



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/ogid> - jodi.deap@uniroma1.it).

SOMMARIO

2025/3(1)AA Pubblicata in GU la legge 23 settembre 2025, n. 132 recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale” – **Andrea Amidei**

2025/3(2)SO Il piano di azione sull'intelligenza artificiale degli Stati Uniti d'America annunciato il 23 luglio 2025 e il “*Bias Order*” emesso in pari data dal Presidente Trump: “*Preventing Woke AI in the Federal Government*” – **Salvatore Orlando**

2025/3(3)RP Il piano di azione sull'intelligenza artificiale della Repubblica Popolare Cinese annunciato il 26 luglio 2025 e le nuove iniziative di cooperazione internazionale del governo cinese del 23 settembre 2025 (*World Cooperation Organization on Artificial Intelligence* e *AI+ International Cooperation Initiative*) per promuovere un'innovazione tecnologica «sicura, inclusiva e a vantaggio dell'umanità» – **Rosalba Potenzano**

2025/3(4)SR Le Linee guida del 2025 del Ministero dell'Istruzione e del Merito “per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche”: la Scuola da comunità educante a *deployer* – **Samuele Francesco Rosa**

* 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.

[2025/3\(5\)ESt](#) Le Linee guida EDPB 3/2025 aperte alla consultazione pubblica sul coordinamento tra DSA e GDPR (versione 1.1 del 12 settembre 2025) – **Elisabetta Stringhi**

[2025/3\(6\)TB](#) Le Linee guida EDPB 2/2025 aperte alla consultazione pubblica sul trattamento di dati personali attraverso tecnologie blockchain (versione 1.1 dell'8 aprile 2025) – **Timoteo Bucci**

[2025/3\(7\)GD](#) - Le sanzioni irrogate il 23.4.2025 dalla Commissione europea a Meta (€ 200 milioni) e ad Apple (€ 500 milioni) per violazioni del DMA in relazione alla formula “consent or pay” di Meta per i dati raccolti su Facebook e Instagram, e alla pratica di Apple di imporre vincoli agli operatori commerciali nel presentare informazioni ed offerte alternative all’App Store di Apple – **Giorgia Diotallevi**

[2025/3\(8\)FZ](#) La sanzione di €2.95 miliardi irrogata dalla Commissione europea a Google il 5 settembre 2025 per condotte anticoncorrenziali tese a favorire i propri servizi di tecnologia per pubblicità online (Google ADTECH) – **Francesca Zampone**

[2025/3\(9\)ST](#) Gli accertamenti preliminari della Commissione europea del 28 luglio 2025 nei confronti di Temu per violazione del DSA relativamente alla valutazione del rischio sistemico di prodotti illegali offerti al pubblico nella sua piattaforma e l’indagine sui *dark patterns* – **Sara Tommasi**

[2025/3\(10\)AG](#) La prima relazione annuale dell’AGCOM quale Coordinatore dei servizi digitali ai sensi del DSA – **Antonio Gorgoni**

[2025/3\(11\)CAT](#) Il protocollo d’intesa del 29.7.2025 tra il Garante privacy italiano e l’AGCM – **Carmine Andrea Trovato**

[2025/3\(12\)VH](#) Il provvedimento dell’AGCM del luglio 2025 di avvio di istruttoria nei confronti di Meta per abuso di posizione dominante in relazione alla pratica di *tying* consistente nell’installazione automatica del servizio di intelligenza artificiale Meta AI nella app di messagistica WhatsApp – **Victor Hartl**

[2025/3\(13\)OL](#) Il provvedimento di inibizione provvisoria del Garante privacy italiano dell’11.9.2025 relativo al sistema di riconoscimento facciale *FaceBoarding* utilizzato presso l’aeroporto di Milano Linate – **Olindo Lanzara**

[2025/3\(14\)EF](#) La sentenza della Cassazione 24204/2025 del 29.8.2025 sulla inutilizzabilità a fini disciplinari delle email personali del lavoratore dipendente – **Emanuela Fiata**

[2025/3\(15\)BG](#) Le sentenze del 16.9.2025 del Tribunale di Torino e del 23.9.2025 del Tribunale di Latina di condanna per responsabilità aggravata



ex art. 96 c.p.c. per uso improprio del supporto di sistemi di intelligenza artificiale nella redazione di difese giudiziali – **Beatrice Gallucci**

2025/3(16)FG La storica transazione da 1,5 miliardi di dollari della class-action americana tra Anthropic e gli autori approvata in via preliminare in sede giudiziale il 25.9.2025 – **Francesco Grossi**

2025/3(17)SR La proposta legislativa danese del giugno 2025 per la tutela autoriale delle “repliche” digitali delle persone – **Samuele Francesco Rosa**

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.



2025/3(1)AA**Publicata in GU la legge 23 settembre 2025, n. 132 recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale”**

| 1016

All’esito di un cammino parlamentare complesso – articolatosi in tre letture, con l’esame di 437 emendamenti – il 17 settembre 2025 il Senato italiano ha approvato in via definitiva la legge n. 132/2025 recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale”, pubblicata in Gazzetta Ufficiale il 25 settembre 2025. La legge, che contiene sia **deleghe al Governo che disposizioni di immediata attuazione**, è entrata in vigore il **10 ottobre 2025**.

L’iter di approvazione della legge ha comportato anche una interlocuzione con la **Commissione UE**, la quale, come si apprende dalla lettura del resoconto di una seduta plenaria della IV Commissione permanente del Senato tenutasi il 27 novembre 2024, ha formulato diverse osservazioni critiche nei confronti della versione originaria del disegno di legge, racchiuse nel parere C(2024) 7814 del 5 novembre 2024, e attinenti principalmente alla compatibilità di alcune disposizioni del d.d.l. rispetto alle prescrizioni dell’AI Act (Regolamento 2024/1689).

