolare, nell'utilizzo di un sistema di IA volta a generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi, entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri (deep fake), debba essere reso noto in modo chiaro e distinto che il contenuto è stato creato o manipolato artificialmente etichettando di conseguenza gli *output* dell'IA e rivelandone l'origine artificiale». Nel merito, l'Autorità ha rilevato l'assenza di un atteggiamento proattivo volto concretamente ad escludere che il servizio reso possa costituire il punto di partenza per attività illecite a danno degli utenti e dei soggetti ritrattati, in particolare se minori di età, in violazione dei principi di correttezza e accountability. In particolare, la Società che gestisce *Clothoff*, in qualità di titolare del trattamento, vista l'oggettiva rischiosità del servizio, ha mancato di adottare misure pienamente efficaci per escludere: i) che soggetti minori di età possano usare *ClothOff* in qualità di utenti; e ii) che possano essere caricate immagini senza consenso, soprattutto quando riferite a minori di età. In questo senso, ricorda l'Autorità, è compito del prestatore del servizio implementare le misure, tecniche e organizzative, che gli

consentano una verifica effettiva sulla legittimità della raccolta e successivo trattamento dei dati, se del caso anche biometrici, riferiti a soggetti terzi ritratti nelle immagini caricate dagli utenti. Misure che, sebbene implementate attraverso il ricorso a watermark e banner sulle immagini prodotte, non sono risultate tuttavia adeguate e idonee a minimizzare i rischi insiti in tali attività.

LUCIO CASALINI

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10174164>

2025/4(38)SR

Il provvedimento del Garante privacy italiano del 10.7.2025 sul trattamento di dati personali di bambini da parte di un asilo nido. Alcune riflessioni sulla tutela della dignità dei minori e la tenuta del consenso genitoriale nell'era digitale.

Il provvedimento del Garante per la protezione dei dati personali (il **Garante** o l'**Autorità**) del 10 luglio 2025, doc.web n. 10162731 (la **Decisione**) riaccende il dibattito sul rapporto tra consenso genitoriale, tutela dei minori e ruolo delle autorità indipendenti nella regolazione dei diritti fondamentali. In particolare, la Decisione, che nasce dalla proposizione di un reclamo ai sensi dell'art. 77 del reg. (UE) 2016/679 (**GDPR**), solleva delle questioni circa la legittimità di un approccio che, di fatto, sembra ridimensionare la portata del consenso espresso dai genitori per il trattamento delle immagini dei figli minori, soprattutto in contesti educativi. La critica più forte si concentra sulla presunta tendenza dell'Autorità a sostituirsi alla famiglia nell'esercizio della responsabilità genitoriale, dando luogo ad una vera e propria interferenza pubblicistica nella sfera dei legami familiari che conduce ad una marginalizzazione della volontà genitoriale nel sistema di tutela del minore.

Il fatto concreto, alla base del reclamo proposto da un genitore, riguarda la condotta di un asilo nido in cui era stato installato un impianto di videosorveglianza finanziato da fondi regionali e che, secondo quanto emerso nel corso dell'accertamento, ha trattato e diffuso immagini di minori in modo non conforme alla disciplina sulla protezione dei dati personali. Inoltre, la struttura educativa subordinava l'iscrizione, e quindi l'erogazione del servizio educativo, alla prestazione del consenso al trattamento delle immagini.

Il Garante inquadra il suo intervento nell'ambito delle proprie competenze istituzionali di vigilanza sul rispetto della normativa in materia di protezione dei dati personali, con specifico riferimento ai trattamenti che coinvolgono soggetti minori di età.

Un primo profilo analizzato riguarda il contenuto delle **informative** consegnate ai genitori dei minori in fase di iscrizione. L'Autorità ha verificato se esse fossero redatte in modo chiaro, comprensibile e specifico, con particolare attenzione alla distinzione tra le diverse finalità del trattamento. Dall'istruttoria è emerso che le informative tendevano a ricomprendere, in

modo unitario, sia finalità strettamente funzionali all'attività principale sia finalità ulteriori, di carattere promozionale. Tale commistione viene considerata problematica, poiché rende difficile per i genitori comprendere l'effettiva portata del consenso prestato.

Un secondo aspetto, centrale dell'istruttoria, concerne le **modalità di acquisizione del consenso**. Il Garante rileva che il consenso genitoriale veniva richiesto mediante moduli standardizzati, spesso predisposti in modo tale da non consentire una scelta realmente granulare tra le diverse opzioni. In particolare, l'Autorità osserva che l'adesione a determinate attività risultava, di fatto, condizionata all'accettazione del trattamento dell'immagine per finalità promozionali, circostanza che solleva dubbi circa la libertà del consenso. L'istruttoria si sofferma, poi, sulla concreta utilizzazione delle immagini dei minori, analizzando i canali di diffusione e la potenziale ampiezza del pubblico destinatario. Il Garante evidenzia che la pubblicazione su siti web, *social network* o materiali promozionali comporta una perdita di controllo sull'ulteriore circolazione delle immagini, con la conseguenza che il trattamento non può essere valutato come circoscritto o temporaneo. Questo elemento viene valorizzato come fattore di rischio specifico, soprattutto in relazione alla possibilità che le immagini rimangano accessibili anche quando il minore abbia raggiunto una maggiore maturità o una diversa percezione della propria identità.

Un ulteriore profilo istruttorio riguarda l'**assenza di una valutazione preventiva dei rischi**. L'Autorità rileva che il titolare del trattamento non aveva effettuato un'analisi specifica dell'impatto del trattamento sull'interesse del minore, limitandosi a fare affidamento sulla raccolta del consenso genitoriale. Tale circostanza viene letta come indice di una concezione riduttiva dell'*accountability*, in contrasto con l'impostazione del GDPR, che richiede una responsabilizzazione sostanziale del titolare, soprattutto in presenza di soggetti vulnerabili. Si legge, infatti, nel Provvedimento in analisi che *«il titolare del trattamento, prima di porre in essere una diffusione di dati personali, dovrebbe attentamente ponderare i rischi per la libertà e i diritti degli interessati giacché, una volta pubblicati, i dati rischiano di rimanere in rete per un tempo indefinito e possono essere utilizzati, anche incrociandoli con altre informazioni presenti sul web, da chiunque, potendo comportare effetti pregiudizievoli per gli interessati, con conseguenze talvolta irreparabili»*.

Sul piano strettamente giuridico, ferma restando la formulazione generica dell'informativa che non permette una manifestazione di volontà libera, specifica, informata e inequivocabile, la questione tocca un nodo complesso: la relazione tra l'**art. 8 GDPR**, che disciplina le condizioni di liceità del consenso prestato dai minori e dai loro genitori, e l'ordinamento interno che riconosce ai genitori la responsabilità e il potere-dovere di assumere decisioni nell'interesse del figlio (**art. 316 c.c.**) a tutela della sua dignità.

A tal proposito, nel provvedimento viene affermato quanto segue: *«Il trattamento in questione non può trovare fondamento neanche nel consenso reso dai soggetti esercenti la responsabilità genitoriale. Il potere-dovere di questi ultimi di prestare o negare il consenso al trattamento dei dati personali del minore, infatti, incontra il limite del perseguimento del superiore*

interesse del minore medesimo, superiore interesse certamente incompatibile con la pubblicazione delle immagini oggetto del presente procedimento per finalità qualificate dal titolare del trattamento come “didattiche” ma, più verosimilmente, da considerarsi promozionali».

La **Costituzione**, nell’ordinamento giuridico italiano, attribuisce alla famiglia un ruolo centrale nella cura e nell’educazione della prole, stabilendo che l’intervento pubblico debba avere natura sussidiaria e limitarsi ai casi di incapacità, inadeguatezza o pregiudizio concreto per il minore. È, dunque, lecito chiedersi se un’interpretazione della prestazione del consenso che ne riduca l’efficacia al punto da renderlo insufficiente a legittimare il trattamento dei dati personali del minore non travalichi i limiti di proporzionalità e ragionevolezza imposti dal principio di legalità.

È evidente che il Garante agisce in un contesto nel quale la protezione dei minori assume un valore particolarmente pregnante. Il **considerando 38 del GDPR** afferma chiaramente che i minori meritano una protezione specifica, poiché meno consapevoli dei rischi e delle conseguenze legati al trattamento dei dati. Tale esigenza si accentua nell’era digitale, in cui la circolazione incontrollata delle immagini può esporre i minori a rischi di sfruttamento, profilazione, commercializzazione e lesione della dignità personale. Tuttavia, proprio la natura rafforzata della protezione non può giustificare un approccio paternalistico che finisca per marginalizzare la dimensione relazionale e giuridica della famiglia. Il consenso dei genitori, infatti, non rappresenta una mera formalità burocratica, ma l’espressione di un diritto-dovere che l’ordinamento riconosce come parte integrante della **responsabilità genitoriale**. Negarne l’efficacia equivale a ridefinire, in via interpretativa, i confini di tale responsabilità, operazione che richiederebbe una base legislativa esplicita e non potrebbe essere affidata a un provvedimento di *soft law* o a un atto amministrativo dell’Autorità.

Un ulteriore profilo critico emerge con riguardo al **principio di proporzionalità**. Se è vero che il consenso non è, nel GDPR, l’unica base giuridica legittimante il trattamento, è altrettanto vero che la sua delegittimazione generalizzata rischia di produrre effetti paralizzanti per una pluralità di contesti sociali e culturali. Basti pensare alle scuole che documentano le attività educative, alle associazioni sportive e culturali che promuovono eventi con la partecipazione dei minori, alle iniziative editoriali o artistiche che utilizzano immagini di bambini. Una concezione rigida, che richieda sempre condizioni aggiuntive rispetto al consenso genitoriale, rischia di determinare un fenomeno di *over-compliance*, con la conseguente rinuncia a iniziative lecite per il timore di incorrere in sanzioni. Il bilanciamento dei diritti fondamentali in gioco, dalla protezione dei dati personali alla libertà di espressione e comunicazione, fino alla stessa identità sociale e culturale del minore, non può essere risolto mediante una generalizzata presunzione di invalidità del consenso espresso da chi esercita la responsabilità genitoriale, ma necessita di un approccio graduato e contestuale, capace di distinguere tra finalità commerciali invasive e usi socialmente utili o culturalmente rilevanti. La questione si sposta, in ultima analisi, sul terreno del rapporto tra Autorità indipendenti e principio democratico. L’intervento del Garante, pur animato da finalità condivisibili, solleva interrogativi circa i **confini del potere delle**

Autorità indipendenti. È legittimo che un'Autorità amministrativa limiti in maniera così incisiva prerogative che l'ordinamento civile e costituzionale attribuisce alla famiglia, senza una base normativa primaria esplicita? Il rischio è quello di una forma di normazione amministrativa che, seppure in nome della tutela del minore, incida su diritti e responsabilità fondamentali, spostando il baricentro dal circuito legislativo-giurisdizionale a quello amministrativo-regolatorio.

Certamente, il provvedimento del Garante sollecita una riflessione critica sulla capacità del diritto contemporaneo di affrontare le sfide poste dall'uso dei dati dei minori in ambienti digitali. La protezione del minore deve restare un obiettivo prioritario, ma non può essere perseguita attraverso una sostanziale esautorazione del ruolo genitoriale, pena la compromissione dei principi di legalità, proporzionalità e sussidiarietà che fondano lo Stato di diritto. La vera sfida consiste nel delineare strumenti di tutela che rafforzino la responsabilità condivisa tra istituzioni, famiglie e operatori, senza ridurre il consenso genitoriale a una mera formalità inefficace, ma piuttosto inserendolo in un quadro di garanzie multilivello, capace di temperare i diversi interessi in gioco e di preservare la centralità della famiglia nella cura e nella protezione dei figli.

SAMUELE FRANCESCO ROSA

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10162731>

2025/4(39)EF

La sentenza della Corte di Cassazione n. 28772/2025 del 31.10.2025 confermativa dell'orientamento sulla etero-organizzazione dei riders

La Cassazione, con la sentenza del 31 ottobre 2025, n. 28772 (la **Sentenza**), torna a pronunciarsi sulla etero-organizzazione dei *riders* (ciclofattorini) ribadendo l'interpretazione dell'art. 2 del d. lgs. n. 81/2015 affermata con il proprio precedente orientamento (vedi Cass. n. 1663/2020), secondo cui tali lavoratori sono collaboratori etero-organizzati e l'art. 2 citato, lungi dall'attribuire rilievo ad implicazioni qualificatorie del rapporto di lavoro, rappresenta una mera tecnica legislativa di estensione della disciplina protettiva della subordinazione.

Tale disposizione, come noto, prevede che si applichi la disciplina del rapporto di lavoro subordinato ai rapporti di collaborazione che si concretano in prestazioni di lavoro prevalentemente personali, continuative e le cui modalità di esecuzione sono organizzate dal committente, anche qualora l'etero-organizzazione avvenga tramite piattaforma digitale.

Nella fattispecie sottoposta all'attenzione della Suprema Corte un gruppo di *riders*, che avevano lavorato in favore di società *food delivery* in virtù di diversi contratti di collaborazione coordinata e continuativa a tempo determinato, adivano il Tribunale di Torino per ottenere l'accertamento della natura subordinata dei loro rapporti di lavoro, l'applicazione di un diverso

CCNL, con condanna generica della datrice di lavoro al pagamento delle conseguenti differenze retributive; nonché il risarcimento del danno per violazione della normativa sulla privacy e sui controlli a distanza.

Il Tribunale dichiarava il diritto dei riders a percepire, ai sensi dell'art. 2 D.Lgs. n. 81/2015, la retribuzione prevista dal CCNL applicato dalla società committente ai propri dipendenti, condannava la stessa al pagamento delle conseguenti differenze retributive e rigettava le altre domande. La decisione veniva confermata in sede di appello.

Anche la Sentenza ha confermato l'applicabilità dell'art. 2 D.Lgs. 81/2015 alle collaborazioni etero-organizzate anche quando il contratto sia formalmente autonomo, ritenendo irrilevanti elementi quali la proprietà del veicolo e l'assenza di un obbligo di disponibilità.

Il quadro normativo e le posizioni della dottrina e della giurisprudenza –

La prestazione resa dai lavoratori per il tramite delle piattaforme digitali può essere organizzata, come ogni altra attività lavorativa, con modalità tra loro significativamente differenti e, in particolare, mediante il lavoro autonomo genuino, il rapporto di lavoro subordinato e le collaborazioni etero-organizzate ex art. 2 del d.lgs. n. 81/2015.

Dal punto di vista normativo, alla disciplina interna (art. 2 e Capo V-bis del d.lgs. n. 81/2015), si è aggiunta la dir. (UE) 2024/2831, relativa al lavoro mediante piattaforme digitali, adottata il 24 ottobre 2024 (su cui v. in questa Rubrica la notizia n. 8 del [numero 2/2024](#) [2024/2(8)RiM], in *PeM*, 2024, p. 680) che gli Stati membri dovranno recepire entro il 2 dicembre 2026 (v. art. 11 della legge n. 91/2025, con cui il Parlamento ha conferito al Governo il recepimento della medesima direttiva).

La direttiva contiene prescrizioni minime comuni, volte a migliorare le condizioni di lavoro e la protezione dei dati personali per questa tipologia di lavoratori. A tal fine prescrive agli Stati membri di garantire che i lavoratori delle piattaforme digitali dispongano di una corretta determinazione della loro situazione occupazionale e di limitare, in questo ambito, il ricorso al lavoro autonomo fittizio.

Per quanto riguarda le tre possibili configurazioni giuridiche per l'attività di lavoro dei *riders*, l'assenza di poteri di controllo, direttivo e disciplinare da parte della piattaforma, unitamente alla facoltà del prestatore di non accettare incarichi senza subire conseguenze pregiudizievoli, costituiscono gli elementi distintivi del lavoro autonomo, al quale in ogni caso il Capo V-bis del d.lgs. n. 81/2015 garantisce un nucleo minimo di tutele, incluso il compenso minimo orario e la copertura assicurativa INAIL.

È dunque riconosciuta la possibilità che la piattaforma digitale instauri (legittimamente) con il *rider* un rapporto di lavoro autonomo. Tali rapporti di lavoro autonomo condividono con i rapporti di collaborazione coordinata e continuativa ex art. 409, n. 3, c.p.c. la nozione di continuità, che nel caso del lavoro tramite piattaforma digitale si apprezza avendo riguardo ai turni opzionati dal *rider* e non solo a quelli effettivamente svolti nell'arco di tempo preso in considerazione.

Tuttavia, nel rapporto di lavoro autonomo non vi è un coordinamento del tipo richiesto dall'art. 409, n. 3, c.p.c. come modificato dall'art. 15, comma 1, della l. 81/2017 – secondo cui “La collaborazione si intende coordinata

quando, nel rispetto delle modalità di coordinamento stabilite di comune accordo dalle parti, il collaboratore organizza autonomamente l'attività lavorativa", poiché la prestazione di lavoro è organizzata dal committente.

Per il lavoro subordinato, vengono invece in rilievo i tradizionali elementi ed indici dell'art. 2094 c.c., declinati alla luce delle specificità del lavoro tramite piattaforme digitali, quali ad esempio una subordinazione che può manifestarsi attraverso direttive specifiche e vincolanti trasmesse tramite app, controllo pervasivo mediante geolocalizzazione e sistemi di punteggio che operano come meccanismi premiali/sanzionatori (Vedi Circolare n. 9 del 2025 del Ministero del Lavoro).

La categoria delle collaborazioni etero-organizzate previste dall'art. 2 del D. Lgs. n. 81 del 2015 si applicano infine quando, pur in assenza di subordinazione in senso stretto, le modalità di esecuzione della prestazione sono organizzate dal committente. L'etero-organizzazione si configura infatti quando sussiste autonomia nella fase genetica del rapporto ma non in quella funzionale, con la piattaforma che detta costantemente le modalità di esecuzione dell'attività.

Tale disposizione sin dalla sua entrata in vigore ha diviso la dottrina tra chi ha individuato nella innovazione un sostanziale rafforzamento, in funzione evolutiva, della nozione civilistica di subordinazione desumibile dall'art. 2094 c.c.; quella che, restando nell'ambito del lavoro autonomo, ne ha esaltato solo la funzione rimediante realizzata con l'applicazione a rapporti di collaborazione autonoma del regime del lavoro subordinato, con differenziazioni tra le posizioni favorevoli ad una estensione totale o parziale; quella che ha interpretato la nuova disposizione come il paradigma legale del *tertium genus* della cd. etero-organizzazione, intermedio dunque tra subordinazione ed autonomia.

In giurisprudenza, la prima pronuncia di legittimità ha verificato quattro diverse soluzioni interpretative: quella della qualificazione tipologica come versione evoluta della subordinazione; della figura intermedia fra subordinazione e autonomia, caratterizzata dalla etero-organizzazione e tipizzata dall'art. 2 del d.lgs. n. 81 del 2015; della permanenza nell'ambito del lavoro autonomo come ulteriore ipotesi di para-subordinazione; infine, dell'approccio rimediante che ove ricorrono gli indicatori previsti dall'art. 2 consente di applicare la tutela "rafforzata" dei lavoratori subordinati.

Nel prendere posizione sulla questione interpretativa, la Cassazione ha definito l'art. 2 in esame come una «norma di disciplina che non crea una nuova fattispecie»; nessun *tertium genus*, ma norma che si limita a regolare l'estensione della disciplina del lavoro dipendente ad una serie di rapporti, collocati in quella che definisce zona grigia tra autonomia e subordinazione, accomunati da elementi tecnico-funzionali che li rendono congeniali ad una tutela omogenea a quella assicurata ai lavoratori subordinati in quanto operanti in una medesima condizione di "debolezza economica" (Vedi Cass. n. 1663/2020).

Personalità della prestazione di lavoro e continuità - Ciò chiarito in ordine al quadro di riferimento, la Sentenza muove dal presupposto secondo cui, nel caso in cui le parti instaurino un rapporto di lavoro autonomo che si connota per la continuità della collaborazione e per la etero-organizzazione della



prestazione lavorativa, in sede di accertamento giudiziale, la conseguenza non è la riqualificazione nei termini della subordinazione ma l'applicazione al rapporto di lavoro della disciplina del lavoro subordinato. La Corte, infatti, ricorda che: “(...) l'art. 2 d. lgs. 81/2015 non introduce una nuova fattispecie (...) bensì una “norma di disciplina”, volta (e limitata) a dichiarare applicabile la disciplina della subordinazione a rapporti di lavoro che possono legittimamente essere pattuiti come di lavoro autonomo”.

Dunque, “il legislatore ha introdotto una “dissociazione” tra qualificazione giuridica della fattispecie e la disciplina applicabile: di solito la seconda segue la prima, salva diversa e specifica previsione normativa, nella specie rappresentata, appunto, dall'art. 2 d. lgs. cit.”.

In tale prospettiva, la proprietà in capo al collaboratore “del veicolo utilizzato per eseguire la prestazione e i relativi costi di eventuale manutenzione” è un profilo attinente alla “qualificazione giuridica del rapporto di lavoro” e non riguarda la “disciplina applicabile”.

Si tratta quindi di un aspetto irrilevante ai fini dell'art. 2 d.lgs. n. 81/2015, che, “in considerazione di determinati elementi, ha appunto la funzione di dichiarare applicabile la disciplina del lavoro subordinato a rapporti che ben possono essere configurati dai contraenti come di lavoro autonomo”.

La pronuncia si sofferma, inoltre, sul requisito della prestazione esclusivamente personale e di continuità della collaborazione che, unitamente alla etero-organizzazione, sono necessari per l'applicazione dell'art. 2, comma 1, vigente *ratione temporis* (poi modificato dalla l. 128/2019 di conversione del d.l. 101/2019).

In particolare, secondo la Cassazione, il fatto che la bicicletta e la relativa manutenzione fossero a carico del *rider* non escludeva la natura esclusivamente personale della prestazione, ma confermava la qualificazione del rapporto di lavoro nei termini della autonomia.

Quanto alla continuità della prestazione, secondo la sentenza in commento, essa non può essere intesa, diversamente da quanto sostenuto dalla società, alla stregua di un obbligo del lavoratore di mettersi a disposizione della committente.

Ed infatti, secondo la sentenza, “non vi è alcuna ragione per intendere il requisito della continuità in modo difforme da quanto ritenuto da questa Corte in relazione alle collaborazioni previste dall'art. 409, n. 3, c.p.c.”

Nel caso di specie erano stati conclusi contratti di collaborazione coordinata e continuativa che lasciavano intendere che sin dall'inizio vi fosse la volontà di instaurare un rapporto di collaborazione di tipo continuativo e la continuità, secondo la sentenza, deve essere valutata sulla base dei turni opzionati dal rider e non in base al numero dei turni effettivamente svolti dallo stesso, data la facoltà del committente di assegnare le consegne a un rider diverso, a prescindere dalla disponibilità fornita dal lavoratore.

L'etero-organizzazione – Come noto, l'etero-organizzazione, ai fini della riconduzione del rapporto alla fattispecie di cui all'art. 2 d.lgs. n. 81/2015, si realizza quando il committente determina unilateralmente tempi, luoghi e modalità di esecuzione, anche tramite strumenti digitali o algoritmici.

Nel caso di specie, la sentenza ha correttamente precisato, nel solco di Cass. n. 1663/2020, che il riferimento “ai tempi e ai luoghi di lavoro” è stato inteso

come meramente esemplificativo, “come dimostrato dall'uso dell'avverbio “anche” da parte del legislatore e dalla successiva soppressione dell'inciso “anche con riferimento ai tempi e al luogo di lavoro” ad opera del D.L. 3 settembre 2019, n. 101, convertito, con modificazioni, nella legge 2 novembre 2019, n. 128”.

Peraltro, anche nella versione dell'art. 2 *ante* l. 128/2019 di conversione del d.l. 101/2019, il requisito della etero-organizzazione non si esauriva nella organizzazione, da parte della committente, dei tempi e del luogo della prestazione lavorativa, trattandosi di un richiamo presente nella disposizione a mero titolo esemplificativo.

Ne deriva dunque che può “essere ravvisata etero-organizzazione rilevante ai fini dell'applicazione della disciplina della subordinazione anche quando il committente si limiti a determinare unilateralmente il quando e il dove della prestazione personale e continuativa”.

Pertanto, conclude la Corte, i *riders* hanno diritto all'applicazione delle norme di tutela del lavoro subordinato, comprese quelle retributive e previdenziali, pur restando formalmente collaboratori autonomi.

La Corte di Cassazione, dunque, ha rigettato il ricorso della società, confermando la decisione della corte territoriale, che aveva riconosciuto il diritto dei riders, ai sensi del citato art. 2, a ricevere la retribuzione diretta, indiretta e differita prevista dal CCNL per i dipendenti del terziario, della distribuzione e dei servizi, applicato ai dipendenti della società, e a essere inquadrati al VI livello, condannando la società al pagamento delle differenze retributive.

Risulta dunque confermato il precedente orientamento di legittimità che ha ritenuto di stemperare il dilemma qualificatorio autonomia /subordinazione, da sempre centrale nel diritto del lavoro sul piano dogmatico, imponendo l'integrale estensione della disciplina protettiva del lavoro subordinato prevista dall'art. 2, comma 2, del d.lgs. n. 81/2015, come modificato dalla legge n. 128/2019 ai rapporti di collaborazione che si concretano in prestazioni di lavoro prevalentemente personali, continuative e le cui modalità di esecuzione sono organizzate dal committente.

In tal senso, l'ordinamento domestico pare allinearsi alla dir. (UE) 2024/2831, che introduce una presunzione relativa di subordinazione in presenza di indici di controllo/direzione via piattaforma, il rafforzamento degli obblighi informativi e della trasparenza algoritmica e adeguamenti su salute, sicurezza e protezione dei dati.

Resta però che se l'attribuzione in prospettiva “rimediale” dello statuto protettivo del lavoro subordinato anche ai collaboratori etero-organizzati appare da condividere sul piano pratico, su quello dogmatico è ancora da risolvere la *querelle* della qualificazione del rapporto di lavoro dei ciclofattorini delle piattaforme digitali.

EMANUELA FIATA

<https://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=.%2F20251031%2Fsnciv%40sL0%40a2025%40n28772%40tS.clean.pdf>

2025/4(40)MC

La sentenza della Corte suprema svedese del 1 luglio 2025 di annullamento di un contratto di gioco per sfruttamento della compulsività del contraente giocatore desumibile dai dati del suo comportamento online

| 1148

Una recente decisione della *Högsta domstolen*, la Corte suprema svedese, mette in luce la possibilità che si configurino nuove e significative forme di tutela inerenti al trattamento automatizzato dei dati sulla base delle tradizionali regole del diritto contrattuale.

La controversia trae origine da una serie di transazioni di gioco compiute tra il 2009 e il 2014 da parte di un soggetto privato presso un operatore di gioco online. Nel corso di tale periodo, il giocatore partecipò in modo intensivo a forme di gioco online, in particolare ad una versione digitale delle slot machine. L'attività di gioco comportò una movimentazione complessiva di somme estremamente rilevanti – pari a quasi quindici milioni di euro – con una perdita netta corrispondente a circa otto milioni di corone svedesi (circa settecentomila euro), di cui l'equivalente di oltre 500.000 euro maturato nel periodo successivo alla sua promozione a *VIP customer*. Nel frattempo, al giocatore era stata diagnosticata una grave forma di dipendenza patologica dal gioco d'azzardo.

In primo grado, vennero respinte integralmente le pretese dell'attore: le singole transazioni di gioco furono considerate validamente stipulate e non venne ravvisata alcuna responsabilità in capo all'operatore.

In secondo grado, invero, il giudice d'appello giunse a una conclusione opposta.

Attraverso l'analisi dei dati comportamentali raccolti e utilizzati dall'operatore, la corte adita ritenne provato che quest'ultimo fosse, o quantomeno dovesse essere, consapevole delle condotte di gioco del cliente, caratterizzate da perdita di controllo, elevata frequenza delle giocate e andamento progressivamente crescente delle perdite. Tale consapevolezza venne ritenuta ulteriormente aggravata dal fatto che l'operatore avesse indirizzato verso il giocatore un'intensa attività di marketing diretto e personalizzato proprio nel periodo in cui i segnali di vulnerabilità risultavano più evidenti.

Sulla base di tali elementi, il giudice d'appello ritenne applicabile la disciplina di cui alla sezione 33 della legge svedese sui contratti (33 § *avtalslagen*), che prevede l'invalidità degli atti giuridici che, per le circostanze in cui sono stati conclusi, risultino contrari alla buona fede e all'onore sociale, qualora la controparte fosse presumibilmente a conoscenza di tali circostanze. In applicazione di tale disposizione, vennero dichiarate nulle tutte le giocate poste in essere nel periodo rilevante – e, in particolare, quelle successive all'attribuzione dello status cliente di *VIP customer* – con conseguente condanna alla restituzione delle perdite nette, per un importo pari a circa cinquecentomila euro.

Il caso è giunto così alla *Högsta domstolen*, che il 1° luglio 2025 ha emesso la sentenza nel caso T 607-24.

Il nucleo della decisione della Corte Suprema riguarda l'interpretazione della citata sezione 33 e, dunque, della portata della relativa tutela verso l'esecuzione di atti "contraria alla buona fede e all'onore sociale". La disposizione svedese riguarda, fra l'altro, i contratti stipulati in circostanze inique o altrimenti improprie e – similmente a quanto previsto dal nostrano art. 428 c.c. in tema di incapacità naturale – può essere applicata, ad esempio, quando una parte contraente, a causa di malattia, intossicazione o altre cause, non è in grado di valutare chiaramente il contenuto o le implicazioni di un contratto. Secondo l'articolata motivazione della Corte, tale disposizione svolge una funzione di equità contrattuale, volta a impedire che una parte possa avvalersi di un rapporto negoziale fondato su un evidente squilibrio sostanziale, noto o conoscibile dalla controparte.

La questione cruciale affrontata dalla Corte Suprema, pertanto, è stata quella relativa al requisito della conoscenza di circostanze rilevanti sulla capacità del giocatore da parte dell'operatore di gioco.

Nel contesto dei servizi digitali, contratti e singole transazioni sono conclusi mediante piattaforme automatizzate, senza un intervento umano diretto; tuttavia, tali sistemi si fondano sulla raccolta e sull'elaborazione di una quantità estremamente dettagliata di dati comportamentali relativi all'utente – quali la frequenza delle giocate, l'ammontare delle puntate, i meccanismi di reinvestimento delle perdite e la risposta agli stimoli promozionali – che la Corte sinteticamente qualifica come "gambling data".

Secondo la Corte svedese, le società che hanno accesso a tali dati e li utilizzano attivamente nell'ambito delle proprie strategie commerciali devono essere considerate consapevoli delle informazioni che da essi emergono, quantomeno nella misura in cui esse sfruttino (deliberatamente, o tramite meccanismi automatizzati) la condizione di debolezza in cui i giocatori versino. Tale consapevolezza non presuppone una diagnosi clinica formale di dipendenza, ma può fondarsi sull'osservazione di indicatori chiari – intensità del gioco, continuità temporale, progressione delle perdite – idonei a rivelare una perdita di controllo da parte del giocatore.

La Corte ha ritenuto che la prosecuzione dell'offerta di servizi di gioco, accompagnata da forme di intrusive marketing e dall'erogazione sistematica di bonus, risultasse incompatibile con i citati standard di buona fede e onore sociale, denotando tale approfittamento una conoscibilità della situazione patologica in cui versava il giocatore. Ciò tanto più in considerazione del fatto che la tipologia di gioco offerta rientrava fra le più rischiose in termini di potenziale di dipendenza. In tale contesto, la conclusione e l'esecuzione ripetuta di contratti di gioco nel periodo considerato è stata ritenuta contraria a buona fede, nei termini di cui alla citata sezione 33, poiché implicava la prosecuzione di un rapporto negoziale in presenza di una vulnerabilità nota e di un marcato squilibrio tra le parti. Nella prospettiva della Corte, dunque, le tecnologie digitali e l'automazione non possono essere utilizzate per eludere le tutele tradizionalmente riconosciute al contraente debole, né per neutralizzare il rilievo giuridico delle condizioni di vulnerabilità emerse nel corso dell'esecuzione del rapporto: di là dall'effettiva presa di consapevolezza del soggetto professionista, l'approfittamento e lo sfruttamento di tali condizioni, pur per il tramite di sistemi automatizzati non

direttamente soggetti a controllo umano, implica una responsabilità dell'operatore di gioco.

Così, la *Högsta domstolen* ha in larga parte confermato la decisione impugnata, dichiarando l'invalidità degli accordi di gioco conclusi nel periodo rilevante e condannando l'operatore alla restituzione delle perdite nette subite dal giocatore, per un importo pari a poco più di 500.000 euro. La Corte ha, invece, escluso la condanna al risarcimento del danno per la sofferenza psicologica patita, in assenza di prove sufficienti circa il nesso causale.

Tale decisione presenta implicazioni di rilievo che travalicano il diritto svedese dei contratti.

Essa costituisce, in primo luogo, un significativo sviluppo nell'applicazione della clausola di buona fede a rapporti negoziali digitalizzati e automatizzati, affermando che il trattamento algoritmico dei dati comportamentali non esonera l'operatore da responsabilità, permanendo l'obbligo di vagliare la vulnerabilità del consumatore e di adeguare di conseguenza la propria condotta. Si ha, infatti, il riconoscimento di una responsabilità in forza della 'conoscibilità algoritmica' dell'altrui incapacità di intendere e volere.

In secondo luogo, la pronuncia si colloca pienamente nel dibattito europeo sulla sostenibilità sociale del gioco d'azzardo e sulla responsabilità degli operatori digitali, ponendo l'accento su una vera e propria responsabilità di vigilanza attiva sui propri sistemi tecnologici, affinché essi non favoriscano né aggravino situazioni di dipendenza.

Da ultimo, il principio secondo cui la conoscenza "digitalizzata" delle condizioni dell'utente può fondare obblighi e responsabilità contrattuali appare suscettibile di estensione a ulteriori mercati regolati – quali il credito al consumo, gli investimenti *online* o altri servizi digitali fondati sulla profilazione – rendendo la decisione della Corte Suprema svedese un precedente di interesse anche in prospettiva comparativa.

Nel complesso, la pronuncia si inserisce in una cornice di sostenibilità regolatoria e di tutela delle vulnerabilità individuali, collegando in modo organico i principi generali del diritto dei contratti con le dinamiche della profilazione comportamentale e imponendo agli operatori di assumersi responsabilità concrete rispetto agli squilibri che essi stessi contribuiscono a generare attraverso le proprie piattaforme digitali.