La legge – che si compone di sei capi e complessivi ventotto articoli – è connotata da un contenuto eterogeneo, che spazia da disposizioni volte a disciplinare l’impiego della IA in ambito sanitario, nelle professioni, nella Pubblica Amministrazione e nel settore della giustizia sino a norme in tema di diritto d’autore, da previsioni in ambito penale alla designazione delle autorità nazionali competenti in materia di IA. Nell’impossibilità di soffermarsi qui sull’intero testo normativo, e nella difficoltà di tratteggiarne un quadro unitario a fronte di un ambito applicativo tanto diversificato, nel prosieguo se ne segnaleranno i contenuti che si ritengono maggiormente degni di nota.

Le previsioni di cui al Capo I (artt. 1-6) enunciano le **finalità** della legge e i **principi** cui essa professa di ispirarsi. Così, all’art. 1 si dichiara l’ambizioso intento di introdurre “principi in materia di ricerca, sperimentazione, sviluppo, adozione e applicazione di sistemi e di modelli di intelligenza artificiale”; di promuovere “un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell’intelligenza artificiale, volto a coglierne le opportunità”; di garantire “la vigilanza sui rischi economici e sociali e sull’impatto sui diritti fondamentali dell’intelligenza artificiale”. Il tutto, con norme da interpretarsi e applicarsi “conformemente” all’**AI Act** (il regolamento (UE) 2024/1689), al quale rinvia anche l’art. 2 quanto alle definizioni.

Nel panorama dei principi e delle statuizioni generali di cui al Capo I – declinati in particolare negli ambiti della informazione e della riservatezza dei dati personali (art. 4), dello sviluppo economico (art. 5) e della sicurezza e difesa nazionale (art. 6) – si ritiene di segnalare:

- la previsione della necessità del consenso dell’esercente la responsabilità genitoriale per l’accesso alle tecnologie di IA da parte dei **minori di quattordici anni**, nonché per il conseguente trattamento dei relativi dati personali (art. 4, comma 4);



- il *favor*, nelle procedure di *e-procurement* delle amministrazioni pubbliche per la scelta di fornitori di sistemi e modelli di IA, nei confronti di “soluzioni che garantiscono la **localizzazione** e l’elaborazione dei dati strategici presso *data center* posti nel **territorio nazionale**” (art. 5, comma 1, lett. d);
- l’esclusione dall’ambito applicativo della legge di una serie di impieghi dell’IA per attività di tutela della sicurezza nazionale e di difesa (art. 6, comma 1).

Seguono, al Capo II, una serie di disposizioni di settore, di cui quattro (artt. 7-10) dedicate all’**impiego dell’IA in ambito sanitario**, che riconoscono, in primo luogo, il contributo che l’IA può apportare, oltre che al miglioramento del sistema nel suo complesso, alle finalità di prevenzione, diagnosi e cura delle malattie. Vengono al riguardo precisati alcuni principi generali, tra cui quello di non discriminazione nell’accesso alle prestazioni sanitarie (art. 7, comma 2) e il primato della decisione umana (art. 7, comma 5). Quanto agli obblighi informativi, la legge riconosce il diritto dell’interessato “a essere informato sull’impiego di tecnologie di intelligenza artificiale” nella prestazione medica (art. 7, comma 3), ma – anche sulla scorta del richiamato parere della Commissione UE – non si spinge a ricomprendere nell’oggetto dell’informazione elementi ulteriori, quali le “informazioni sulla logica decisionale utilizzata” dal sistema di IA, come prevedeva la versione originaria del d.d.l.

Tra le disposizioni più controverse e destinate a suscitare ampio dibattito – soprattutto in relazione alle interazioni con il regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari (**EHDS**) – merita menzione l’art. 8 (“Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario”). In sintesi estrema, la norma classifica i trattamenti di dati, anche personali, eseguiti da soggetti pubblici e privati senza scopo di lucro per finalità di **ricerca e sperimentazione nella realizzazione di sistemi di IA in ambito sanitario**, in quanto necessari per la realizzazione di banche di dati e modelli di base, come “**di rilevante interesse pubblico in attuazione degli articoli 32 e 33 della Costituzione**”. Si supera così la necessità di consenso diretto dell’interessato a tali tipologie di trattamenti, pur restando fermi l’obbligo di informativa – da assolversi anche mediante una informativa generale pubblicata online – e di curare che i dati in questione siano privati degli elementi identificativi diretti.

Si segnalano altresì le norme in materia di **professioni intellettuali** (art. 13), **Pubblica Amministrazione** (art. 14) e **attività giudiziaria** (art. 15), accomunate dalla tendenza ad ammettere il ricorso all’IA in tali ambiti unicamente in funzione strumentale e di supporto. Tale approccio risulta particolarmente evidente con riferimento all’uso dell’IA nell’attività giurisdizionale, ove l’impiego di tali tecnologie è espressamente previsto per funzioni quali “l’organizzazione dei servizi relativi alla giustizia”, “la semplificazione del lavoro giudiziario” e “le attività amministrative accessorie”, mentre si riserva al magistrato “ogni decisione sull’interpretazione e sull’applicazione della legge, sulla valutazione dei fatti e delle prove e sull’adozione dei provvedimenti”. Per vero, la norma non sembra escludere la possibilità di ricorso a sistemi di IA anche nel contesto

di tali attività, ma potrebbe essere letta nel senso di riservare al giudice umano la decisione finale, ma non anche di impedirgli di avvalersi di strumenti di IA a supporto. Sia l'art. 13 che l'art. 15 hanno subito significative modifiche nell'iter di approvazione della legge, anche su impulso della Commissione europea, che aveva censurato l'iniziale approccio del legislatore italiano, ritenuto eccessivamente restrittivo in rapporto a quanto previsto dall'AI Act. Venendo ora al Capo III (artt. 19-24), specifica attenzione merita l'art. 20, che designa l'**Agenzia per l'Italia digitale (AgID)** e l'**Agenzia per la cybersicurezza nazionale (ACN)** quali "Autorità nazionali per l'IA". In particolare:

- all'AgID è assegnato il compito di "promuovere l'innovazione e lo sviluppo" dell'IA, nonché di esercitare funzioni in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di IA, e di svolgere il ruolo di autorità di notifica ai sensi dell'art. 70 dell'AI Act;
- all'ACN è attribuita l'attività di vigilanza dei sistemi di IA, nonché di promozione e sviluppo dell'IA relativamente ai profili di cybersicurezza. L'Agenzia è inoltre designata quale autorità di vigilanza del mercato e punto di contatto unico con le istituzioni dell'UE *ex art.* 70 dell'AI Act.