MICHELE CIANCIMINO

Testo in inglese:

<https://www.domstol.se/globalassets/filer/domstol/hogstodomstolen/avgoranden/engelska-oversattningar/t-607-24-eng.pdf>

Provvedimento originale in svedese:

<https://rattspraxis.etjanst.domstol.se/sok/publicering/71b81b3c-cce8-4354-88cf-c2559b1c7ca6>

2025/4(41)AF

Il GENIUS Act del 18.7.2025: confronto con il MiCAR

Da strumenti esotici forieri del cosiddetto *crypto winter* a mezzi di regolamento consolidati nel mercato delle cripto-attività, con una chiara ambizione per i pagamenti, gli *stablecoins* sono stati i protagonisti delle cronache finanziarie dell'ultimo anno. La significativa crescita che tali cripto-attività hanno subito e la progressiva concentrazione del loro mercato, trainata in misura prevalente da *stablecoins* ancorati al dollaro statunitense, ha reso evidente la necessità di un quadro regolamentare capace di affrontare i rischi ad essi connessi. Pur essendo concepiti per mantenere un valore stabile, gli *stablecoins*, difatti, operano in un contesto altamente volatile e transfrontaliero, in assenza di regole armonizzate a livello globale. La loro diffusione ha evidenziato la necessità di quadri normativi coerenti e uniformi tra gli ordinamenti. In questo contesto si collocano il regolamento (UE) 2023/1114 (**MiCAR**) (sul quale v. in questa Rubrica la notizia n. 1 del [numero 2/2023](#) [2023/2(1)AF], in *PeM* 2023, p. 374 e in *Atlante*, p. 338), che va a predisporre regole uniformi per i mercati delle cripto-attività nell'Unione, e il *Guiding and Establishing National Innovation for US Stablecoins Act* del 18 luglio 2025 (**GENIUS Act**), che, invece, stabilisce un quadro federale per lo sviluppo degli *stablecoins* di pagamento per il mercato statunitense. Sebbene i due testi legislativi appaiano simili, a un più attento esame essi risultano profondamente diversi. Difatti, sebbene entrambi i quadri normativi mirino a disciplinare l'emissione e l'uso degli *stablecoins*, i diversi principi a cui si ispirano e le differenze strutturali che ne derivano riflettono priorità e politiche profondamente diverse, la cui interazione potrebbe potenzialmente influenzare l'evoluzione degli *stablecoins* nell'Unione, nonché la formazione di quadri regolamentari divergenti negli altri ordinamenti.

Le prime differenze tra MiCAR e GENIUS Act si riscontrano nel loro ambito di applicazione oggettivo. Il GENIUS Act si applica ai soli *payment stablecoins*, vale a dire quegli *stablecoins* destinati a essere impiegati come mezzo di pagamento e di regolamento delle transazioni. MiCAR, invece, ha un ambito di applicazione più ampio e distingue gli *stablecoin* tra *e-money tokens*, quali *stablecoins* ancorati a una valuta ufficiale, e *asset-referenced tokens*, *stablecoins* facenti riferimento potenzialmente alle attività più disparate, quali materie prime o panieri di valute ufficiali. Attraverso queste due categorie, MiCAR, a differenza del GENIUS Act modella il regime per gli *stablecoins* a seconda della funzione che essi svolgono: gli *e-money tokens* vengono equiparati a fondi e regolati come tali, assolvendo a una funzione di pagamento; gli *asset-referenced tokens*, più adatti a fungere da riserva di valore, sono sottoposti a un regime che richiama talvolta la loro natura di veicolo di investimento. Ne seguono anche regimi diversi per quanto riguarda l'emissione: se gli *asset-referenced tokens* possono essere emessi da soggetti stabiliti nell'Unione purché previamente autorizzati sotto MiCAR o sotto altro regime, l'emissione di *e-money tokens* è riservata ai soli enti creditizi e agli istituti di moneta elettronica. Il GENIUS Act limita anch'esso l'emissione a specifiche categorie di emittenti- quali *subsidiaries of insured depository institutions*, *federal qualified issuers*, *state qualified issuers* -, ma lo fa per i soli cosiddetti *payment stablecoins*. Inoltre, se MiCAR richiede che gli emittenti siano stabiliti nell'Unione, il GENIUS Act permette agli

emittenti esteri di operare direttamente nel mercato statunitense, purché il regime domestico sia comparabile a quello statunitense. Per quanto riguarda i requisiti per gli emittenti, se l'impianto di base tra MiCAR e GENIUS Act sembra essere simile e basato su norme analoghe- quali requisiti per le riserve di attività, regole sul rimborso e norme prudenziali-, MiCAR si caratterizza per prescrizioni dettagliate, mentre il GENIUS Act rinvia la specificazione di tali requisiti a future determinazioni regolamentari. Esempio di tale differenza d'approccio ci è dato dai requisiti prudenziali. Vi sono, poi, anche delle differenze di sostanza, come nel caso delle riserve che gli emittenti devono detenere a sostegno del valore dello *stablecoin* emesso e a garanzia della promessa di rimborso che lo strumento implica. Mentre MiCAR richiede agli emittenti di tenere una porzione minima di riserve come conti di deposito presso enti creditizi dell'Unione, il GENIUS Act non impone alcuna soglia minima. Stessa dinamica si ha per altre norme. Mentre MiCAR proibisce la corresponsione di interessi su *stablecoins* sia agli emittenti che ai prestatori di servizi, il GENIUS Act limita tale divieto ai soli emittenti. Da ultimo, se agli emittenti dell'Unione non è concesso applicare commissioni al rimborso degli e-money tokens e degli *asset-referenced tokens*, il GENIUS Act lascia carta bianca agli emittenti statunitensi se e in che misura applicare *redemption fees*. Vi sono poi una serie di norme e requisiti che MiCAR prevede e che, invece, sono del tutto assenti nel GENIUS Act, tra cui le misure di crisi, come il *recovery plan* e il *redemption plan*, e i requisiti aggiuntivi e la supervisione a livello dell'Unione per gli *stablecoin* cosiddetti significativi.

A un occhio più attento, quindi, il GENIUS Act e MiCAR, per quanto all'apparenza simili, riflettono delle differenze sostanziali nell'approccio. MiCAR si configura come un quadro regolamentare compiuto e definito con un'impronta territoriale, mentre il GENIUS Act si basa su norme di principio che richiedono interventi attuativi, la cui definizione spetterà ai regolatori. Ne deriva che, se MiCAR disciplina in maniera stringente gli *asset-referenced tokens* e gli *e-money tokens* nell'ottica di preservare la stabilità finanziaria e tutelare i detentori, il GENIUS Act si colloca più come regime flessibile il cui principale obiettivo sembra essere quello di consolidare la *leadership* statunitense nei mercati delle cripto-attività, come anche apertamente dichiarato nell'Executive Order del 23 gennaio 2025. La differenza tra i due approcci è rilevante in quanto potrebbe influenzare non solo l'evoluzione del mercato delle cripto-attività -facendo sì che questa sia determinata da considerazioni di competitività e, talvolta, di arbitraggio regolamentare-, ma anche la definizione dei quadri regolamentare negli altri ordinamenti, potenzialmente accentuandone la divergenza e amplificando i rischi che gli *stablecoins* potrebbero porre al sistema finanziario.

ALICE FILIPPETTA*

Banca Centrale Europea

*Le opinioni o i punti di vista espressi sono esclusivamente dell'autore e non dell'istituzione

<https://www.congress.gov/bill/119th-congress/senate-bill/1582/text>

2025/4(42)AF

Verso il CLARITY Act: l'incertezza regolamentare per gli *asset* digitali

| 1153

Il destino del mercato delle cripto-attività sta per essere segnato da quello che sarà il testo legislativo che andrà a governare la struttura del mercato dei *digital assets* nell'ordinamento statunitense. Al momento, gli *asset* digitali nel mercato statunitense sono soggetti a supervisione frammentaria e incertezza giuridica. In questo contesto, i riflettori sono puntati sul *Digital Asset Market Clarity Act (CLARITY Act)*, presentato nel giugno 2025, che avrebbe il compito di definire regole a tutela dei clienti e investitori e a sostegno dell'innovazione nel mercato statunitense. In un'atmosfera incerta, in cui il voto del Senato è stato rinviato, il CLARITY Act è particolarmente discusso perché, oltre a definire delle norme, andrà a stabilire chi regolerà le cripto-attività e i *digital assets* più in generale, la *Securities and Exchange Commission (SEC)* o la *Commodity Futures Trading Commission (CFTC)*, ambendo a chiudere le esistenti lacune regolamentari. Difatti, il CLARITY Act attribuirebbe alla CFTC un ruolo centrale nella regolamentazione delle *digital commodities*, definite come *asset* digitali il cui valore è intrinsecamente collegato all'uso della *blockchain* e diverse da *securities*, derivati e *stablecoin*. Norme specifiche sarebbero predisposte per assicurarsi che le *digital commodities* abbiano carattere decentralizzato e non conferiscano alcun diritto di *governance* o patrimoniale. Alla SEC rimarrebbe la giurisdizione su quei *digital assets* considerati *securities*, vale a dire qualificabili come contratti di investimento e emesse da un soggetto con l'aspettativa per i detentori di trarne profitto. Si introdurrebbero poi anche regole per il mercato secondario e i prestatori di servizi, dove la SEC manterrebbe sotto la propria ala le transazioni in *digital commodities* effettuate da operatori dei mercati dei valori mobiliari registrati, mentre la CFTC sarebbe responsabile per le cosiddette *digital commodity exchanges*, le quali non sarebbero altro che le piattaforme di negoziazione che così di sovente dominano l'universo delle cripto-attività. Tuttavia, se al principio il CLARITY Act non aveva destato clamore, ora che si giugne a un più attento esame e a norme di dettaglio, discussioni su punti come il divieto di corresponsione di interessi su payment *stablecoin* in via indiretta da parte dei prestatori di servizi, lasciano il mercato degli *asset* digitali statunitensi in balia di interessi contrapposti e in attesa di regole chiare e uniformi.

ALICE FILIPPETTA*

<https://www.congress.gov/bill/119th-congress/house-bill/3633/text>

2025/4(43)FG

La sentenza del Landesgericht di Monaco dell'11.11.2025 (causa 42 O 14139/24) nel caso GEMA (collecting tedesca) contro Open AI in

materia di tutela del diritto d'autore e addestramento di modelli di IA a proposito di testi di canzoni

| 1154

Con sentenza emanata l'11 novembre 2025 dal Tribunale Regionale di Monaco (il **Tribunale**) nella causa 42 O 14139/24 (la **Sentenza**), OpenAI Ireland Ltd e la holding americana OpenAI LLC (collettivamente **OpenAI**) sono state dichiarate responsabili per violazione dei diritti d'autore nell'addestramento di ChatGPT, in accoglimento di una domanda avanzata dalla società tedesca di gestione collettiva “Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte” (**GEMA**).

La sentenza origina da un atto di citazione proposto di fronte al Tribunale il 13 novembre 2024 da GEMA contro OpenAI, quale operatore del chatbot ‘ChatGPT’ in Europa, nel quale GEMA lamentava la riproduzione e messa a disposizione non autorizzata di **testi di opere musicali** (lyrics), amministrate da GEMA in forza del mandato ricevuto dagli aventi diritto, tramite il suddetto chatbot.

Secondo GEMA, quando vengono inseriti semplici prompt, come ad esempio “Qual è il testo di [titolo della canzone]?”, il chatbot riproduce i testi originali delle opere musicali con cui il sistema è stato addestrato. GEMA sostiene che “mentre altri servizi internet pagano diritti di licenza agli autori per l'utilizzo dei loro testi, OpenAI fa sistematicamente uso dei contenuti degli autori, violando deliberatamente il diritto d'autore”.

GEMA ha ottenuto il mandato dai propri iscritti per la gestione del diritto di riproduzione grafica dei testi delle opere musicali e ha effettuato l'opt-out come previsto ai sensi dell'art. 4 della Direttiva (UE) 2019/790 (“Direttiva DSM”), riservandosi di autorizzare l'utilizzo del proprio repertorio per finalità di Text and Data Mining.

Con questa azione legale, GEMA è diventata la prima società di gestione collettiva al mondo a citare in giudizio un fornitore di sistemi di intelligenza artificiale generativa che ha utilizzato opere musicali tutelate per addestrare i propri sistemi senza aver acquisito le necessarie licenze. L'obiettivo di GEMA era chiarire la situazione giuridica e, su tale base, avviare trattative con gli AI providers per la stipula di licenze, utilizzando eventualmente come template la licenza pubblicata nel settembre 2024 per l'addestramento dei sistemi di IA generativa e per la generazione di nuove opere musicali tramite gli stessi sistemi di IA.

È importante precisare che il presente caso riguarda i testi di opere musicali e **non riguarda le composizioni musicali** che sono oggetto di un procedimento separato che GEMA ha intentato contro la società americana Suno Inc. (**Suno**) per Suno AI nel gennaio 2025. Suno AI genera opere musicali (file audio) utilizzando un sistema di IA generativa.

In data 11 novembre 2025, il Tribunale di Monaco ha dunque ritenuto OpenAI responsabile per violazione dei diritti d'autore nell'addestramento di ChatGPT, come anticipato dalla Corte nell'udienza del 29 settembre 2025. In quella sede, il Tribunale aveva rilevato che i fatti erano in realtà “non complicati”, dato che OpenAI non contestava l'utilizzo delle opere tutelate nell'addestramento del proprio modello ChatGPT. I giudici, inoltre, non si

sono lasciati convincere dall'argomento secondo cui sarebbero gli utenti, e non OpenAI, a dover rispondere degli output di ChatGPT.

Il Tribunale ha sostanzialmente accolto le domande di inibitoria, informazione e risarcimento dei danni proposte da GEMA contro due società del gruppo OpenAI. In particolare, ha emesso un'inibitoria nei confronti di OpenAI dalla riproduzione nei modelli e dalla violazione tramite gli output di testi di opere musicali non autorizzate e dalla memorizzazione dei dati correlati su qualsiasi infrastruttura ubicata in Germania; ha dichiarato OpenAI responsabile per i danni da determinarsi in un procedimento successivo, in quanto le convenute avrebbero potuto e dovuto riconoscere che l'utilizzo dei testi delle canzoni per il training e la loro restituzione mediante output avvenivano senza una base giuridica valida; e ha, infine, rifiutato di accogliere la proposta di entrambe le parti di rinviare alcune questioni relative all'interpretazione del diritto d'autore dell'UE alla Corte di giustizia dell'Unione europea.

La parte motiva della Sentenza muove da una discussione dettagliata sul funzionamento dei modelli linguistici di grandi dimensioni (LLM). GEMA ha indicato 30 esempi di violazione relativi ai testi di nove canzoni. La sentenza nomina diversi esempi di violazioni identificate; il più breve consiste di sole 15 parole.

OpenAI ha sostenuto che le risposte del suo LLM non sono deterministiche, poiché derivano da correlazioni statistiche tra token. OpenAI ha contestato le pretese di GEMA, sostenendo che i loro modelli linguistici non memorizzano né copiano dati di addestramento specifici, ma riflettono nei propri parametri quanto appreso sulla base dell'intero set di dati di addestramento. Poiché gli output vengono generati solo a seguito dell'input dell'utente (prompt), non sarebbero i convenuti, bensì il rispettivo utente, a essere responsabili dell'output in quanto suo creatore. In ogni caso, eventuali violazioni di legge sarebbero coperte dalle eccezioni al diritto d'autore di cui alla direttiva (UE) 2019/790 (**direttiva DSM**). Tuttavia, gli esempi di output violativi forniti da GEMA sono stati sufficienti a convincere il Tribunale che un'inibitoria fosse giustificata.

Il Tribunale ha riconosciuto che l'eccezione per la riproduzione ai fini del text and data mining potrebbe in linea di principio essere legittimamente utilizzata per creare corpora di addestramento per sistemi di IA. Tuttavia, ha anche stabilito che la mera possibilità di ricostruire un'opera dai parametri del modello è sufficiente a violare il diritto di riproduzione, anche in assenza di una copia fisica all'interno del modello. Secondo il Tribunale, sia la memorizzazione nei modelli linguistici sia la riproduzione dei testi delle canzoni negli output del chatbot costituiscono violazioni dei diritti di sfruttamento economico. Tali violazioni, si motiva nella Sentenza, non sono coperte da alcuna limitazione, in particolare non dalla limitazione di cui alla direttiva DSM, la cui ratio è che tali riproduzioni siano effettuate esclusivamente a fini di analisi successiva e non incidano sugli interessi di sfruttamento dell'autore. Poiché questi atti puramente preparatori non pregiudicano gli interessi di sfruttamento, la legge non prevede un obbligo di remunerazione a favore dell'autore.

La memorizzazione dei testi di alcune opere del repertorio di GEMA è stata accertata confrontando gli stessi testi contenuti nei dati di addestramento con le riproduzioni negli output. Considerata la complessità e la lunghezza dei testi delle canzoni, la coincidenza casuale può essere esclusa come causa della riproduzione.

Le domande dell'attrice sono fondate nella misura in cui sono dirette contro la riproduzione dei testi delle canzoni nei modelli linguistici. Secondo il Tribunale, i modelli linguistici delle convenute costituiscono esemplari di riproduzione ai sensi dell'art. 2 della direttiva 2001/29/CE (**direttiva InfoSoc**). Le riproduzioni si realizzano, da un lato, mediante la fissazione temporanea degli output nella memoria di lavoro dei dispositivi terminali degli utenti e, dall'altro, mediante la memorizzazione durevole delle conversazioni nella cronologia delle chat sui server cloud delle convenute.

OpenAI ha cercato di beneficiare di un'esenzione applicabile agli istituti di ricerca senza scopo di lucro. Secondo il Tribunale, OpenAI avrebbe dovuto allegare e provare di reinvestire il 100% dei propri profitti in ricerca e sviluppo o di agire nell'interesse pubblico con un mandato riconosciuto dal governo.

La direttiva InfoSoc consente l'inclusione incidentale di un'opera "in altro materiale" ai sensi dell'articolo 5(3)(i). Tuttavia, il Tribunale di Monaco ha respinto questo argomento, affermando che la legge richiede che il materiale più ampio sia esso stesso un'opera. In assenza di un'opera principale, le riproduzioni dei testi delle canzoni in questione non costituiscono un accessorio inammissibile ai sensi del § 57 UrhG.

Gli output contestati costituiscono altresì una messa a disposizione del pubblico ai sensi dell'art. 3 della direttiva InfoSoc. Le convenute consentono a una pluralità indeterminata di utenti di accedere ai contenuti generati mediante il chatbot. In particolare, la possibilità di salvare le conversazioni, richiamarle in un momento successivo e condividerle tramite link pubblici indicizzabili dai motori di ricerca apre l'accesso ai contenuti a un pubblico potenzialmente illimitato. È sufficiente che le opere siano rese disponibili in modo tale che i membri del pubblico possano accedervi dal luogo e nel momento scelti individualmente.

OpenAI ha cercato di evitare l'inibitoria sostenendo che tale rimedio drastico sarebbe sproporzionato. Il Tribunale ha tuttavia osservato che i titolari dei diritti o coloro che ottengono una licenza esclusiva da essi hanno diritto a un provvedimento inibitorio.

Il Tribunale ha inoltre rifiutato di esonerare OpenAI dalla responsabilità solo perché esistono siti web di terze parti dove i testi delle canzoni in questione possono essere ottenuti gratuitamente. L'uso da parte di altri, che potrebbe essere non autorizzato, non legalizza la memorizzazione e la riproduzione senza permesso.

Questa decisione potrebbe avere ripercussioni significative sull'industria dei sistemi di IA generativa, imponendo la necessità, almeno in Europa, di acquisire licenze per l'utilizzo di opere protette nell'addestramento dei modelli e aprendo la strada a nuovi modelli di business basati sulla remunerazione equa dei creatori di contenuti.

GEMA ha prevalso su quasi tutti i punti, ma le pretese fondate sui diritti morali, relative all'alterazione dell'integrità dei testi, invece, sono state respinte. Secondo la Corte, trattandosi di diritti strettamente personali, non trasferibili né azionabili in via di rappresentanza processuale, le domande fondate su tali diritti sono pertanto inammissibili. L'8 dicembre 2025, GEMA ha, quindi, presentato appello contro l'inibitoria del tribunale tedesco (numero di appello: 6 U 3662/25) presso l'Oberlandesgericht München (Corte Regionale Superiore di Monaco).

In attesa di conoscere l'esito dell'appello, il parallelo procedimento per violazione del diritto d'autore promosso da GEMA contro il fornitore di IA Suno è incardinato nello stesso tribunale con udienze fissate nel 2026. In quel caso si tratta di composizioni musicali anziché di testi.

FRANCESCO GROSSI

<https://www.euipo.europa.eu/it/law/recent-case-law/the-higher-regional-court-of-munich-considered-memorization-and-temporary-copies-occurred-in-model-training-as-infringing-reproductions-of-works>

2025/4(44)FR

La sentenza della High Court of England and Wales del 4.11.2025 nel caso Getty Images contro Stability AI in materia di tutela del diritto d'autore, addestramento di modelli di IA generativa e ruolo dei "pesi"

Il 4 novembre 2025 la *High Court of Justice Business and Property Courts of England and Wales* (la **Corte**) ha pronunciato una [sentenza](#) nel caso Getty Images (US) Inc & Ors c. Stability AI Limited [2025] EWHC 2863 (Ch) (la **Sentenza**).

La controversia è stata promossa da varie società del gruppo Getty Images (collettivamente **Getty**), attive nella concessione in licenza di fotografie, video, illustrazioni e relativi metadati di alta qualità su diverse piattaforme, nei confronti di Stability AI Limited (**Stability AI**), società registrata nel Regno Unito e provider di **Stable Diffusion**, un modello di deep learning per la generazione di immagini basato su tecniche di diffusione latente, inizialmente sviluppate da ricercatori della LMU di Monaco e dell'IWR di Heidelberg – per violazione di diritti di proprietà intellettuale di Getty.

Il procedimento ha preso avvio il 16 gennaio 2023, quando Getty ha promosso l'azione contro Stability AI deducendo:

- (i) una **violazione "primaria"** o "diretta" del **diritto d'autore** ("*primary copyright infringement*") per le attività di *web scraping* e di addestramento del modello (il c.d. "**Training and Development Claim**") e per la generazione di output potenzialmente lesivi dei diritti d'autore (il c.d. "**Output Claim**");
- (ii) una **violazione "secondaria"** del diritto d'autore ("*secondary copyright infringement*");
- (iii) una violazione della disciplina sulle **banche dati** (il c.d. "*Database Rights Infringement Claim*");

- (iv) una violazione del diritto dei **marchi**, ivi inclusa l'ipotesi di “*passing off*” (“abuso di denominazione”).

Quanto alle prime due rivendicazioni, val la pena sin da subito evidenziare come ai sensi del Copyright, [Designs and Patents Act 1988](#) (CDPA), una violazione “primaria” o “diretta” del diritto d'autore può sussistere ogniqualvolta vi siano atti di riproduzione diretta di opere protette dal diritto d'autore, laddove invece gli “atti di violazione secondaria” del diritto d'autore riguardano le attività illecite condotte “a valle” (“*downstream dealings or involvement*”) (par. 543 Sentenza).

Nel corso del giudizio, l'oggetto della controversia si è notevolmente ridotto in seguito alla presa d'atto, da parte di Getty, che (a) non vi fossero prove sufficienti che lo sviluppo e l'addestramento di Stable Diffusion avessero avuto luogo nel Regno Unito (cfr. parr. 9 e 100 della Sentenza); e che (b) i prompt asseritamente utilizzati per generare output in violazione del diritto d'autore, prodotti come prova nel procedimento, fossero stati bloccati da Stability AI nel corso del giudizio e che, pertanto, la tutela cui Getty Images avrebbe avuto diritto in relazione alle proprie accuse di violazione primaria del diritto d'autore risultava, in ogni caso (anche ove in ipotesi fondata), sostanzialmente già conseguita (par. 9 Sentenza).

Tali constatazioni hanno portato alla rinuncia, da parte di Getty, della richiesta di risarcimento per violazione diretta del diritto d'autore e, conseguentemente, di quella di violazione del diritto sulle banche dati (par. 9 Sentenza).

Il processo si è quindi concentrato sulle mere rivendicazioni relative al diritto dei marchi e sulla violazione secondaria del diritto d'autore, lasciando la risoluzione delle altre questioni a futuri contenziosi o a un intervento legislativo.

Quanto alla violazione del diritto dei marchi, Getty sosteneva che Stability AI avesse posto in essere atti in violazione delle proprie prerogative ai sensi delle sezioni 10(1), 10(2) e 10(3) del *Trade Marks Act* 1994 (TMA), in quanto alcuni output generati da Stable Diffusion recavano **filigrane** (“*watermarks*”) identiche o simili ai marchi di cui Getty è titolare e che, pertanto, Stability AI avesse utilizzato tali segni distintivi nell'ambito della prestazione dei propri servizi, segnatamente nella fornitura di immagini sintetiche (par. 134 Sentenza).

Stability AI, dal canto suo, riconosceva che fosse “possibile” che taluni output contenessero filigrane recanti segni identici o simili ai marchi Getty e ammetteva, nelle proprie conclusioni, che Stable Diffusion potesse essere “spinto” (“*push*”) a generare tali filigrane mediante specifici prompt (par. 138 Sentenza). Essa sosteneva tuttavia che le prove offerte non fossero sufficienti a soddisfare l'onere probatorio gravante su Getty in ordine all'avvenuta violazione dei marchi, anche in considerazione del fatto che quest'ultima non aveva fornito alcuna dimostrazione circa la probabilità statistica che le diverse versioni del modello potessero generare immagini recanti tali filigrane.

A tali argomentazioni Getty si opponeva con fermezza, sottolineando come la difesa di Stability AI su tale punto fosse, nella migliore delle ipotesi, equivoca e come il proprio onere probatorio non si estendesse fino a

comprendere la dimostrazione dell’“esistenza di una determinata probabilità che uno dei modelli generasse immagini recanti filigrane”.

La Corte, seppur solo in relazione a un numero limitato di casi (par. 453 e 465), ha accolto la domanda di Getty per le violazioni di cui alle sezioni 10(1) e 10(2) TMA, rispettivamente per la riproduzione di marchi identici per servizi identici a quelli del titolare e per la riproduzione di marchi identici per servizi simili, nonché di marchi simili per servizi identici a quelli coperti dal marchio, non accogliendo, invece, la richiesta di risarcimento presentata da Getty ai sensi della Sezione 10(3) del TMA per violazione del marchio che goda di una certa reputazione, non trovando prove che gli output generati dall'intelligenza artificiale avessero recato pregiudizio al marchio Getty (par. 25 Sentenza). Sulla base di tali considerazioni e, vista la loro interconnessione con l'azione di “passing off”, la Corte ha rigettato altresì quest’ultima domanda.

Quanto alla “violazione secondaria del copyright”, Getty sosteneva che Stable Diffusion dovesse essere considerata una “copia illecita” (“*infringing copy*”) ai sensi delle sezioni 22 e 23 CDPA, in combinato disposto con l’art. 27(3) CDPA. Riteneva ciò sulla base della considerazione che il modello fosse stato importato nel Regno Unito (principalmente mediante download) e che il suo sviluppo e addestramento, qualora fossero avvenuti nel Regno Unito, avrebbero di certo costituito una violazione del diritto d’autore (par. 544 Sentenza). In particolare, Getty sosteneva che i suoi pesi (“*model weights*”) avrebbero costituito “copie” potenzialmente lesive del diritto d’autore.

Stability AI respingeva tale argomentazione, sostenendo che il modello non contenesse “copie”, ovvero riproduzioni, di alcuna immagine protetta dal diritto d’autore.

La Corte ha identificato sul punto due principali questioni giuridiche: (1) se Stable Diffusion possa essere ritenuto un “**articolo**” (“*article*”) ai sensi degli articoli 22 e 23 CDPA, e (2) se lo stesso, se e in quanto articolo, possa essere considerato una “**copia illecita**” ai sensi dell’art. 27 CDPA.

Getty Images sosteneva che a entrambe tali questioni si dovesse rispondere in senso affermativo.

Essa evidenziava come la definizione di “copia illecita” contenuta nella sezione 27(3) CDPA fosse sufficientemente ampia da ricomprendere un qualsiasi bene (ivi incluso un bene immateriale) la cui creazione o “realizzazione” (“*making*”) abbia comportato una violazione del diritto d’autore.

Rilevava, inoltre, che era pacifico tra le parti che l’addestramento del modello avesse comportato la riproduzione delle opere di propria titolarità, mediante **memorizzazione**, sia su sistemi locali sia su risorse di cloud computing.

Sosteneva che, nel caso di specie, l’“articolo” di cui alla sezione 27(3) CDPA non fosse il modello in sé – non costituendo esso una riproduzione di opere protette – bensì **i suoi pesi** (“*model weights*”), la cui “realizzazione”, o più propriamente ottimizzazione, aveva richiesto la loro ripetuta esposizione ai dati di addestramento.



Affermava infine che, se la realizzazione del modello fosse avvenuta nel Regno Unito, essa avrebbe integrato una violazione ai fini della sezione 27(3) CDPA.

Dal canto suo, Stability AI si opponeva alle pretese di Getty, sostenendo che il concetto di “article” di cui alla normativa vigente si riferisce esclusivamente a un bene materiale e che, considerato che l’addestramento di Stable Diffusion era avvenuto negli Stati Uniti e che il modello non contenesse al proprio interno copie (riproduzioni) delle opere di titolarità di Getty, esso non potesse integrare la nozione di “copia illecita” di cui all’art. 27(3) CDPA.

Accogliendo parzialmente tali argomentazioni, **la Corte ha ritenuto che i modelli Stable Diffusion, pur potendo essere qualificati come “articoli” ai sensi della normativa vigente, non contengono né conservano riproduzioni delle opere sulle quali sono stati addestrati e che, conseguentemente, non costituiscono “*infringing copies*” ai fini della fattispecie di violazione secondaria del diritto d’autore.**

La Corte è giunta a questa conclusione basandosi sul principio “*always speaking*” (ovvero, che le leggi devono essere interpretate in modo da applicarsi nel tempo anche alle nuove circostanze e tecnologie – par. 580 Sentenza) e su una lettura sistematica del CDPA.

Più nello specifico, quanto alla questione se Stable Diffusion potesse essere considerato un “articolo” ai sensi della normativa vigente, **la Corte ha affermato che un bene immateriale ben possa essere considerato un “articolo”**. La Corte ha, infatti, sottolineato che la sezione 17 CDPA (contenente la definizione del diritto di riproduzione) prevede espressamente che la “copia” di un’opera dell’ingegno possa avvenire “in qualsiasi supporto mediante mezzi elettronici” e che negare la tutela contro la violazione secondaria unicamente perché il supporto di memorizzazione è intangibile risulterebbe incoerente con tale previsione (parr. 562 ss. Sentenza).

Richiamando casi come Sony v Ball e C-433/20 Austro-Mechana, la Corte ha, in particolare, ritenuto che “lo scopo della legge - la protezione dei titolari del diritto d’autore – sarebbe (...) soddisfatto” soltanto da un’interpretazione che includa nel concetto di ‘articolo’ anche ‘le moderne tecnologie’ (par. 580)”. Diversamente, ha motivato la Corte, gli autori verrebbero privati di tutela in tutti i casi in cui la copia sia elettronica e venga trattata per via digitale e “ciò non solo sarebbe incoerente con il testo della legge, ma anche con l’impianto complessivo della protezione del diritto d’autore, che mira a ricompensare gli autori per i loro sforzi creativi” (par. 590).

Quanto alla seconda questione (se Stable Diffusion costituisca una “*infringing copy*”), **la Corte ha ritenuto che Getty non abbia fornito prova dell’avvenuta memorizzazione**, all’interno del modello, di specifiche opere di propria titolarità (par. 559 Sentenza) e che, pertanto, il modello non possa essere qualificato come “copia illecita” ai sensi della normativa vigente.

In particolare, la Corte ha osservato che **i pesi** di ciascuna versione di Stable Diffusion non contengono, né hanno mai contenuto, riproduzioni delle opere di titolarità di Getty: essi rappresentano il risultato di un addestramento (o meglio, dei “pattern e delle caratteristiche appresi nel tempo durante il processo di training” – par. 600 Sentenza) e, in quanto tali, **non costituiscono essi stessi copie delle opere in questione.**

Secondo la Corte, tale conclusione è specifica con riferimento al modello Stable Diffusion e potrebbe non estendersi ad altri modelli di diffusione, poiché **la valutazione del funzionamento del singolo sistema deve essere compiuta caso per caso**.

Con riguardo al funzionamento di Stable Diffusion, ad ogni modo, la Corte ha chiarito che esso, a differenza di altri modelli, si fonda sul **processo di “inferenza”**, definito come “(in termini semplici) un sistema input-output in cui l’utente specifica gli input, la rete addestrata esegue calcoli su tali input e genera l’output desiderato”, e che **“l’inferenza non richiede l’uso dei dati di addestramento”, con la conseguenza che “il modello stesso non conserva i dati di addestramento”** (parr. 5 e 7 Sentenza).

La Sentenza è senza dubbio una pronuncia di particolare rilievo, sia perché affronta per la prima volta nel Regno Unito taluni aspetti relativi alle interazioni tra i diritti di proprietà intellettuale e lo sviluppo, l’addestramento e l’utilizzo di sistemi di intelligenza artificiale, sia perché fornisce un’interpretazione di alcuni concetti di diritto d’autore della normativa d’Oltremania (tra cui quello di “article” di cui alla sezione 27 CDPA) che fino ad oggi erano stati oggetto di un numero limitato di decisioni giurisprudenziali.

FRANCESCA ROTOLO

<https://www.judiciary.uk/wp-content/uploads/2025/11/Getty-Images-v-Stability-AI.pdf>

2025/4(45)FZ

Il provvedimento interlocutorio del Giudice Donato del 6.11.2025 nel caso *Fortnite*: l’accordo transattivo Epic Games–Google tra rimedi antitrust e regolazione privata del mercato delle app

Il contenzioso tra Epic Games Inc. (**Epic Games**) e Google LLC (**Google**), che ha interessato il prodotto di punta della Epic Games, il videogame *Fortnite*, avviato nel 2020 e giunto a una prima svolta decisiva con il verdetto dell’11 dicembre 2023 e la successiva *permanent injunction* del 7 ottobre 2024, continua a rappresentare uno dei casi più rilevanti nel dibattito contemporaneo sul diritto della concorrenza nei mercati digitali. Come già analizzato in questa Rubrica nel contributo n. 28 del numero [4/2023](#) ([2023/4(28)FP] in *PeM* 2023, p. 807 e in *Atlante*, p. 485), la decisione aveva accertato l’abuso di posizione dominante di Google nel Play Store, aprendo una nuova fase nella quale la questione dei rimedi assumeva un ruolo centrale. In tale contesto, il baricentro del contenzioso si è, pertanto, progressivamente spostato dall’accertamento dell’abuso alla definizione di rimedi capaci di incidere in modo effettivo e strutturale sull’assetto concorrenziale del mercato.

L’annuncio, nel novembre 2025, di un accordo transattivo tra le parti volto a chiudere la storica controversia sul Google Play Store ha alimentato una



narrazione di “svolta definitiva”, prospettando una riscrittura delle regole di funzionamento del Play Store e, più in generale, dell’ecosistema Android.

L’ingiunzione del 7 ottobre 2024, confermata in secondo grado, ha imposto a Google una serie di obblighi strutturali, tra cui l’apertura del Play Store a sistemi di pagamento alternativi e la possibilità di installare *store* di terze parti; è su questo impianto che si innesta l’accordo negoziato con Epic Games, il quale non elimina l’ingiunzione, ma ne propone una riformulazione concordata. In particolare, esso prevede due direttrici principali di intervento:

- 1) in primo luogo, in materia di metodi di pagamento, fino al 30 giugno 2032 gli sviluppatori potranno mostrare all’interno delle app sistemi di pagamento alternativi a quello di Google. In funzione della tipologia di acquisto, Google applicherà una commissione di servizio pari al 20% o al 9%, cui si aggiunge un’ulteriore trattenuta del 5% nel caso in cui venga utilizzato il sistema di pagamento proprietario. Nessuna commissione aggiuntiva è prevista qualora l’utente scelga un metodo di pagamento alternativo;
- 2) in secondo luogo, con riferimento agli *store* di terze parti, l’accordo conferma la possibilità di *sideloading*, ma introduce i cosiddetti “*Registered App Store*”, ovverosia *store* certificati da Google, installabili con un solo clic dal *web*, previo rispetto di requisiti minimi di sicurezza e *privacy* definiti dalla stessa Google, che potrà richiedere una commissione a copertura dei costi di certificazione.