La norma testimonia, dunque, la scelta del legislatore italiano di non affidare tali ruoli a una o più autorità indipendenti (Garante privacy, AGCM, ecc.), bensì ad agenzie, dotate di ben minori spazi di indipendenza politica.

L'art. 24 enumera, poi, le diverse **deleghe** affidate al Governo, chiamato in primo luogo ad adottare, entro un anno dall'entrata in vigore della nuova legge, uno o più decreti legislativi per l'**adeguamento della normativa nazionale all'AI Act**, ivi inclusa l'attribuzione ad AgID e ACN dei poteri di vigilanza, ispettivi e sanzionatori previsti dal Regolamento. Nell'esercizio di tale delega il Governo dovrà attenersi a una serie di criteri direttivi, tra cui particolare attenzione è riservata al tema della alfabetizzazione e formazione in materia di IA.

Lo stesso art. 24 (commi 3, 4 e 5) delega, inoltre, il Governo ad adottare, entro il medesimo termine, uno o più decreti legislativi per "adeguare e specificare la disciplina dei **casi di realizzazione e impiego illeciti di sistemi di IA**", anche con la introduzione di autonome fattispecie di reato per omessa adozione di misure di sicurezza nella produzione e nell'impiego di IA ove ne derivi pericolo per la vita, l'incolumità pubblica o la sicurezza dello Stato. Si segnala inoltre, la delega a prevedere, nei casi di responsabilità civile, una specifica regolazione del riparto dell'onere della prova tenuto conto della classificazione basata sul rischio di cui all'AI Act; prospettiva, questa, che sembrerebbe voler riproporre in chiave nazionale i meccanismi di cui alla nota proposta di direttiva UE in materia di responsabilità extracontrattuale per danni causati da sistemi di IA [COM(2022) 496 del 28 settembre 2022], recentemente ritirata dalla Commissione.

La legge interviene anche sul tema dell'impatto dell'IA sul **diritto d'autore** (Capo IV, art. 25), e in particolare su due versanti, ossia quello della tutela dell'opera generata con l'ausilio dell'IA e quello del regime giuridico

dell'elaborazione di opere e altri materiali a fini di addestramento dell'IA. In sintesi:

- sulla prima questione, si modifica l'art. 1 della legge n. 633/1941 per specificare che sono protette dal diritto d'autore le opere dell'ingegno "umano" anche "laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del **lavoro intellettuale dell'autore**". La norma lascia, dunque, all'interprete la definizione di quale livello e tipologia di apporto umano siano necessari, e sufficienti, perché l'opera meriti tutela autoriale, dalla quale restano invece escluse le opere generate dall'IA senza (significativo?) contributo dell'uomo;
- sul secondo punto, si introduce nella stessa legge n. 633/1941 un nuovo art. 70-septies, che prevede che "le riproduzioni e le estrazioni da opere o da altri materiali contenuti in rete o in banche di dati a cui si ha legittimamente accesso, ai fini dell'estrazione di testo e di dati attraverso modelli e sistemi di intelligenza artificiale, anche generativa, sono consentite in conformità alle disposizioni di cui agli articoli 70-ter e 70-quater", ossia alle norme (di derivazione eurounitaria) in materia di **text and data mining**. Il che potrebbe, quantomeno *prima facie*, deporre nel senso di una assimilazione delle operazioni di elaborazione e riproduzione di opere ai fini dell'addestramento dell'IA a quelle di *text and data mining*, in gran parte liberalizzate ad opera della Direttiva 2019/790 (ferma restando la possibilità di preventivo *opt-out*); questione per vero non scontata, sulla quale peraltro pende un rinvio pregiudiziale dinanzi alla Corte di Giustizia UE (causa C-250/25, *Like Company v. Google Ireland*).

Al riguardo, inoltre, l'art. 26 (Capo V) della legge sancisce la possibile rilevanza penale della condotta di chi, nell'effettuazione di tali operazioni, travalichi i limiti di cui agli artt. 70-ter e 70-quater della legge n. 633/1941.

Il medesimo art. 26 introduce, poi, ulteriori modifiche al **codice penale** e ad altre disposizioni penali, tra cui l'introduzione:

- di una nuova circostanza aggravante comune, costituita dall'aver commesso il fatto mediante l'impiego di sistemi di IA come "mezzo insidioso" o con un uso che abbia ostacolato la pubblica o la privata difesa o aggravato le conseguenze del reato;
- di una aggravante speciale legata all'impiego di sistemi di IA nella commissione del delitto di attentato contro i diritti politici del cittadino (art. 294 c.p.);
- di un nuovo reato legato alla diffusione illecita di contenuti generati o alterati con l'IA, se "idonei a indurre in inganno sulla loro genuinità", punito con la reclusione da uno a 5 anni "se dal fatto deriva un danno ingiusto" (art. 612-quater c.p.).