Si tratta, dunque, di un accordo che incide in modo significativo sull’assetto del Play Store, ma che mantiene un ruolo centrale per Google nella definizione delle condizioni di accesso al mercato.

Proprio in virtù di tale elemento – ritenuto principale fattore di criticità – l’accordo ha incontrato un ostacolo significativo. Nel corso dell’udienza del 6 novembre scorso, infatti, il giudice federale James Donato, che presiede il caso *Epic Games Inc. v. Google LLC*, ha espresso scetticismo, sollevando seri dubbi sulla legalità e la portata dell’intesa. Le perplessità manifestate dal giudice Donato – culminate nel **rinvio dell’approvazione dell’accordo e nella fissazione di un’udienza probatoria** – appaiono tutt’altro che sorprendenti.

L’accordo sembra infatti muovere da un presupposto problematico: **l’idea che l’abuso accertato possa essere corretto attraverso un insieme di regole negoziate, affidando al medesimo soggetto ritenuto responsabile dell’illecito un potere regolatorio sostanzialmente intatto.**

Quanto ai metodi di pagamento, la possibilità di indicare sistemi alternativi non equivale necessariamente a una neutralità economica. La permanenza di una *service fee* significativa, unita al controllo di Google sull’architettura tecnica e sull’esperienza utente, rischia di tradurre l’alternativa in una mera opzione formale, potenzialmente disincentivata sul piano economico o funzionale.

Il tema, ben noto nel diritto antitrust, non è tanto l’esistenza astratta di una scelta, quanto la sua effettiva praticabilità in termini concorrenziali.

Analoghe considerazioni valgono per gli *store* di terze parti. La creazione di un registro ufficiale gestito da Google, con requisiti e costi di certificazione definiti unilateralmente, solleva interrogativi sulla reale apertura del mercato. Piuttosto che rimuovere il potere di *gatekeeping*, l'accordo sembra trasformarlo, sostituendo al controllo diretto sull'accesso un potere di autorizzazione e certificazione che consente comunque a Google di incidere selettivamente sulla struttura del mercato.

In una simile prospettiva, il rischio è che i rimedi si traducano in una forma di regolazione privata della concorrenza, nella quale l'apertura del mercato è concessa e amministrata dal *gatekeeper* stesso, anziché garantita da regole esterne e neutrali.

È alla luce di tali ambiguità che si comprende la decisione del giudice Donato di sottoporre l'accordo a un vaglio probatorio: nel diritto antitrust statunitense, infatti, l'approvazione giudiziale di un accordo che modifica un'ingiunzione non si limita a una verifica formale del consenso delle parti, ma implica una valutazione sostanziale dell'idoneità dei rimedi a eliminare gli effetti anticoncorrenziali accertati.

Il fatto che il giudice abbia disposto un'udienza probatoria, rinviando l'approvazione dell'accordo, segnala la consapevolezza che la questione non riguarda più soltanto il comportamento passato di Google, bensì la legittimità di un nuovo assetto di mercato destinato a durare per un periodo lungo (perlomeno fino al 2032) e, in parte, ad avere effetti globali. In altri termini, il tribunale è chiamato a decidere se stia realmente correggendo un abuso o se, al contrario, stia avallando una nuova configurazione del potere di mercato.

Sotto questo profilo, la fase attuale del contenzioso conferma le analisi già sviluppate nel 2023. La vittoria di Epic contro Google, lungi dal fondarsi su una teoria antitrust univoca e generalizzabile, appare il risultato di una combinazione di fattori – delimitazione ristretta del mercato, accertamenti fattuali, comportamento processuale delle parti – che rende particolarmente delicata la fase dei rimedi.

L'accordo Epic–Google non smentisce tali considerazioni, ma ne rappresenta un naturale sviluppo: l'instabilità teorica della decisione si riflette nella difficoltà di individuare rimedi capaci di incidere strutturalmente sul mercato senza ricadere in forme di regolazione privatizzata. In questo senso, la prudenza del giudice appare coerente con la funzione pubblicistica dell'*enforcement* antitrust, che non può essere integralmente delegata alla contrattazione tra imprese, per quanto formalmente contrapposte.

Il confronto con l'esperienza europea, segnata dall'entrata in vigore del reg. (UE) 2022/1925 (Digital Markets Act, **DMA**), rafforza ulteriormente questa lettura. Mentre il DMA opta per una regolazione *ex ante* dei *gatekeeper*, sottraendo loro la possibilità di definire unilateralmente le condizioni di accesso, il caso Epic–Google mostra i limiti di un approccio affidato prevalentemente all'*enforcement* giudiziario *ex post* e alla negoziazione dei rimedi.

L'accordo Epic–Google non rappresenta, dunque, la conclusione del contenzioso né una soluzione definitiva ai problemi concorrenziali del mercato delle app; esso segna piuttosto il passaggio a una fase nella quale il

nodo centrale diventa la legittimità di una regolazione della concorrenza affidata al soggetto che ne è stato ritenuto responsabile.

La decisione del giudice Donato di sottoporre l'accordo a un vaglio probatorio conferma che la posta in gioco non è la soddisfazione delle parti, ma la tutela dell'interesse pubblico alla concorrenza. Resta da vedere se i rimedi proposti sapranno superare questo scrutinio, dimostrando di incidere realmente sulla struttura del mercato, o se il contenzioso *Epic v. Google* continuerà a essere, come già accaduto in passato, un laboratorio aperto delle tensioni tra antitrust, mercati digitali e potere dei *gatekeeper*.

FRANCESCA ZAMPONE

<https://www.documentcloud.org/documents/26215006-epic-and-googles-argument-for-modified-injunction/>
<https://www.documentcloud.org/documents/26214893-epic-and-googles-proposed-modified-injunction/>

Banca Centrale Europea

*Le opinioni o i punti di vista espressi sono esclusivamente dell'autore e non dell'istituzione

2025/4(46)RP

La legge dello Stato di New York “The Responsible Artificial Intelligence Safety and Education” (RAISE Act) sui modelli di intelligenza artificiale “di frontiera”. Il comunicato stampa della Governatrice del 19.12.2025 e la nuova proposta legislativa dell'8.01.2026.

Il 19 dicembre 2025, a breve distanza dall'[ordine esecutivo](#) “*Ensuring a National Policy Framework for Artificial Intelligence*”, con cui il Presidente Trump ha promosso l'adozione di uno standard nazionale unitario in materia di intelligenza artificiale che limita le iniziative regolatorie statali (su cui v. *supra*, in questo numero di questa Rubrica la notizia n. 1 [2025/4(1)SO]), lo Stato di New York ha adottato il *Responsible AI Safety and Education Act* (RAISE Act). Il testo di legge mira a garantire la sicurezza e la trasparenza dei modelli di IA “più avanzati” o “di frontiera” (c.d. “*frontier models*”), ossia quelli addestrati con ingenti quantità di dati e con una potenza di calcolo superiore a 10^{26} FLOPs. Tali modelli si distinguono per capacità inedite ed elevate potenzialità di innovazione in molteplici settori strategici; elementi che, se da un lato accrescono i benefici dell'intelligenza artificiale per la collettività, dall'altro amplificano i rischi connessi al suo impiego, giustificando l'esigenza di un intervento normativo ad hoc.

Il RAISE Act è stato votato a larghissima maggioranza da entrambe le Camere ([S6953B/A6453B](#)) nel giugno 2025. A distanza di sei mesi, la legge è stata firmata dalla Governatrice Kathy Hochul, a condizione che, nel corso della sessione legislativa successiva, vi fossero apportate alcune modifiche, stabilite d'intesa con il legislatore statale e rese note mediante un comunicato stampa ([Governor's Press Office, 19.12.2025](#)). In particolare, gli interventi

emendativi concordati in sede di confronto istituzionale si concentrano su tre ambiti rilevanti della nuova disciplina dell'IA di frontiera, inserita nell'[Articolo 44-B, capitolo 20, della legge generale sul commercio](#). In primo luogo, si assume l'impegno di riformare gli obblighi imposti ai “grandi sviluppatori” (c.d. *large frontier developers*) che realizzano, implementano o utilizzano, anche solo in parte, tali modelli nel territorio dello Stato. Si ritiene opportuno, infatti, fornire a questi ultimi indicazioni più dettagliate in ordine sia al contenuto dei protocolli di sicurezza da redigere e pubblicare, sia alla procedura da seguire per la segnalazione degli incidenti critici legati al funzionamento o all'uso dell'IA che comportano un grave rischio per la collettività. Ulteriori modifiche riguardano, in secondo luogo, le sanzioni comminate ai grandi sviluppatori in caso di inadempimento, convenendo che oscillino non più tra dieci milioni per la prima violazione e trenta milioni di dollari per ogni violazione successiva, bensì, rispettivamente, tra un milione e tre milioni di dollari. Infine, in terzo luogo, si prevede di istituire un nuovo organo di controllo all'interno del *Department of Financial Services* (DFS) di New York, a cui affidare compiti di vigilanza e la definizione di standard specifici per la sicurezza e la trasparenza dei modelli di frontiera.

In attuazione del suddetto accordo politico, in data 8 gennaio 2026, è stata posta all'esame dell'Assemblea e del Senato statali una nuova proposta di legge ([S8828/A09449](#)) volta a introdurre, a decorrere dal 1° gennaio 2027, nuovi requisiti di trasparenza e sicurezza per gli sviluppatori di intelligenza artificiale avanzata. La proposta non si limita a emendare, in alcune parti, il testo del RAISE Act, ma ne dispone l'abrogazione, operando una riscrittura integrale della normativa sull'IA di frontiera.

Tra le principali innovazioni, che segnano un allontanamento significativo dalla disciplina inizialmente approvata dal legislatore newyorkese, spicca l'eliminazione del divieto per i grandi sviluppatori di utilizzare o rendere disponibili a soggetti terzi i modelli di frontiera, quando appaia irragionevole esporre la collettività a danni gravissimi e irreparabili. In particolare, il divieto di cui all'Art. 44-B, §1421(2), Gen. Bus. L., nel suo testo originario, riguarda ogni uso dell'intelligenza artificiale che presenti un rischio sproporzionato di morte o lesioni per almeno cento persone, o di danno non inferiore a un miliardo di dollari, derivante dalla creazione di armi chimiche, biologiche, radiologiche o nucleari, dalla realizzazione di cyberattacchi o dalla commissione di gravi reati (c.d. “*unreasonable risk of critical harm*”). La nuova proposta legislativa, al contrario, prescinde dal valutare l'entità, l'estensione, la probabilità ed evitabilità dei suddetti rischi dell'IA in rapporto ai benefici che possono derivare dal suo impiego. Contro tali eventualità altamente dannose, infatti – ricondotte ora alla più ampia categoria dei “rischi catastrofici” (c.d., *catastrophic risks*), in cui sono inclusi sia i danni all'incolumità di cinquanta persone sia l'elusione, da parte dell'IA, del controllo umano – la proposta adotta solo degli obblighi di trasparenza, senza più porre alcuna limitazione sostanziale all'utilizzo o alla diffusione dell'intelligenza artificiale, in circostanze in cui appare inaccettabile esporre la collettività a pericoli così elevati. Si tratta di una modifica che ridefinisce in profondità l'approccio regolatorio del RAISE Act, allineandolo al modello

normativo in materia di IA di frontiera adottato dalla California nel settembre 2025 ([*Transparency in Frontier Artificial Intelligence Act*](#) (TFAIA - SB 53)). Un'ulteriore novità riguarda gli obblighi di trasparenza che, diversamente da quanto disposto nel testo originario della legge di New York, sono stati parzialmente modificati, incrementati ed estesi a una platea più ampia di soggetti. La proposta legislativa, infatti – in aderenza al TFAIA – non si rivolge più esclusivamente ai grandi sviluppatori di IA avanzata, ma, in generale, a chiunque addestri un modello di frontiera. Al contempo, però, nel caso in cui le prescrizioni di legge non siano rispettate, si consente all'*Attorney General* di agire (per un importo che, come preannunciato, è stato ridotto, conformemente alla legge californiana, di dieci volte rispetto alla disciplina iniziale) soltanto nei confronti dei suddetti grandi sviluppatori (§ 1427). Tale complessiva, limitata capacità sanzionatoria del nuovo testo del RAISE Act non è stata, tuttavia, compensata mediante un rafforzamento delle tutele per i lavoratori che denunciano gli illeciti aziendali. A differenza della legge adottata in California, infatti, non vi è alcuna disciplina a favore dei *whistleblowers* che segnalano alle autorità competenti problemi di sicurezza connessi ai modelli di frontiera. Il testo si snoda, piuttosto, lungo un articolato reticolo di prescrizioni rivolte alla generalità degli sviluppatori di IA avanzata e di obblighi aggiuntivi destinati ai c.d. *large frontier developers*, i quali non sono più definiti come coloro che hanno investito oltre cento milioni in costi computazionali, bensì – sull'esempio della normativa californiana – identificati soltanto in base al loro fatturato annuale, superiore a cinquecento milioni di dollari (§ 1420(10)).

Per un verso, tutti i soggetti coinvolti nello sviluppo dell'IA di frontiera, a prescindere dalla spesa sostenuta in infrastrutture di calcolo e dal fatturato, sono ora tenuti a pubblicare sul proprio sito web un documento (c.d. *transparency report*) che renda noti, prima o contestualmente alla distribuzione di un nuovo modello, le caratteristiche principali di quest'ultimo e i contatti dello sviluppatore (§ 1421(3)(a)). Sui medesimi soggetti grava altresì l'obbligo di riportare, entro settantadue ore (dunque, entro un tempo assai più breve dei quindici giorni concessi dal TFAIA), il verificarsi di incidenti critici per la sicurezza (c.d. *critical safety incidents*) (§ 1422(3)). Tali eventi consistono, segnatamente, nell'accesso, modifica o estrazione non autorizzati dei valori numerici da cui dipendono gli output del modello di frontiera o nella perdita di controllo su di esso, ove ciò provochi morte o lesioni fisiche; nella realizzazione di danni conseguenti alla materializzazione di un rischio catastrofico; nonché nell'elusione inaspettata, mediante tecniche ingannevoli, da parte della stessa IA, dei sistemi di supervisione del proprio sviluppatore, con aumento sostanziale del rischio catastrofico (§ 1420(4)). A differenza di quanto previsto in precedenza, la nuova proposta di legge richiede che la segnalazione sia indirizzata non all'*Attorney General* e alla Divisione per la Sicurezza Interna e i Servizi di Emergenza dello Stato di New York, bensì al nuovo ufficio istituito presso il DFS, che valuterà discrezionalmente se condividere o meno tali informazioni riservate con altre autorità. Nell'ipotesi di rischio imminente di morte o lesioni, però, come stabilito anche nel TFAIA, la comunicazione deve essere effettuata dallo sviluppatore entro ventiquattro ore e trasmessa all'autorità che lo stesso

ritiene più appropriata, inclusa qualsiasi agenzia di polizia o di sicurezza pubblica. Gli sviluppatori, ad ogni modo, possono assolvere ai suddetti obblighi di segnalazione in maniera alternativa, vale a dire conformandosi ad altri requisiti e/o standard di trasparenza e sicurezza, non inferiori a quelli statali, introdotti con leggi, norme o altri documenti federali, elencati in un apposito regolamento adottato dal DFS (§ 1422(9)).

Per un altro verso, nella nuova proposta di legge, i grandi sviluppatori, oltre a rispettare i doveri di trasparenza e di segnalazione sopra riportati, sono soggetti ad obblighi integrativi. I *large frontier developers*, infatti, in primo luogo, devono garantire la redazione e la pubblicazione annuale, sul proprio sito Internet, di un protocollo di sicurezza (c.d. *frontier AI framework*) per la gestione, l'accertamento e la mitigazione dei rischi catastrofici derivanti dall'uso, non solo esterno (come previsto nell'originario testo del RAISE Act) ma anche interno, dei propri modelli di frontiera (§ 1421(1)). In secondo luogo, devono includere nel proprio *transparency report* una sintesi delle valutazioni dei suddetti rischi, dei relativi risultati, del grado di coinvolgimento di valutatori terzi, nonché delle ulteriori misure adottate in attuazione dei rispettivi protocolli (§ 1421(3)(b)). Gli esiti degli accertamenti inerenti all'uso interno dell'IA devono, inoltre, essere riferiti trimestralmente, in forma sintetica e riservata, al nuovo ufficio presso il DFS, che valuta se trasmettere tali informazioni ad altre autorità governative (§ 1422(2)(a)). Infine, in terzo luogo, si richiede ai grandi sviluppatori di intelligenza artificiale all'avanguardia che intendono iniziare a operare nello Stato di depositare presso il suddetto ufficio una dichiarazione (c.d. *disclosure statement*), aggiornata ogni due anni, in cui siano specificati l'identità, l'indirizzo, le denominazioni commerciali e i referenti dello sviluppatore, nonché i soggetti che detengono, direttamente o indirettamente, un interesse economico pari o superiore al cinque per cento nella sua attività (§ 1428(3)). Essi sono altresì tenuti al pagamento, pro quota, di un contributo per le spese connesse all'amministrazione degli obblighi imposti dal RAISE Act. In caso di omessa o falsa dichiarazione, nonché di ritardo nei versamenti richiesti, si prevede che l'ufficio possa applicare una sanzione di mille dollari per ciascun giorno di violazione, cui si aggiunge una somma equivalente all'importo dovuto (§ 1428(5)).