Ci è qui precluso soffermarci su altre norme della legge n. 132/2025 che pur meriterebbero menzione, tra cui quelle sull'impiego dell'IA in materia di lavoro (artt. 11 e 12), l'ampia delega al Governo per la definizione del regime giuridico dell'utilizzo di dati e algoritmi per l'addestramento dei sistemi di IA (art. 16), la previsione della competenza del tribunale per le cause che hanno a oggetto il funzionamento di un sistema di IA (art. 17), le previsioni

sulla strategia nazionale per l'IA (art. 19), le misure sugli investimenti nei settori dell'IA, della cybersicurezza e del calcolo quantistico (art. 23). Ci si limita allora, in conclusione, a segnalare la clausola di invarianza finanziaria di cui all'art. 27, che potrebbe frapporre più di un problema al raggiungimento di obiettivi ambiziosi previsti dalla legge, tra cui, ad esempio, la realizzazione di una piattaforma di IA per il supporto alle finalità di cura (art. 10, comma 2) e l'adozione di sistemi di IA a supporto dell'attività della P.A. (art. 14) o dei tribunali (art. 15).

ANDREA AMIDEI

<https://www.gazzettaufficiale.it/eli/id/2025/09/25/25G00143/sg>.

2025/3(2)SO

Il piano di azione sull'intelligenza artificiale degli Stati Uniti d'America annunciato il 23 luglio 2025 e il “Bias Order” emesso in pari data dal Presidente Trump: “Preventing Woke AI in the Federal Government”

Il 23 luglio 2025 l'amministrazione Trump ha pubblicato un documento di 28 pagine intitolato “[Vincere la gara: il Piano di azione dell'intelligenza artificiale dell'America](#)” (*Winning the Race: America's AI Action Plan*) (il **Piano di azione americano** o il **Piano**).

Il Piano contiene più di 90 raccomandazioni alle agenzie federali, che coprono 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. Se implementato, il Piano verosimilmente comporterà specifici obblighi per gli sviluppatori di IA in particolare per i fornitori del governo federale.

Nella parte del Piano chiamata “Introduzione” (firmata da Michael J. Kratsios, *Assistant to the President for Science and Technology*, David O. Sacks, *Special Advisor for AI and Crypto* e Marco A. Rubio, *Assistant to the President for National Security Affairs*) è scritto che gli Stati Uniti d'America sono in gara per conquistare il dominio globale nell'intelligenza artificiale.

Si sottolineano i benefici “economici e militari” in palio in questa competizione e la necessità per l'America di vincerla insieme ai suoi “alleati”. Si richiama dunque l'Executive Order 14179 del Presidente Trump, “*Removing Barriers to American Leadership in Artificial Intelligence*” (sul quale v. in questa Rubrica la notizia n.1 del [numero 2/2025](#) [2025/2(1)SO]) e le relative finalità, indicate nei termini della promozione della c.d. “*human flourishing*”, della competizione economica e della sicurezza nazionale, con una serie di ulteriori affermazioni sulla “età dell'oro” e la “vittoria” che il Piano intende assicurare al popolo americano.

Il Piano si struttura in **tre “pilastri”**.

Il primo “pilastro” intitolato *Accelerating AI Innovation* contiene 15 punti che riguardano essenzialmente la **riduzione delle barriere regolatorie alla**

innovazione sia a livello federale che statale e la fissazione di principi da rispettare per l'**approvvigionamento di sistemi di tecnologie IA da parte del governo federale**, tra i quali quello della **rimozione di “bias ideologici”**. In proposito, si trova scritto che i sistemi di IA usati dal governo federale devono essere **liberi da “misinformation”**. A tal fine, *inter alia*, il Piano richiede al Dipartimento del Commercio di modificare il *National Institute of Standards and Technology (NIST) AI Risk Management Framework* al fine di **“eliminare riferimenti al cambiamento climatico e ad iniziative DEI”** (Diversità Equità Inclusione).

Il Piano istruisce le agenzie federali affinché esse si approvvigionino soltanto di *large language models* (LLMs) che siano **“objective and free from top-down ideological bias”**.

Il Bias Order del 23 luglio 2025: “Preventing Woke AI in the Federal Government”

Se il Piano non fornisce ulteriori informazioni in proposito, indicazioni piuttosto dettagliate sono offerte dal coevo ordine esecutivo del 23 luglio 2025 del Presidente Trump intitolato *“Preventing Woke AI in the Federal Government”* (il [Bias Order](#)). Il Bias Order richiede alle agenzie federali di attenersi a due c.d. *Unbiased AI Principles*: **“Ricerca della Verità”** (*“Truth-Seeking”*) e **“Neutralità Ideologica”** (*“Ideological Neutrality”*). Quest’ultima, si legge nel Bias Order, dovrebbe essere assicurata da applicazioni di IA che non devono **“manipolare le risposte favorendo dogmi ideologici come DEI”**. In particolare, il Bias Order richiede agli sviluppatori di non **“intentionally encode partisan or ideological judgments into an LLM’s outputs unless those judgments are prompted by or otherwise readily accessible to the end user.”** Il Bias Order richiede inoltre al Direttore dell’*Office of Management and Budget (OMB)* di emanare delle linee guida sui predetti *Unbiased AI Principles* rispettando certi criteri, tra i quali quello per cui deve essere possibile richiedere ai fornitori informazioni ma deve anche essere permesso loro di non rivelare **“sensitive technical data”**. Infine, il Bias Order richiede alle agenzie federali di includere nei contratti di fornitura di LLM clausole che obbligano i fornitori a garantire la conformità agli *Unbiased AI Principles* e di pagare i costi associati alla risoluzione dei contratti nel caso in cui l’agenzia federale risolva il contratto per non conformità agli *Unbiased AI Principles*.

Il secondo “pilastro” intitolato **“Costruire l’Infrastruttura IA americana”** è incentrato sullo sviluppo dell’infrastruttura dell’intelligenza artificiale all’interno degli Stati Uniti, e contiene otto punti tra i quali una serie dettagliata di *policy recommendations* per snellire i procedimenti autorizzativi e facilitare lo sviluppo di *data centers* (inclusi quelli per uso militare), fabbriche di semiconduttori ed infrastrutture energetiche, nonché per sviluppare misure di cybersicurezza e per formare la forza lavoro all’impiego della IA.