Da ultimo, la proposta legislativa stabilisce che, a partire dal 1° gennaio 2028, il nuovo ufficio del DFS competente in materia di modelli di frontiera rediga un resoconto annuale che faciliti la comprensione e il monitoraggio, da parte degli organi politici, dei rischi dell'intelligenza artificiale avanzata. Tale report deve includere, in forma anonimizzata, i dati ricevuti ogni tre mesi dai grandi sviluppatori sulle valutazioni relative agli usi interni dell'IA e, altresì, le informazioni tratte dalle segnalazioni di incidenti critici, salvo che ciò possa compromettere i segreti commerciali o costituire una violazione di legge o un pericolo per la sicurezza informatica o pubblica (§ 1422(7)). L'ufficio è, infine, autorizzato ad adottare ogni ulteriore regola necessaria all'attuazione delle disposizioni del RAISE Act, inclusa l'introduzione di requisiti supplementari di segnalazione o di pubblicazione, volti a favorire maggiore sicurezza e trasparenza nell'uso dei modelli di frontiera (§ 1429).

Nel suo complesso, la disciplina dello Stato di New York in materia di intelligenza artificiale avanzata, così come delineata dalla recente proposta legislativa, si discosta notevolmente dall'impianto originario del RAISE Act, attenuandone i profili di originalità a favore dell'adesione al quadro normativo californiano, ormai assunto quale modello di riferimento. Tale risultato, tuttavia, non configura solo un indice di indebolimento della regolazione statale dell'IA di frontiera, ma riflette una strategia politica precisa, coerente con l'obiettivo dichiarato di «creare un modello legislativo di riferimento comune tra gli Stati tecnologicamente avanzati del Paese, supplendo all'inerzia del governo federale, che non riesce ad attuare norme di buon senso a tutela della collettività» ([Governor's Press Office, 19.12.2025](#)).

ROSALBA POTENZANO

<https://www.governor.ny.gov/news/governor-hochul-signs-nation-leading-legislation-require-ai-frameworks-ai-frontier-models>

2025/4(47)FF

La legge dell'Illinois del 1.8.2025 che proibisce di affidare decisioni terapeutiche a sistemi di IA (il *Wellness and Oversight for Psychological Resources Act*)

Il 1° agosto 2025 lo Stato dell'Illinois ha approvato il [Wellness and Oversight for Psychological Resources Act](#) (HB 1806), ossia la **Legge sul Benessere e la Supervisione delle Risorse Psicologiche**. La legge, entrata in vigore immediatamente, al momento della sua promulgazione (**Section 99**), a seguito della firma del Governatore J.B. Pritzker, mira a limitare l'uso dell'intelligenza artificiale nei servizi di terapia e psicoterapia – intesi come i servizi prestati per diagnosticare, trattare o migliorare la salute mentale o comportamentale di un individuo – limitandone l'uso consentito a funzioni meramente amministrative e di supporto supplementare. Come esplicitato nella **Section 5**, la finalità primaria del testo è quella di tutelare gli individui che si rivolgono a servizi di salute mentale, garantendo che tali prestazioni siano erogate da professionisti qualificati e autorizzati, e di proteggere i consumatori dal rischio di interazioni con fornitori non legittimati. Al contempo, la legge afferma il rispetto della libertà di scelta individuale e dell'accesso a forme di supporto alla salute mentale basate sulla comunità o sulla fede, che restano escluse dall'ambito delle restrizioni introdotte.

In un [comunicato stampa](#) del 4 agosto 2025, il Segretario del Dipartimento per la regolamentazione finanziaria e professionale dell'Illinois (*Illinois Department of Financial and Professional Regulation –IDFPR*) Mario Treto ha chiarito l'impostazione sottesa all'intervento legislativo, affermando che «i cittadini dell'Illinois meritano un'assistenza sanitaria di qualità da parte di professionisti reali e qualificati, non da programmi informatici che raccolgono informazioni da ogni angolo di Internet per generare risposte che finiscono per danneggiare i pazienti». La legge ha inoltre ottenuto

un'approvazione unanime sia alla Camera che al Senato, evidenziando come la preoccupazione per i rischi legati all'IA in ambito terapeutico attraversi le tradizionali divisioni politiche americane.

Dal punto di vista strutturale, il testo normativo si caratterizza per un impianto snello ed essenziale. Esso si articola in nove sezioni (*Section* 1, 5, 10, 15, 20, 25, 30, 35 e 99), numerate in modo non consecutivo, secondo una tecnica redazionale fondata su “intervalli” di sezioni. Tale scelta risponde a esigenze di organizzazione sistematica e di futuribilità normativa, ed è coerente con le regole di *drafting* previste dall'[*Illinois Legislative Reference Bureau Manual*](#), il manuale ufficiale di tecnica legislativa utilizzato per la predisposizione dei testi normativi nello Stato dell'Illinois.

Dopo il titolo, l'enunciazione dello scopo e le definizioni, il nucleo normativo della legge è contenuto nella **Section 15**, rubricata “**Permitted use of artificial intelligence**”. Il **paragrafo (a)** consente al professionista l'impiego di strumenti di IA esclusivamente per attività di supporto amministrativo o supplementare, a condizione che egli mantenga la totale responsabilità per ogni iterazione, *output* e uso dei dati associati al sistema. L'uso consentito deve in ogni caso riguardare compiti estranei alla **comunicazione terapeutica**, intendendosi con questa espressione “qualsiasi interazione verbale, non verbale o scritta, svolta in un contesto clinico o professionale, intesa a diagnosticare, trattare o affrontare problemi mentali, emotivi o comportamentali di un individuo. Rientrano in tale nozione, a titolo esemplificativo ma non esaustivo: le interazioni dirette con i clienti volte a comprendere o riflettere pensieri, emozioni o vissuti personali; la fornitura di strategie o interventi terapeutici orientati al conseguimento di risultati di salute mentale; l'offerta di supporto emotivo, rassicurazione o empatia in risposta a situazioni di disagio psicologico o emotivo; la collaborazione con il cliente per la definizione o la modifica di obiettivi terapeutici o piani di trattamento; la restituzione di *feedback* comportamentali diretti a promuovere la crescita psicologica o ad affrontare specifiche condizioni di salute mentale. Le attività consentite si articolano, in primo luogo, nel **supporto amministrativo**, inteso come l'insieme di compiti che non implicano comunicazione terapeutica, quali, ad esempio: la gestione della programmazione degli appuntamenti e dei relativi promemoria; l'elaborazione delle procedure di fatturazione e delle richieste assicurative; la redazione di comunicazioni di carattere generale attinenti alla logistica del percorso terapeutico, purché prive di contenuti valutativi o di consiglio clinico. In via residuale, la legge ammette l'impiego dell'IA anche per attività di **supporto supplementare**, tra cui rientrano, a titolo esemplificativo: la preparazione e l'aggiornamento delle cartelle dei clienti, comprese le note terapeutiche; l'analisi di dati debitamente anonimizzati finalizzata al monitoraggio dei progressi del cliente o all'individuazione di tendenze, sempre subordinata alla revisione di un professionista autorizzato; nonché l'identificazione e l'organizzazione di risorse esterne o di rinvii destinati all'eventuale utilizzo da parte del cliente.

Con specifico riferimento all'impiego dell'IA per attività di supporto supplementare, la **Section 15, paragrafo (b)** introduce un'ulteriore limitazione: essa non può essere impiegata qualora la sessione di terapia del



cliente sia registrata o trascritta, salvo che il paziente sia preventivamente informato dell'uso dell'IA e delle finalità specifiche di questo, e abbia successivamente espresso un consenso esplicito. La necessità del consenso deriva dal fatto che, in tali ipotesi, il supporto supplementare opererebbe su informazioni sensibili provenienti direttamente dal paziente, incluse le sue parole testuali, espressive di vissuti personali, esperienze traumatiche e condizioni di vulnerabilità psicologica. Inoltre, una sessione registrata o trascritta presenta una potenzialità di diffusione e riutilizzo intrinsecamente superiore, potendo essere archiviata, incrociata con altri dati, riutilizzata nel tempo e, soprattutto, trasferita o trattata in ambienti tecnologici esterni, quali server remoti, processi di addestramento dei modelli o sistemi di terze parti. Il legislatore dell'Illinois assume l'esistenza di un rischio strutturalmente più elevato, anche quando l'IA sia adoperata solo per funzioni di supporto. L'innalzamento del livello di tutela deve essere letto alla luce della **Section 25**, che sancisce il divieto di divulgazione dei registri e delle comunicazioni tra paziente e professionista se non nel rispetto del [*Mental Health and Developmental Disabilities Confidentiality Act*](#) (MHDDCA). La regola generale per la divulgazione delle informazioni è rappresentata dal consenso scritto e firmato dell'interessato, sempre revocabile, il quale deve indicare in modo specifico: il destinatario delle informazioni, la finalità della divulgazione, l'oggetto dei dati comunicati e il termine finale di efficacia del consenso. (cfr. *Section 5* del MHDDCA). La medesima logica è riproposta anche con riferimento all'uso dell'IA in presenza di sessioni registrate o trascritte, come confermato altresì dai requisiti previsti dalla **Section 10** sub voce *Consent*. Tale impiego può essere qualificato come una forma di «divulgazione digitale» dei dati del paziente al sistema di IA, e pertanto richiede un'adeguata informativa scritta e un consenso informato espresso in modo consapevole.

In parallelo, la legge dedica una specifica disciplina ai divieti relativi all'erogazione di servizi terapeutici non autorizzati, contenuta nella **Section 20**, rubricata **“Prohibition on unauthorized therapy services”** e articolata in due paragrafi. Il **paragrafo (a)** amplia i destinatari del divieto e le condotte vietate, includendovi la pubblicizzazione di servizi terapeutici non autorizzati (come le attività di *marketing*, i *claim* promozionali e i contenuti diffusi tramite siti *web* o *app store*); ciò, al fine di prevenire pratiche elusive e forme di legittimazione commerciale indiretta di servizi non autorizzati, attraverso un approccio di *law enforcement* preventivo. Il divieto si estende, inoltre, all'offerta del servizio, intesa come qualsiasi proposta di vendita o di fruizione rivolta non solo al professionista sanitario, ma anche direttamente al cliente finale, in assenza dell'intermediazione di un soggetto abilitato. In tal modo, la norma colpisce non soltanto l'erogazione materiale della prestazione, ma anche la fase antecedente del contatto con l'utente. La disposizione assume particolare rilievo poiché coinvolge anche gli «strumenti indipendenti», ossia quei sistemi offerti direttamente al cliente e operanti al di fuori di una relazione terapeuta-paziente e che, proprio per tale ragione, si sottraggono ai presidi di responsabilità professionale.

Il **paragrafo (b)** rafforza ulteriormente l'impostazione restrittiva della legge, ribadendo che l'IA, a prescindere dalla modalità di impiego – sia essa mediata

dal professionista o incorporata in un *chatbot* indipendente – non può in alcun caso: assumere decisioni terapeutiche autonome; interagire direttamente con i clienti in forme riconducibili alla comunicazione terapeutica; generare raccomandazioni cliniche o piani di trattamento senza la preventiva revisione e approvazione di un professionista autorizzato; né, infine, rilevare o inferire emozioni, stati mentali o condizioni psicologiche dell'utente.

La **Section 30** disciplina i meccanismi di applicazione e sanzione della normativa, assicurandone l'effettività. Essa si articola in due disposizioni complementari, rispettivamente dedicate al regime sanzionatorio e ai poteri di indagine dell'autorità competente. Il **paragrafo(a)** introduce una sanzione civile applicabile a qualsiasi individuo, società o entità che violi la normativa. La sanzione, fissata in un importo massimo di 10.000 dollari per violazione, viene determinata dall'IDFPR sulla base del grado di danno arrecato e delle circostanze del caso, all'esito di un'udienza amministrativa. L'importo deve essere corrisposto entro sessanta giorni dalla decisione e, in caso di inadempimento, la sanzione assume efficacia esecutiva, risultando assimilabile ad una sentenza resa da un tribunale ordinario. L'entità economica della sanzione è concepita come un deterrente efficace sia per le aziende tecnologiche che per i singoli operatori, tentati di aggirare le restrizioni. Il **paragrafo(b)** attribuisce al Dipartimento un ampio potere di indagine, esteso non solo alle violazioni accertate, ma anche a quelle presunte o sospette, conferendo all'autorità una rilevante funzione non solo repressiva, bensì anche preventiva e proattiva.

Completa il quadro la **Section 35**, che individua specifiche eccezioni all'ambito di applicazione della normativa. In particolare, restano escluse la consulenza religiosa, le forme di supporto tra pari, i materiali di auto-aiuto e risorse educative: la *ratio* di tali esclusioni risiede nell'esigenza di preservare pratiche di supporto fondate sulla buona fede, sui doveri religiosi e sulla solidarietà sociale, evitando un'estensione della normativa anche a contesti non clinici, purché tali attività non siano esplicitamente presentate come servizi di terapia o psicoterapia.

L'impostazione adottata dallo Stato dell'Illinois risulta solo parzialmente sovrapponibile a quella italo-europea. Il Reg. (UE) 2024/1689, cd. *AI Act* (sul quale, v. in questa Rubrica la notizia n. 2 del [numero 2/2024](#) [2024/2(2)SO]) infatti, a differenza del *Wellness and Oversight for Psychological Resources Act*, non introduce un divieto espresso all'impiego dell'IA nei processi di cura della salute mentale. Tale utilizzo è ricondotto nell'alveo degli usi ad alto rischio, in quanto i sistemi di IA impiegati a fini di diagnosi o trattamento in ambito di salute mentale rientrano nella categoria dei dispositivi medici disciplinati dal Regolamento (UE) 2017/745 (MDR), e, come tali, sono qualificati «ad alto rischio» ai sensi dell'art. 6, par. 1, lett. a) e b), dell'*AI Act*. Questa qualificazione discende, da un lato, dall'inclusione del MDR tra gli atti di armonizzazione elencati nell'Allegato I dell'*AI Act* e, dall'altro, dal fatto che i dispositivi medici sono soggetti a una procedura di valutazione della conformità da parte di organismi notificati quale condizione per l'immissione sul mercato. L'ordinamento europeo, dunque, non esclude in via generale l'impiego dell'IA in ambito di salute mentale, ma lo sottopone a

un regime di controllo particolarmente rigoroso, che si traduce nel rispetto degli obblighi previsti dagli artt. 8-27 dell'*AI Act*.

Ciò nondimeno, dal sistema normativo europeo può ricavarsi una implicita preclusione della delega alla macchina della decisione psicoterapeutica. Tale limite emerge, in primo luogo, dall'art. 13 dell'*AI Act*, che impone l'obbligo di una sorveglianza umana effettiva sui sistemi di IA ad alto rischio, e, in secondo luogo, dalla normativa italiana sull'intelligenza artificiale (L. n. 132 del 2025; (sulla quale, v. in questa Rubrica la notizia n. 1 del [numero 3/2025](#) [2025/3(1)AA]), la quale, oltre a riconoscere all'interessato il diritto di essere informato sull'uso delle tecnologie di IA in ambito sanitario, attribuisce espressamente la titolarità della decisione clinica in capo al medico (cfr. art. 7, commi 3 e 5).

Ne consegue che una delega autonoma alla macchina di decisioni cliniche in materia di salute mentale risulta incompatibile tanto con la dimensione antropocentrica dell'intelligenza artificiale, che permea l'attuale quadro regolatorio europeo, quanto, ancora a monte, con la tutela della persona umana, quale principio fondamentale dell'ordinamento italo-europeo. L'uso dell'IA è pertanto ammesso esclusivamente come strumento di supporto – anche a livello clinico (diagnostico e terapeutico) – per il professionista sanitario, restando preclusa ogni forma di sostituzione dell'agente umano con un *chatbot* artificiale.

In tale contesto di rafforzamento del primato della decisione umana nei processi di cura, l'intervento legislativo dell'Illinois assume una collocazione temporale e sistematica particolarmente significativa. Da un lato, infatti, a livello federale era stato prospettato un approccio di segno opposto. Nella versione originaria del disegno di legge noto come [One Big Beautiful Bill Act](#) (P.L. 119-21) presentato nella primavera del 2025, l'amministrazione di Washington aveva avanzato l'ipotesi di una moratoria decennale su qualsiasi intervento normativo statale in materia di intelligenza artificiale. Tale proposta si fondava sul timore che la proliferazione di discipline locali eterogenee potesse determinare un quadro regolatorio frammentato, con ricadute negative sulla certezza del diritto e sulla capacità innovativa del sistema tecnologico statunitense. Il 1° luglio 2025, tuttavia, il Senato degli Stati Uniti ha respinto in modo pressoché unanime tale impostazione, con 99 voti contrari e uno solo favorevole, riaffermando la legittimità dell'iniziativa regolatoria statale. In questo senso, la scelta dell'Illinois si inserisce coerentemente nello spazio riaperto dall'esito del voto federale, ponendosi come un modello di regolazione preventiva oltre che sanzionatoria, orientato alla tutela dei soggetti più vulnerabili nei contesti di impiego dell'IA.

In linea con l'esperienza dell'Illinois, anche altri Stati federati hanno introdotto interventi normativi mirati. In particolare, il Nevada ha emanato l'[Assembly Bill 406](#) (AB406) che vieta ai fornitori di rendere disponibile agli utenti qualsiasi sistema di IA specificamente programmato per offrire servizi o esperienze che integrerebbero la pratica professionale dell'assistenza sanitaria mentale o comportamentale, qualora tali servizi fossero erogati da una persona fisica. Il divieto si estende altresì ai professionisti sanitari, ai quali è precluso l'uso dell'IA come parte integrante della pratica clinica, salvo che per funzioni di supporto meramente amministrativo, quali la

pianificazione delle attività o l'analisi dei dati. Le violazioni sono sanzionate con sanzioni pecuniarie fino a 15.000 dollari.