Infine, **il terzo “pilastro”** intitolato **“In testa nella politica internazionale e nella sicurezza dell’IA”** contiene sette punti. Vi si trovano, tra le altre, raccomandazioni per “esportare la IA americana” a “partner e alleati” degli Stati Uniti, per implementare misure di controllo alle esportazioni di tecnologie verso paesi avversari degli Stati Uniti, per **contrastare l’influenza**

cinese, per valutare rischi di cybersecurity e per la sicurezza nazionale inclusi quelli derivanti da una possibile “*malign foreign influence*” e per investire in biosicurezza.

Probabilmente, l'impatto complessivo del Piano di azione americano risulterà evidente solo quando le agenzie federali cominceranno ad attuare gli oltre 90 punti delle relative *recommended policy actions*. Esso offre però sin d'ora, insieme al Bias Order, una chiara indicazione di come l'amministrazione Trump intende affrontare i temi di governance della IA nei prossimi anni.

SALVATORE ORLANDO

<https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>

<https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/>

2025/3(3)RP

Il piano di azione sull'intelligenza artificiale della Repubblica Popolare Cinese annunciato il 26 luglio 2025 e le nuove iniziative di cooperazione internazionale del governo cinese del 23 settembre 2025 (*World Cooperation Organization on Artificial Intelligence e AI+ International Cooperation Initiative*) per promuovere un'innovazione tecnologica «sicura, inclusiva e a vantaggio dell'umanità».

Il 26 luglio 2025, ad appena tre giorni dalla pubblicazione del [piano strategico statunitense sull'IA](#) (sul quale v. in questa Rubrica la notizia n. 2 *supra* in questo numero [2025/3(2)SO]), la Cina ha adottato il [Global AI Governance Action Plan](#) (il **Piano di azione cinese** o il **Piano**), presentato a Shanghai dal primo ministro del Consiglio di Stato Li Qiang, nel corso della cerimonia inaugurale della *World Artificial Intelligence Conference* (WAIC). Il Piano di azione cinese palesa un'ampia disponibilità al confronto con tutti i Paesi del mondo, con particolare attenzione a quelli del Sud globale, per favorire, nel rispetto delle sovranità nazionali, uno sviluppo dell'IA sicuro, equo, inclusivo e benefico per l'umanità e il pianeta. In particolare, il Piano promuove l'adozione di misure volte ad accelerare l'innovazione nel campo dell'intelligenza artificiale e a garantirne la massima sicurezza e controllabilità, nonché efficienza energetica e sostenibilità, individuando nella cooperazione internazionale e nella governance collaborativa il motore per sfruttare appieno il potenziale della tecnologia a vantaggio della collettività. Il Piano di azione cinese formula, in sintesi, un programma di progresso scientifico responsabile, fondato sul dialogo transnazionale con attori istituzionali, cittadini e imprese, nel rispetto degli obiettivi dell'Agenda 2030, del Patto per il Futuro e del *Global Digital Compact*, a cui il testo fa espressamente riferimento.

Il documento si articola in tredici punti che ruotano attorno a tre direttrici principali, le quali, come chiarito dal Premier Li Qiang nel suo [discorso](#) di

apertura della WAIC, riflettono gli obiettivi di innovazione, inclusione e cooperazione alla base del Piano. In primo luogo, infatti, si propone di potenziare l'intelligenza artificiale, elevandone gli attuali livelli qualitativi, allo scopo di conseguire dei risultati scientifici significativi e di ampia portata, a servizio della collettività. A tal fine, si invitano tutti i soggetti interessati – governi, organizzazioni internazionali, imprese, istituti di ricerca, associazioni e cittadini – ad avviare un percorso di collaborazione volto ad esplorare congiuntamente le opportunità offerte dall'IA (punto 1). Una volta compiuta un'analisi delle attuali tecnologie più avanzate, è necessario consentirne l'applicazione su scala mondiale e condurre delle nuove ricerche e sperimentazioni comuni (punto 2) che favoriscano lo sviluppo dell'intelligenza artificiale in diversi ambiti, tra cui la produzione industriale, i consumi, l'agricoltura (punto 3) e, soprattutto, il settore pubblico (sanità, istruzione e trasporti), il quale “dovrebbe fungere da guida e modello nell'applicazione e nella governance di una IA” sicura, affidabile e inclusiva, nel rispetto delle privacy e dei diritti di proprietà intellettuale (punto 9). In questo scenario, teso a promuovere un avanzamento ambizioso e pionieristico dell'intelligenza artificiale, occorre incoraggiare lo scambio di buone pratiche e la circolazione transfrontaliera sia di linee guida di sicurezza e di documentazioni tecniche (punto 5), sia di risorse di base e set di dati di alta qualità entro sistemi open-source che consentano un addestramento affidabile e responsabile dell'intelligenza artificiale, nel rispetto della privacy e al riparo da *bias* e discriminazioni (punto 6). È fondamentale, infatti, non sottovalutare i rischi di tale tecnologia e proporre delle misure di prevenzione e risposta mirate, nonché rafforzare la gestione della sicurezza dei dati nei processi di raccolta e generazione dei modelli (punto 10). Si pone, infine, l'attenzione anche sull'uso responsabile delle risorse, proponendo la definizione di standard unificati che permettano la realizzazione di infrastrutture digitali e tecnologie di calcolo efficienti, in grado di ridurre l'impatto energetico e ambientale complessivo dell'intelligenza artificiale (punti 4 e 7).