Diversa, ma complementare, è l'impostazione adottata nello Utah, dove il 7 maggio 2025 è entrata in vigore l'[Artificial Intelligence Amendments](#) (H.B. 452), che introduce restrizioni specifiche ai *chatbot* per la salute mentale. Anziché vietare in modo generalizzato l'impiego dell'intelligenza artificiale in questo ambito, il legislatore statale ha privilegiato un approccio fondato sulla trasparenza, imponendo ai fornitori di *chatbot* terapeutici obblighi informativi stringenti. In particolare, gli utenti devono essere informati in modo chiaro circa le modalità di raccolta dei dati, i limiti intrinseci dei sistemi di IA e il fatto che l'interazione avvenga con un sistema automatizzato e non con un essere umano. La normativa si applica esclusivamente ai *chatbot* generativi specificamente progettati o ragionevolmente destinati a fornire servizi di salute mentale, restando invece esclusi gli strumenti di uso generale, quali i modelli di linguaggio ad ampia finalità (ad es. *chatbot* generalisti), che non siano presentati o configurati come servizi terapeutici.

La regolamentazione dell'uso dell'intelligenza artificiale nei servizi di salute mentale appare oggi non solo opportuna, ma necessaria. Le esperienze normative di Stati come Utah, Nevada e, soprattutto, Illinois dimostrano una crescente consapevolezza istituzionale dei rischi connessi all'impiego di *chatbot* e sistemi automatizzati in ambiti che incidono direttamente sulla salute mentale, sull'autodeterminazione e sulla dignità della persona. Tali interventi legislativi muovono dalla constatazione che sistemi di IA sono stati in grado di fornire consigli inappropriati o potenzialmente dannosi a soggetti in condizioni di fragilità emotiva, confermando che la cosiddetta «terapia automatica» non possa essere ridotta a un mero «gesto tecnologico», ma costituisca un atto con rilevanti implicazioni sanitarie, etiche e giuridiche.

La risposta normativa non può, pertanto, esaurirsi nella sola logica del divieto o della restrizione. I dati empirici più recenti mostrano infatti come il ricorso crescente ai *chatbot* da parte soprattutto dei giovani non sia riconducibile unicamente a curiosità tecnologica o interesse per l'innovazione, bensì alla percezione di un vuoto di ascolto e di supporto nel sistema umano e istituzionale. In tale contesto, l'intelligenza artificiale finisce per rappresentare, talvolta, non una scelta, ma l'unica alternativa disponibile per soggetti che non riescono a trovare risposte adeguate nel sistema sanitario, educativo o sociale. In questo senso, è particolarmente significativo il [recente studio pubblicato su JAMA Network Open](#) del 7 novembre 2025, che evidenzia l'ampiezza del fenomeno e le motivazioni che spingono adolescenti e giovani adulti a ricorrere a sistemi di IA per ottenere consigli in materia di salute mentale. Alla luce di tali evidenze, il rischio è che una disciplina esclusivamente repressiva produca effetti elusivi o spinga ulteriormente questi fenomeni in aree non regolamentate, senza incidere sulle cause strutturali del problema. Proprio per questo, accanto al necessario contenimento degli usi impropri dell'IA, appare fondamentale sviluppare strategie positive di prevenzione, supporto e ascolto. In tale prospettiva, le eccezioni previste dalla normativa dell'Illinois – in particolare quelle relative al supporto tra pari, alla consulenza religiosa e alle risorse educative e di auto-aiuto – meritano una valutazione favorevole, in quanto riconoscono e

valorizzano forme di ascolto e accompagnamento non cliniche, ma socialmente rilevanti, purché non si presentino come sostitutive della terapia o della psicoterapia.

In definitiva, la regolazione dell'intelligenza artificiale in ambito di salute mentale non può limitarsi a stabilire ciò che è vietato, ma deve interrogarsi sulle condizioni che rendono tali tecnologie attrattive e, in alcuni casi, percepite come indispensabili dai soggetti vulnerabili. Solo un approccio integrato, che affianchi alla disciplina giuridica un rafforzamento delle reti di supporto umano, dei servizi pubblici e delle forme di solidarietà sociale, può evitare che l'IA diventi un surrogato improprio della relazione terapeutica e garantire una tutela effettiva della persona, in linea con i principi fondamentali degli ordinamenti democratici contemporanei.

FRANCESCA FERRETTI

<https://ilga.gov/Legislation/BillStatus?DocNum=1806&GAID=18&DocTypeID=HB&LegId=159219&SessionID=114>

2025/4(48)DI

Il New York Algorithmic Pricing Disclosure Act entrato in vigore il 10.11.2025

Il 10 novembre 2025 è entrato in vigore il *New York Algorithmic Pricing Disclosure Act* (NYAPD Act). La disciplina è inserita nella legislazione statale relativa alla *Consumer Protection From Deceptive Acts and Practices*. Essa intende il “dynamic pricing” come il “pricing that fluctuates dependent on conditions” e definisce il “Personalized algorithmic pricing” nei termini di un “dynamic pricing set by an algorithm that uses personal data”. Il NYAPD Act si applica a tutti coloro operino nello Stato di New York (“any natural person, firm, organization, partnership, association, corporation, or any other entity domiciled or doing business in New York state”) e gli impone un obbligo di inserire, in modo chiaro e in stampatello, l'espressione per cui **“This price was set by an algorithm using your personal data”** allorché questi fissino “the price of a specific good or service using personalized algorithmic pricing, and that directly or indirectly, advertises, promotes, labels or publishes a statement, display, image, offer or announcement of personalized algorithmic pricing to a consumer in New York, using personal data specific to such consumer”. In caso di mancato assolvimento dell'obbligo di informazione, “the court may impose a civil penalty of not more than one thousand dollars for each violation”.

Il NYAPD Act prevede delle eccezioni. Sul piano soggettivo, l'obbligo di disclosure circa l'utilizzo di un prezzo determinato da un algoritmo che ha trattato i dati del consumatore non si applica agli istituti finanziari e assicurativi autorizzati e rispetto a contratti con consumatori in abbonamento (“subscription-based”). Sul piano oggettivo, si è fuori dall'ambito applicativo del dovere di informare il consumatore allorché, nell'ambito dell'offerta di un trasporto a noleggio, il dato personale riguardi la posizione del

consumatore (“*location data*”) e il trattamento automatizzato sia esclusivamente rivolto al calcolo del “*fare based on mileage and trip duration between the passenger's pickup and drop-off locations*”.

L’entrata in vigore del NYAPD Act, approvato già nel maggio del 2025, è stata ritardata per via di un procedimento intentato dinnanzi al *U.S. District Court Southern District of New York* dalla *National Retail Federation*, che contestava una violazione del *First Amendment*. Con un provvedimento dell’8.10.2025 la doglianza è stata rigettata e l’obbligo confermato, ritenendo che l’informazione che il NYAPD Act impone venga trasmessa al consumatore sia “*purely factual and uncontroversial*” e rientri, dunque, tra le ipotesi in cui il legislatore statale può obbligare un inserzionista a divulgare determinate informazioni.

DANIELE IMBRUGLIA

NYAPD

National Retail Federation vs James

2025/4(49)LS

La legge dello Stato della California sull’intelligenza artificiale “*The Transparency in Frontier Artificial Intelligence Act*” (SB53) del 29.9.2025

Il [Senate Bill No. 53](#), approvato dal Governatore della California il 29 settembre 2025 e depositato presso il Segretario di Stato il medesimo giorno, nota come “*Transparency in Frontier Artificial Intelligence Act (TFAIA)*” (la **Legge**), introduce significative regolamentazioni sull’intelligenza artificiale (IA), con un focus sulla trasparenza, sicurezza e innovazione etica. Nello specifico, la legge in esame aggiunge il Capitolo 25.1 alla Divisione 8 del *Business and Professions Code*; la Sezione 11546.8 al *Government Code* nonché il Capitolo 5.1 alla Parte 3 della Divisione 2 del *Labor Code*. La Legge mira a bilanciare i benefici e i potenziali rischi derivanti dall’uso dell’IA promuovendo soprattutto la trasparenza e l’*accountability*. Essa riconosce, da un lato, la *leadership* della California nell’incentivare l’innovazione sull’IA ma, dall’altro lato, sottolinea la necessità di interventi mirati per evitare che questa tecnologia venga utilizzata maliziosamente come, ad esempio, per condurre attacchi cibernetici, produrre armi biologiche o per realizzare condotte ingannevoli.

Ciò premesso, la Legge pone, innanzitutto, una serie di dichiarazioni rivolte a contestualizzare tale intervento normativo. La California viene infatti descritta come leader mondiale nello sviluppo e utilizzo dell’IA, grazie ad aziende e università, sia pubbliche che private. L’IA, inclusi i modelli di base (c.d. *foundation models*), può sì giocare un ruolo fondamentale nell’avanzamento, ad esempio, della medicina e della scienza climatica ma, senza le necessarie precauzioni, potrebbe essere utilizzata scorrettamente. Per evitare questo rischio, la Legge si concentra sugli sviluppatori più sofisticati e più grandi, c.d. “di frontiera” (*frontier developers* e *large frontier developers*), vale a dire coloro che operano con sistemi IA avanzati (c.d.



frontier models) e che generano guadagni importanti, escludendo invece quelli minori. L'obiettivo è, quindi, quello di creare un quadro normativo che bilanci i benefici e i rischi catastrofici derivanti dall'IA, attraverso l'introduzione di una serie di misure volte a garantire la trasparenza, la sicurezza e l'innovazione etica nell'ambito dei modelli IA avanzati. A tal fine, viene imposto un sistema di report obbligatori, standardizzato e oggettivo a carico di questi grandi sviluppatori, così da poter fornire al governo e al pubblico informazioni tempestive e accurate. Inoltre, si enfatizza l'importanza di sistemi di reportistica degli incidenti per verificarne e controllarne gli impatti *post-deployment*, nonché di protezioni per i segnalatori (c.d. *whistleblower*).

Per far ciò, la normativa in esame chiarisce innanzitutto il significato di alcuni concetti fondamentali tra cui, soprattutto, l'**oggetto** di regolamentazione e l'identità dei **soggetti** a cui essa si rivolge.

Per quanto riguarda il primo, si specifica, infatti, che l'attenzione di tale normativa è circoscritta ai **“modelli di frontiera”** ossia modelli di base (*foundation models*) addestrati con una potenza computazionale superiore a 10^{26} operazioni, inclusi *fine-tuning* e modifiche, su dati ampi per output generali e adattabili a vari compiti; dall'altro lato, vengono individuati gli **“sviluppatori di frontiera”** (*frontier developers*) vale a dire coloro che addestrano siffatti modelli di frontiera e i **“grandi sviluppatori di frontiera”** (*large frontier developers*) ossia quegli sviluppatori che, insieme ai propri affiliati, abbiano registrato, nell'anno precedente, un fatturato lordo annuo superiore a 500 milioni di dollari.

Non solo, la Legge specifica anche il concetto centrale di **“rischio catastrofico”** (*catastrophic risk*) come quel rischio prevedibile e concreto che lo sviluppo, l'uso, l'archiviazione e l'implementazione di un modello di frontiera contribuisca in modo significativo alla morte o al ferimento grave di più di 50 soggetti o a danni o perdite di proprietà per valori superiori a un miliardo di dollari derivanti da un singolo incidente, a causa di: assistenza esperta nella creazione o rilascio di armi chimiche, biologiche, radiologiche o nucleari; di condotte senza supervisione umana equivalenti a crimini come omicidio, estorsione o furto; o di evasione dal controllo dello sviluppatore. Tale definizione non include, però, i rischi derivanti da: (i) informazioni fornite da un modello di frontiera se esse sono già accessibili al pubblico; (ii) attività governative lecite; nonché (iii) danni causati da un modello di frontiera in combinazione con altro software, se esso non ha contribuito in modo rilevante al danno. Ancora, con “incidente critico per la sicurezza” (*critical safety incident*) la legge si riferisce ai casi di: (i) accesso non autorizzato, modifica o sottrazione dei pesi di un modello di base che cagioni la morte o il ferimento di persone così come danni o perdite di proprietà; (ii) danno derivanti dalla materializzazione di rischi catastrofici; (iii) perdita di controllo di un modello di base che causa morte o lesioni personali; (iv) un modello di base che utilizza tecniche ingannevoli per sovvertire i controlli o il monitoraggio dello stesso, al di fuori di un contesto di valutazione del modello volto a suscitare appositamente tale comportamento e, comunque, in un modo che dimostri un aumento significativo del rischio catastrofico. Infine, per “quadro di riferimento per l'IA di frontiera” (*frontier AI*

framework) si intende un set di protocolli tecnici e organizzativi documentati per gestire, valutare e mitigare i rischi catastrofici dell'uso di tali sistemi di IA. Per assicurare che queste definizioni rimangano allineate con gli sviluppi tecnologici, si prevede che esse siano soggette a revisioni annuali da parte del Dipartimento di Tecnologia a far data dal 2027 considerando diversi elementi tra cui, ad esempio, gli standard internazionali e gli input degli *stakeholders*. Tuttavia, la parte centrale della Legge consiste nell'imposizione di un **pacchetto di obblighi** rigorosi in capo ai grandi sviluppatori di frontiera per promuovere una governance trasparente dell'IA avanzata. Nello specifico, essi devono:

- redigere, implementare e pubblicare online un quadro di riferimento per l'IA che descriva in dettaglio come incorporare standard nazionali, internazionali e *best practices* industriali;
- definire e valutare soglie per identificare capacità che potrebbero porre rischi catastrofici, possibilmente con livelli multipli;
- applicare mitigazioni basate su tali valutazioni; rivedere queste valutazioni prima di sviluppare un modello o usarlo internamente in modo esteso;
- coinvolgere terze parti per valutazioni indipendenti;
- aggiornare il framework almeno annualmente o per modifiche materiali, con giustificazione pubblica entro 30 giorni;
- implementare pratiche di cybersicurezza per proteggere i pesi del modello da modifiche o trasferimenti non autorizzati;
- identificare e rispondere a incidenti critici;
- stabilire governance interna per l'implementazione; nonché gestire rischi da uso interno, inclusi possibili meccanismi per evitare fraudolentemente i meccanismi di supervisione umana. Prima o contestualmente allo sviluppo di un nuovo modello o di una versione con modifiche sostanziali deve essere pubblicato un report di trasparenza contenente diversi elementi tra cui, ad esempio, il sito web dello sviluppatore, meccanismi di contatto, data di rilascio, lingue e modalità supportate così come usi previsti e restrizioni. Per i grandi sviluppatori, questo report include altresì riassunti dettagliati circa le valutazioni effettuate e i risultati ottenuti circa i rischi catastrofici individuati, nonché l'eventuale coinvolgimento di terze parti nel processo. Coerentemente, la Legge vieta la possibilità di fare dichiarazioni materialmente false o fuorvianti su rischi o compliance, salvo se in buona fede.

Inoltre, i grandi sviluppatori devono trasmettere sommari di valutazioni ad uso interno dell'Ufficio dei Servizi di Emergenza ("*Office of Emergency Services (OES)*"), ogni tre mesi o sulla base di scadenze concordate in modo confidenziale.

Per quanto riguarda invece gli incidenti critici per la sicurezza, si prevede che l'Ufficio dei Servizi di Emergenza stabilisca precisi meccanismi per la redazione di report da parte degli sviluppatori, che devono tra l'altro includere alcuni elementi come la data, le ragioni e la descrizione dell'incidente. Gli sviluppatori devono riportare entro 15 giorni (che diventano 24 ore se il rischio è imminente) alle autorità appropriate. Una volta ricevuti, l'Ufficio revisiona questi report, li trasmette in forma anonimizzata e aggregata alle Autorità (Governatore, governo federale e agenzie statali). Dal 2027, è

previsto che l'Ufficio produca altresì report annuali aggregati, escludendo tutte le informazioni sensibili. In caso di violazione di tali prescrizioni (mancata redazione o pubblicazione dei report, false dichiarazioni, mancato rispetto del quadro di riferimento), la legge prevede diverse sanzioni che arrivano fino a un milione di dollari per infrazione, recuperabili dal Procuratore Generale tramite azione civile.

Un altro pilastro della normativa in commento consiste nell'istituzione di un **consorzio temporaneo all'interno dell'Agenzia per le Operazioni Governative** ("Government Operations Agency") per sviluppare una cornice di riferimento, chiamata "CalCompute", consistente in un **cluster cloud pubblico per un'IA sicura, etica, equa e sostenibile**.

Questo consorzio, composto da 14 membri tra rappresentanti universitari, organizzazioni lavoristiche, stakeholders etici ed esperti tech nominati da varie autorità, ha l'obiettivo di favorire la ricerca e l'innovazione pubblica. Quest'ultimo dovrà sottoporre, entro il 1° gennaio 2027, un report alla legislatura contenente un'analisi del panorama infrastrutturale californiano, i costi e i finanziamenti necessari, nonché raccomandazioni sulla governance, sui parametri d'uso (inclusi i processi per selezionare utenti e progetti), così come un'analisi del personale tecnologico e una descrizione di possibili collaborazioni con entità non governative.

Specifiche norme sono poi dedicate alla **tutela dei whistleblower** coinvolti nei processi di valutazione e risposta agli incidenti. Ad esempio, la Legge vieta a qualsiasi sviluppatore di frontiera di impedire, in qualsiasi modo, a un dipendente interessato di divulgare informazioni (al Procuratore Generale, alle autorità federali, a superiori o colleghi) laddove egli abbia un ragionevole motivo di credere che queste siano capaci di dimostrare che l'attività di tale sviluppatore costituisca un pericolo specifico e sostanziale per la salute o la sicurezza pubblica oppure che egli abbia violato la Legge. In più, i grandi sviluppatori hanno altresì l'obbligo di offrire dei processi interni anonimi per favorire la divulgazione, con aggiornamenti mensili su indagini e azioni, condivisi periodicamente con soggetti competenti.