Oltre a promuovere uno sviluppo innovativo, sicuro e sostenibile dell'IA, il Piano di azione cinese individua, in secondo luogo, delle linee di intervento specificamente volte a garantire un accesso universale e inclusivo all'intelligenza artificiale, specialmente nei contesti che presentano ridotte capacità scientifiche, tecnologiche e di innovazione. In continuità con gli impegni già assunti dalla Cina nell'ambito dei programmi siglati in seno alle Nazioni Unite, il documento ribadisce, infatti, la necessità di sostenere i Paesi in via di sviluppo nella costruzione e nell'impiego di infrastrutture e sistemi di IA (punto 4), riconoscendo la responsabilità dei Paesi leader del settore di adottare misure concrete per colmare il divario digitale (punto 12). Infine, in terzo luogo, il Piano propone l'instaurazione di un sistema di governance dell'IA basato su un ampio consenso e su regole condivise. Il conseguimento di un risultato siffatto richiede, per un verso, che si valorizzi il ruolo delle organizzazioni internazionali di standardizzazione, come l'Unione internazionale delle telecomunicazioni (ITU), l'Organizzazione Internazionale per la normazione (ISO) e la Commissione elettrotecnica internazionale (IEC), nonché dell'industria, nella formulazione e nella revisione di standard tecnici nei settori strategici dell'IA (punto 8). Per altro



verso, occorre che si introducano delle nuove piattaforme globali e regionali, basate sull'interesse pubblico e sulla partecipazione congiunta, che permettano a tutti gli attori coinvolti nella governance dell'IA, inclusi governi, ricercatori, sviluppatori e imprese di tutto il mondo, di dialogare e cooperare per affrontare le principali sfide in materia di innovazione, applicazione, etica e sicurezza dell'IA in specifici settori (punto 13).

In adesione alle linee di intervento indicate nel nuovo programma di governance globale dell'IA, **la Cina ha avviato due nuove iniziative di cooperazione internazionale: la *World Cooperation Organization on Artificial Intelligence (WAICO)* e l'*AI+ International Cooperation Initiative***. Il 26 luglio 2025, contestualmente all'adozione del Piano d'azione, il Premier Li Qiang ha proposto l'istituzione della [WAICO](#), una nuova organizzazione mondiale per la cooperazione sull'intelligenza artificiale, con sede a Shanghai. Come si legge nel [comunicato stampa](#), tale iniziativa costituisce una conferma della serietà dell'impegno del governo cinese nel sostenere il multilateralismo e lo sviluppo dell'intelligenza artificiale orientato al bene comune e all'inclusione universale, offrendo, al contempo, una risposta concreta alle richieste di aiuto del Sud Globale. Questa organizzazione opererà, infatti, come una piattaforma volta al perseguimento di tre obiettivi principali: favorire il dialogo della Cina con gli altri Paesi e tra questi ultimi, affinché si possa sfruttare appieno l'infinito potenziale dell'intelligenza artificiale e dividerne i benefici; aiutare i Paesi in via di sviluppo a rafforzare le proprie capacità tecnologiche, in attuazione degli impegni assunti in seno alle Nazioni Unite; e potenziare il coordinamento tra i diversi Paesi per introdurre strategie, regole di governance e standard tecnici dell'IA condivisi. La nuova organizzazione, aperta a tutti i Paesi che vogliono aderirvi in condizioni di parità e nel rispetto delle sovranità nazionali, opererà in sinergia con l'ONU e le sue agenzie specializzate, che continueranno a costituire per la Cina il canale principale per la governance globale dell'IA. In linea con questa visione, il 23 settembre 2025, a New York, nel corso della riunione di Alto livello sulla *Global Development Initiative (GDI)* per sostenere l'attuazione dell'Agenda 2030, il Primo ministro cinese ha presentato alle Nazioni Unite l'[AI+ International Cooperation Initiative](#). Tale iniziativa di cooperazione internazionale sull'intelligenza artificiale si articola in cinque campagne, ognuna con un focus specifico: il benessere pubblico, il progresso tecnologico, l'applicazione industriale, la prosperità culturale e la formazione dei talenti. L'obiettivo è quello di coinvolgere tutti i Paesi a collaborare attivamente per realizzare una piena integrazione dell'intelligenza artificiale nello sviluppo economico e sociale a beneficio dei popoli di tutti i Paesi, incluso il Sud del mondo. A tal fine, ci si impegna a sfruttare il potenziale dell'IA per migliorare i servizi pubblici essenziali, soprattutto nel settore sanitario e dell'istruzione, nonché a potenziare la ricerca e l'innovazione tecnologica, promuovere nuove forme di business e la creazione di nuovi posti di lavoro, preservare e valorizzare le diverse tradizioni culturali e, altresì, sostenere l'alfabetizzazione digitale e la formazione di figure professionali nel settore dell'intelligenza artificiale.

ROSALBA POTENZANO



https://www.fmprc.gov.cn/eng/xw/zyxw/202507/t20250729_11679232.html
https://www.gov.cn/yaowen/liebiao/202507/content_7033957.htm

https://www.fmprc.gov.cn/eng/xw/zyjh/202509/t20250924_11715960.html

| 1025

2025/3(4)SR

Le Linee guida del 2025 del Ministero dell'Istruzione e del Merito “per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche”: la Scuola da comunità educante a *deployer*

L'introduzione dell'intelligenza artificiale (IA) nei sistemi educativi segna un passaggio cruciale nel processo di digitalizzazione della società. Le [Linee guida per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche](#), emanate dal Ministero dell'istruzione e del merito nel 2025 (le **Linee guida**), si inseriscono in un contesto normativo europeo e nazionale in rapido mutamento, che vede nel regolamento (UE) 2024/1689 (**AI Act**) (su cui v. in questa Rubrica la notizia n. 2 del [numero 2/2024](#) [2024/2(2)SO]), nella Convenzione del Consiglio d'Europa del 2024 (su cui v. in questa Rubrica la notizia n. 1 del [numero 2/2024](#) [2024/2(1)RR]), nella [Strategia nazionale per l'intelligenza artificiale 2024-2026](#) dell'Agenzia per l'Italia digitale (**AGID**) e del [Dipartimento per la trasformazione digitale](#) (struttura di supporto della Presidenza del Consiglio dei Ministri) e nella legge 132/2025 *Disposizioni e deleghe al Governo in materia di intelligenza artificiale* (sulla quale v. in questa Rubrica la notizia n. 1 *supra* in questo numero [2025/3(1)AA]) i principali riferimenti regolatori. L'obiettivo dichiarato delle Linee guida è quello di orientare le Istituzioni scolastiche verso un'adozione consapevole, etica e sicura delle tecnologie emergenti, garantendo allo stesso tempo la tutela dei diritti fondamentali. Si legge nel documento, inoltre, che “*il Ministero stabilisce i principi di riferimento e i requisiti etici, tecnici e normativi che guidano l'elaborazione delle istruzioni operative e degli strumenti di supporto per l'introduzione strutturata, organizzata e governata dell'IA nelle scuole, con un'attenzione particolare alla gestione dei rischi associati*”.

Dal punto di vista giuridico, la regolamentazione rappresenta lo strumento attraverso il quale realizzare “*l'obiettivo principale di garantire che la diffusione e lo sviluppo della tecnologia avvengano in conformità ai valori fondamentali dell'Unione Europea e siano ispirati a un approccio antropocentrico, incentrato sul rispetto della dignità umana e dei diritti e delle libertà fondamentali*”. Per questa ragione, il cuore delle Linee guida risiede nel bilanciamento tra l'autonomia scolastica, garantita dal D.P.R. 275/1999, e l'esigenza di uniformare criteri e standard di introduzione dei sistemi di IA nel rispetto delle normative sovranazionali.

Molto significativo è il passaggio delle Linee guida (par. 1.1, p.6) dove “[s]i precisa che, nell'ambito della gestione dei sistemi di IA, l'Istituzione scolastica opera in qualità di «*deployer*»” ai sensi dell'art. 3 (1) n. 4 dell'AI Act, assumendo, di conseguenza, una responsabilità diretta nell'utilizzo dei

sistemi, con obblighi di monitoraggio, valutazione d'impatto sui diritti fondamentali e sorveglianza umana. Tale qualificazione sposta l'attenzione dalla dimensione puramente tecnica a quella giuridico-istituzionale, imponendo alle Istituzioni scolastiche di divenire non soltanto fruitori, ma anche garanti della legittimità e dell'equità delle soluzioni adottate.

Nelle Linee guida vengono richiamate, in coerenza con l'art. 5(1) dell'AI Act, le “pratiche” che risultano espressamente considerate dai divieti previsti in quel paragrafo e che, quindi, non possono trovare spazio all'interno delle Istituzioni scolastiche. Esse riguardano l'uso di sistemi di IA che fanno impiego di tecniche subliminali o volutamente manipolative o ingannevoli, capaci di condizionare in maniera occulta o distorta il comportamento degli studenti o del personale; l'uso di sistemi di IA per la valutazione o classificazione delle persone fisiche sulla base del comportamento sociale o di caratteristiche personali, con attribuzione di un “punteggio sociale” e conseguente applicazione di trattamenti pregiudizievole o sfavorevoli; l'impiego di sistemi di IA di categorizzazione biometrica finalizzati a classificare individualmente le persone sulla base di dati biometrici, per trarre inferenze riguardanti aspetti sensibili come razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; con particolare riferimento al settore scolastico, l'utilizzo di sistemi di IA destinati a individuare le emozioni di studenti o personale all'interno degli istituti di istruzione, salvo che tali strumenti siano introdotti per comprovati motivi medici o di sicurezza

Un aspetto particolarmente delicato, in relazione alla Scuola come *deployer* e ai conseguenti obblighi, riguarda la classificazione dei sistemi di IA come “ad alto rischio” quando impiegati in attività connesse all'accesso, alla selezione, alla valutazione degli studenti o al monitoraggio durante le prove d'esame. La scelta normativa riflette la consapevolezza che le decisioni algoritmiche possono incidere in maniera determinante sul percorso educativo e professionale di un individuo, ponendo questioni di uguaglianza sostanziale e di rispetto del diritto all'istruzione, sancito dall'art. 34 della Costituzione e dall'art. 14 della Carta dei diritti fondamentali dell'Unione europea (CDFUE). L'eventuale utilizzo di sistemi discriminatori o non trasparenti comporterebbe, infatti, un rischio di violazione degli artt. 2 e 3 Cost., oltre che dell'art. 21 CDFUE in materia di non discriminazione.

La protezione dei dati personali costituisce l'altro asse centrale del documento ministeriale.

Le Istituzioni scolastiche, in qualità di titolari del trattamento, sono chiamate a rispettare le disposizioni del regolamento (UE) 2016/679 (GDPR) e del d.lgs. 196/2003 (Codice privacy), adottando misure di *privacy by design* e *by default*. L'attenzione alla specifica condizione dei minori, qualificati come soggetti vulnerabili dal Considerando 38 del GDPR, impone l'adozione di ulteriori cautele, quali la minimizzazione dei dati, l'anonimizzazione e il ricorso a tecniche innovative come i dataset sintetici e le *privacy-enhancing technologies*. In questo senso, la prospettiva europea sottesa all'AI Act e alle Linee guida converge nell'affermare che il diritto all'educazione digitale debba necessariamente integrarsi con il diritto alla riservatezza, ponendo i minori al centro di una tutela rafforzata.

Le Linee guida richiamano, inoltre, principi di carattere etico, quali la centralità della persona, l'equità, l'innovazione responsabile e sostenibilità, che assumono una valenza giuridica indiretta nella misura in cui orientano l'interpretazione e l'applicazione delle norme vigenti. Si tratta, tuttavia, di principi programmatici che, pur costituendo un riferimento essenziale, rischiano di restare dichiarazioni di intenti in assenza di meccanismi concreti di *enforcement*. È questo uno dei punti critici del documento: se da un lato si delineano in maniera chiara gli obblighi delle Scuole in qualità di *deployer*, dall'altro non vengono forniti strumenti operativi sufficientemente dettagliati per assicurare l'effettiva attuazione dei principi etici e giuridici.