LUDOVICA SPOSINI

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53

2025/4(50)GDM

Le Linee guida dell'UNESCO del 2025 sull'uso dei sistemi di IA nei tribunali

Similmente a quanto accade in tutto il mondo con le pubbliche amministrazioni, dove sistemi di intelligenza artificiale vengono sempre più adottati con gli obiettivi di migliorare l'erogazione dei servizi pubblici, di automatizzare certe fasi dei procedimenti amministrativi, di rafforzare il coinvolgimento dei cittadini, di monitorare le infrastrutture pubbliche e di ottimizzare l'allocazione delle risorse, anche per quanto riguarda

l'amministrazione della giustizia, corti e tribunali di tutto il mondo mostrano una tendenza crescente ad adottare strumenti di intelligenza artificiale (IA) a supporto dell'attività giudiziaria.

Il fenomeno è stato fatto oggetto di uno specifico documento dell'Organizzazione delle Nazioni Unite per l'Educazione, la Scienza e la Cultura, la Comunicazione e l'Informazione (UNESCO o l'**Organizzazione**), pubblicato il 3 dicembre 2025 dal titolo "[Linee Guida per l'uso dei sistemi di IA nelle Corti e nei Tribunali](#)" (le **Linee guida** o il **Documento**).

Le Linee guida hanno innanzitutto rilevato che i campi di attività interessati sono molteplici, ed includono:

- la ricerca, l'analisi e la discovery documentale su larga scala;
- la risoluzione delle controversie online;
- la previsione circa l'esito dei contenziosi;
- i processi decisionali e di emissione dei provvedimenti;
- l'anonimizzazione e la pseudo-anonimizzazione delle decisioni;
- la classificazione degli atti depositati;
- la trascrizione e la traduzione di atti.

Ne costituiscono esempi il sistema VICTOR, usato dalla Corte Suprema brasiliana, il quale elabora migliaia di ricorsi presentati alla Corte per agevolare l'individuazione dei casi che soddisfano il requisito della "general repercussion", o ancora il software SUVAS adottato dalla Corte Suprema dell'India per tradurre migliaia di documenti dall'inglese in dieci lingue locali e viceversa. Per non parlare, allargando la panoramica al mondo delle professioni legali, degli strumenti di elaborazione del linguaggio naturale (natural language processing, NLP) per prevedere le decisioni giudiziarie (come accade nell'Unione europea con riguardo alla Corte di giustizia) o di quei sistemi di IA per la revisione e la gestione dei contratti e per la ricerca giuridica sui fascicoli, utilizzati in Paesi come il Sudafrica o lo Zimbabwe. Così come si diffondono sempre di più i chatbot basati su Large Language Models (LLM) per redigere documenti legali, provvedimenti o per sviluppare argomentazioni nelle udienze, soprattutto in materie quali il diritto costituzionale, amministrativo, della privacy, penale e di famiglia.

Le trasformazioni che l'IA sta importando all'interno del settore della giustizia sono evidenti e molte di queste rappresentano dei miglioramenti perché incidono positivamente sull'efficienza, sull'efficacia e sulla facilità di accesso al sistema giustizia, così come contribuiscono allo snellimento nella gestione dei procedimenti e costituiscono un utile supporto dei giudici per il processo decisionale.

Malgrado la diffusione sempre maggiore di tali tecnologie, solo un numero relativamente limitato di paesi ha pubblicato principi, regole o linee guida sull'impiego etico e responsabile di tali strumenti. Tra questi, le Linee guida annoverano: Argentina (2024), Australia (2024), Brasile (2020, 2025), Canada (2023, 2024), Colombia (2024), Nuova Zelanda (2023), Singapore (2024), Regno Unito di Gran Bretagna e Irlanda del Nord (2023) e Stati Uniti (2024). A tali interventi di carattere nazionale si affiancano alcune decisioni adottate isolatamente da singoli tribunali indicanti principi e regole per l'uso degli strumenti di IA da parte della magistratura.

Questo aspetto non può essere trascurato posto che, ai benefici che l'IA reca con sé, si contrappongono altrettanti rischi, che non possono essere sottovalutati. I sistemi di IA, infatti, quando siano integrati all'interno dei processi decisionali, potrebbero produrre effetti negativi sull'intero sistema giudiziario dando origine a una serie di esternalità negative e di violazioni dei diritti umani: ad esempio, l'adozione di tali sistemi potrebbe contribuire a discriminare sistematicamente individui, o gruppi interi di soggetti vulnerabili. Del pari, l'adozione di sistemi intelligenti che si rivelino difettosi o l'uso negligente dei sistemi di IA, da parte della magistratura, potrebbero pregiudicare il giusto processo e le garanzie procedurali, l'accesso alla giustizia e il diritto a un rimedio effettivo, nonché diritti come la privacy e la protezione dei dati, l'uguaglianza davanti alla legge e la non discriminazione, oltre a valori della funzione giudiziaria come imparzialità, indipendenza e responsabilizzazione (accountability).

Non è un caso, d'altronde, che già il regolamento (UE) 2024/1689 (**AI Act** o **AIA**) abbia classificato come “ad alto rischio” i sistemi di IA «destinati a essere utilizzati da un'autorità giudiziaria o per suo conto per assisterla nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione del diritto a un insieme concreto di fatti, oppure a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie» (Considerando 61 AIA, e cfr. anche art. 6 e Allegato III, punto 8 lett. a) AIA). Una classificazione che fa scattare per i soggetti che impiegano questi sistemi gli obblighi di cui agli artt. 8 ss. AIA, tra cui l'implementazione di un sistema di gestione del rischio e la garanzia di un'adeguata supervisione umana sui sistemi.

Per questa ragione, le Linee guida possono costituire un testo al quale il settore giudiziario potrà fare riferimento per rafforzare le proprie capacità nel contesto della trasformazione digitale.

Le Linee Guida rappresentano «il primo quadro etico e operativo a livello globale volto ad assicurare che l'IA sia al servizio della giustizia, nel rispetto dello Stato di diritto e dei diritti fondamentali» e «promuovono l'uso dell'IA come strumento di supporto, non sostitutivo – da utilizzare in modo responsabile e sempre sotto una significativa supervisione umana». L'obiettivo vuol essere quello di bilanciare l'innovazione con la tutela dei diritti fondamentali, nell'ottica di mettere il progresso tecnologico al servizio dei valori democratici e dello sviluppo sostenibile, e non viceversa.

E dal momento che l'utilizzo dell'IA esorbita dal sistema giudiziario in senso stretto e abbraccia in generale tutte le professioni legali, il Documento precisa che la maggior parte dei principi e delle raccomandazioni proposte ben potrebbe essere adattata alle attività svolte da pubblici ministeri, arbitri, avvocati, ordini forensi, funzionari pubblici e ricercatori; in questa prospettiva, peraltro, anche organizzazioni della società civile, quali associazioni professionali e università, hanno recentemente pubblicato indicazioni e raccomandazioni analoghe.

Le Linee Guida ampliano il quadro di documenti che l'UNESCO ha già pubblicato in tema di etica dell'AI (ossia la “Raccomandazione sull'etica dell'intelligenza artificiale” (2021); la “Valutazione d'impatto etico: uno strumento della Raccomandazione sull'etica dell'intelligenza artificiale”

(2021); e il “Global Toolkit su IA e Stato di diritto per la magistratura” (2023)) e, in effetti, proprio il concetto di etica viene posto in particolare risalto dall’UNESCO, posto che il termine ricorre oltre venti volte nell’arco di tutto il testo.

Il Documento è frutto di un ampio lavoro svolto nell’ultimo decennio dall’Organizzazione di concerto con operatori della giustizia di tutto il mondo e costituisce l’esito di un processo composto di numerose consultazioni pubbliche, di una revisione da parte di esperti internazionali di IA applicata al diritto, oltre che di studio svolto su fonti secondarie e letteratura specialistica. Un percorso che, peraltro, ha visto l’UNESCO impegnata dal 2013 in programmi di formazione volti a rafforzare le competenze degli operatori della giustizia (trentaseimila in centosessanta Paesi) su temi quali libertà di espressione, l’accesso all’informazione e l’applicazione e l’impatto dell’IA nei sistemi di giustizia.

Proprio il costante lavoro di revisione e consultazione su cui si fondano le Linee guida impone di guardare a queste come «un documento “vivente” che, pertanto, richiede aggiornamenti periodici per tenere il passo con il rapido avanzamento della tecnologia IA e con la crescita delle sue applicazioni all’interno dei sistemi di giustizia».

Dunque, nell’ottica di promuovere il rispetto universale della giustizia e dello stato di diritto, salvaguardando al contempo la tutela e la promozione dei diritti umani e delle libertà fondamentali, il Documento si divide in una prima sezione dedicata ai “principi”, una seconda in cui vengono indicate alcune “raccomandazioni” e una terza contenente “indicazioni specifiche per i singoli membri della magistratura”.

Per “principi” si intendono tutte quelle «prescrizioni generali volte a orientare organizzazioni e individui nello sviluppo, nell’acquisizione e nell’uso di sistemi di IA in modo etico e rispettoso dei diritti umani». Il Documento ne individua quindici.

Il primo principio riguarda la tutela dei diritti umani, che impone di adottare tutte le misure necessarie per rispettare, proteggere e promuovere i diritti umani e lo Stato di diritto «lungo l’intero ciclo di vita dei sistemi di IA» e che a sua volta si declina nei sottoprincipi di non discriminazione, di uguaglianza, di equità procedurale, di diritto alla privacy e alla protezione dei dati personali e di libertà e sicurezza.

Per l’UNESCO è fondamentale prevedere garanzie affidabili per i sistemi di IA che potrebbero rappresentare un rischio elevato per i diritti umani, soprattutto con riguardo a quei soggetti che potrebbero essere discriminati in ragione di particolari condizioni personali (donne, persone con disabilità, bambini, rifugiati, migranti, apolidi, minoranze). In tal senso, è indispensabile prevenire sviluppi e applicazioni distorti dei sistemi di IA che possano «aggravare, riprodurre, rafforzare o perpetuare discriminazioni» di qualsiasi tipo; così come occorre scongiurare la possibilità che tali sistemi creino barriere aggiuntive nell’accesso alla giustizia per chi non dispone di risorse o competenze digitali, richiamando sul punto il principio Leave No One Behind (LNOB), già evocato nell’ambito dell’Agenda ONU per lo Sviluppo Sostenibile per contrastare l’esclusione digitale; nonché evitare che tali

strumenti vengano utilizzati in modi che generino rischi di divulgazione di dati o consentano accessi non autorizzati da parte di terzi.

Seguono a questo gli ulteriori principi di proporzionalità, di realizzabilità dei benefici, di sicurezza, di sicurezza delle informazioni, di accuratezza e affidabilità, di spiegabilità (ossia rendere intelligibili, a chi implementa e a chi utilizza, gli input, il procedimento di ragionamento, i risultati e il funzionamento dei sistemi di IA), di verificabilità (o auditabilità), di giustizia trasparente e aperta, di consapevolezza e uso informato, di responsabilità, di accountability e contestabilità, di supervisione umana e processo decisionale, di progettazione incentrata sull'essere umano e partecipativa e, infine, di governance e collaborazione multi-stakeholder.

Le Linee guida proseguono con le “raccomandazioni”, definite dalle Linee guida come «percorsi d'azione suggeriti che discendono dai “principi” e che aiutano sia le organizzazioni ad acquisire e sviluppare sistemi di IA sicuri, protetti e affidabili, sia i singoli a utilizzare i sistemi di IA in modo etico, responsabile e rispettoso dei diritti umani».

Le raccomandazioni vengono al loro interno tripartite tra quelle relative a “sviluppo, acquisizione, uso e valutazione dei sistemi di IA”; quelle che si concentrano sul “capitale umano” per fornire indicazioni sulle azioni che la magistratura dovrebbe intraprendere per supportare le persone che implementeranno e utilizzeranno sistemi di AI; e infine quelle che attengono all’“uso dei sistemi di AI”, relative alle azioni che le autorità giudiziarie dovrebbero intraprendere in relazione all'adozione, all'implementazione e all'uso dei sistemi di IA generativa.

Tra le prime, si annoverano quelle miranti a: proteggere l'indipendenza e l'imparzialità della magistratura; invitare quest'ultima a riflettere sulle diversità culturali della popolazione interessata dall'implementazione dei sistemi di IA e a tenere conto delle barriere all'accesso alla giustizia per le persone prive delle conoscenze necessarie a interagire con il sistema giudiziario (specialmente i più anziani); istituire una governance multi-stakeholder degli strumenti di IA; adottare fin dall'inizio misure di trasparenza algoritmica e spiegabilità, verificando l'opportunità di optare per sistemi open source invece che proprietari; rispettare i criteri di necessità, proporzionalità, adeguatezza e allineamento sull'uso di tali sistemi; adottare misure che contemplino “by design” l'equità (anche procedurale), in modo da prevenire sin dallo sviluppo dei sistemi bias nei dati e nella progettazione di algoritmi; l'implementazione per fasi degli strumenti di IA; sensibilizzare la magistratura sulla sostenibilità e sull'impatto ambientale dei sistemi di IA; stabilire regole e linee guida interne per lo sviluppo, l'implementazione e l'uso degli strumenti di IA sulla base del quadro dei diritti umani, enfatizzando il fatto che i membri della magistratura si assumono la responsabilità di qualsiasi materiale prodotto con l'uso dell'IA; prevedere ove necessario l'intervento umano; implementare quadri di accountability prima dell'adozione operativa dei sistemi di IA realizzando una “valutazione d'impatto algoritmico” per individuare gli effetti probabili (positivi e negativi), una “valutazione del rischio algoritmico” per mappare i rischi potenziali (es. malfunzionamenti del sistema) oppure una “valutazione d'impatto sui diritti fondamentali”; condurre audit algoritmici e valutazioni

d’impatto dopo l’implementazione dei sistemi di IA; cessare l’uso di sistemi di IA che incidono negativamente sui diritti umani, come quelli che perpetuano esiti discriminatori (sul punto, il Documento richiama il Rapporto del Segretario generale delle Nazioni Unite “Human rights in the administration of justice”, secondo il quale la magistratura dovrebbe astenersi dall’utilizzare o cessare l’uso di strumenti di IA “impossibili da gestire in conformità al diritto internazionale dei diritti umani”, tra cui rientrano applicazioni predittive “nelle decisioni giudiziarie in materia penale e nelle valutazioni del rischio di recidiva per decisioni su cauzione e libertà condizionale, salvo e fino a quando le autorità responsabili non dimostrino che tali applicazioni sono conformi al diritto a un equo processo, inclusa un’autorità giudiziaria indipendente, e ai diritti alla libertà e sicurezza, alla non discriminazione, alla libertà dalla tortura e dai maltrattamenti e alla privacy, nonché agli altri diritti umani interessati, e che le autorità abbiano affrontato l’impatto negativo sproporzionato che l’uso di queste tecnologie può avere su gruppi specifici”); assicurare l’accessibilità degli strumenti di IA; predisporre misure di sicurezza e rafforzamento della cybersicurezza; rafforzare la protezione dei dati personali e della privacy; divulgare proattivamente informazioni chiave sui sistemi di IA utilizzati dalla magistratura; garantire la contestabilità delle decisioni supportate o fondate su sistemi di IA.

Tra le seconde sono incluse quelle di rivedere i curricula delle scuole di formazione giudiziaria, assicurare l’accesso alla formazione, condurre ricerche sull’uso e sugli effetti degli strumenti di IA per mostrare buone pratiche e potenziali criticità da evitare e, infine, valutare la necessità di aggiornare politiche e pratiche di gestione delle risorse umane.

Tra le terze si annoverano raccomandazioni in merito alla consapevolezza delle funzioni e dei limiti di tali sistemi, alla garanzia circa l’autenticità e l’integrità dei contenuti e alle limitazioni d’uso.

Le Linee guida si chiudono con un’apposita sezione contenente una serie di “Indicazioni specifiche per i singoli membri della magistratura”, ossia un insieme di raccomandazioni rivolto alle persone che fanno parte della magistratura (intesa nel Documento in senso ampio, come comprensiva anche di funzionari giudiziari e personale di supporto giudiziario) che intendono implementare e utilizzare sistemi di IA. Le indicazioni sono suddivise in tre categorie.

Una prima concerne le azioni che dovrebbero essere intraprese prima di utilizzare e implementare sistemi di AI, e dunque che si abbia una piena consapevolezza e alfabetizzazione sull’IA (AI literacy), che vi sia un costante sviluppo di competenze e, da ultimo, che l’utilizzo degli strumenti di IA testati tramite valutazioni algoritmiche avvenga seguendo le indicazioni dei report di due diligence sui diritti umani che dovrebbero essere predisposti dalle autorità giudiziarie tenendo in considerazione l’intero ciclo di vita dei sistemi di IA.

Una seconda attiene alle azioni che dovrebbero essere intraprese durante l’uso e l’implementazione dei sistemi di IA, tra cui evitare un eccessivo affidamento sui sistemi di IA per assumere decisioni sostanziali, rispettare i termini d’uso, trasparenza proattiva, responsabilità e accountability,

possibilità di riesame delle decisioni e contestabilità e segnalazioni proattive per prevenire danni.

Una terza indica le azioni che dovrebbero essere intraprese in relazione all'adozione, all'implementazione e all'uso dei sistemi di IA generativa, tra cui proteggere i dati personali e le informazioni riservate e, con riguardo agli usi principali degli LLM, verificare l'output del sistema di IA e confrontarli con fonti affidabili. Seguono inoltre, il monito sulla scarsa affidabilità di tali sistemi quando utilizzati come motori di ricerca o per l'analisi giuridica; il dovere di non sostituire le perizie dei consulenti tecnici o testimonianze con dei LLM; la consapevolezza dei limiti e dei rischi degli LLM; verificare gli output prima dell'uso; utilizzare tali sistemi secondo criteri di trasparenza, integrità e responsabilità.

GENNARO DI MARTINO

<https://www.unesco.org/en/articles/guidelines-use-ai-systems-courts-and-tribunals>