Ulteriore elemento problematico riguarda la duplicazione degli oneri documentali, poiché alle Scuole viene richiesto di redigere sia la Valutazione d'impatto sulla protezione dei dati (DPIA) prevista dal GDPR sia la Valutazione d'impatto sui diritti fondamentali (FRIDA) introdotta dall'AI Act. Tale sovrapposizione, pur giustificata dall'esigenza di garantire una tutela multilivello, rischia di gravare eccessivamente su Istituzioni spesso prive di risorse adeguate e di competenze giuridiche e tecniche interne. Il rischio concreto è che tali valutazioni vengano ridotte a meri adempimenti formali, senza una reale capacità di prevenire violazioni dei diritti.

In prospettiva critica, occorre interrogarsi inoltre sul rapporto tra innovazione e responsabilità.

L'adozione di sistemi di IA nelle scuole può certamente contribuire a una didattica più personalizzata e inclusiva, salvaguardando *bias* discriminatori, ma la dipendenza crescente da processi automatizzati solleva il pericolo di una riduzione della funzione educativa a mera gestione tecnologica. In tal senso, il richiamo alla "sorveglianza umana" non è soltanto un presidio etico, ma una vera e propria condizione giuridica di legittimità: senza un controllo umano significativo, le decisioni algoritmiche rischiano di compromettere l'autonomia dell'insegnamento e la stessa libertà educativa.

Le Linee guida del Ministero rappresentano, certamente, un passo importante verso la regolamentazione fattiva e concreta dell'IA nel settore scolastico, ponendo le basi per un approccio integrato che tenga insieme innovazione tecnologica e tutela dei diritti fondamentali. Tuttavia, restano da sciogliere nodi rilevanti. Primo tra tutti la distribuzione della responsabilità tra fornitori e Scuole, l'effettiva capacità delle Istituzioni di adempiere agli obblighi previsti, la necessità di meccanismi di vigilanza e di sanzione più chiari. In assenza di tali garanzie, il rischio è che l'introduzione dell'IA nella Scuola si traduca in una mera digitalizzazione di processi esistenti, senza il salto di qualità promesso in termini di equità, inclusione e rispetto della dignità umana. È, quindi, necessario leggere le Linee guida come un punto di partenza, non come un traguardo. Infatti, solo attraverso un costante dialogo tra norme giuridiche, principi etici e pratiche educative sarà possibile costruire un ecosistema scolastico capace di coniugare innovazione tecnologica e tutela dei diritti.

Sullo sfondo vi è, però, un passaggio concettuale che emerge e che merita una riflessione, ed è quello che – secondo le Linee guida (par. 1.1, p.6) - qualifica l'Istituzione scolastica come *deployer* di sistemi di intelligenza artificiale, secondo la definizione introdotta dall'AI Act. Questa trasformazione

semantica e giuridica non è un mero tecnicismo normativo, ma segna un vero e proprio cambio di paradigma. La Scuola, tradizionalmente intesa come comunità educante, cioè luogo di relazioni formative, di crescita personale e di costruzione di cittadinanza, viene collocata in una dimensione nuova, quella di soggetto giuridico chiamato ad assumere responsabilità operative, organizzative e legali nella gestione di strumenti tecnologici complessi.

Il mutamento, come si è visto, produce effetti ambivalenti. Sul piano positivo, l'attribuzione dello status di *deployer* conferisce alle Istituzioni scolastiche un ruolo attivo e consapevole nella gestione delle tecnologie, sottraendole a una condizione passiva di meri utilizzatori. La Scuola diviene così presidio di legalità e garante della corretta implementazione dei sistemi di IA. Tuttavia, tale assimilazione della Scuola alla figura del *deployer* rischia di oscurare la sua natura di comunità educante. La prospettiva relazionale e umana, che dovrebbe restare il nucleo fondante dell'esperienza scolastica, può essere compressa da una visione in cui l'Istituzione è trattata alla stregua di un operatore tecnologico, gravato da obblighi burocratici e di *compliance*. In altre parole, il rischio è che l'adozione di sistemi di IA accentui la tendenza alla burocratizzazione della Scuola, trasformandola in un nodo amministrativo piuttosto che in un luogo di relazione pedagogica dove si insegna prima di tutto a pensare piuttosto che a farsi sostituire nella produzione del pensiero e delle relazioni da una macchina. Le Istituzioni scolastiche, vieppiù, non dispongono sempre delle competenze tecniche necessarie per valutare i sistemi di IA, né delle risorse economiche per garantirne una gestione sicura e trasparente. Si apre dunque un problema di adeguatezza tale per cui l'imposizione di obblighi pensati per grandi operatori pubblici o privati rischia di essere sproporzionata rispetto alla realtà concreta delle Scuole, specialmente in territori caratterizzati da fragilità socio-economiche.

Il vero nodo, allora, consiste nel bilanciare queste due dimensioni. La Scuola non può rinunciare al suo essere comunità educante, pena lo snaturamento della sua identità costituzionale. Allo stesso tempo, non può sottrarsi al ruolo di *deployer* che le viene assegnato, poiché ciò significherebbe abdicare a una parte significativa della sua funzione pubblica nella società digitale. La sfida è costruire un modello in cui la responsabilità tecnica e giuridica si integri con la missione educativa, senza che l'una soffochi l'altra.

SAMUELE FRANCESCO ROSA

https://www.mim.gov.it/documents/20182/0/MIM_Linee+guida+IA+nella+Scuola_09_08_2025-signed.pdf/b70fdc45-4b75-1f7e-73bf-eab12989b928?t=1756468797694

https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf

2025/3(5)ESt**Le Linee guida EDPB 3/2025 aperte alla consultazione pubblica sul coordinamento tra DSA e GDPR (versione 1.1 del 12 settembre 2025)**

L'11 settembre 2025, il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato per la consultazione pubblica la bozza di linee guida n. 3 del 2025 (le **Linee guida**) relative all'interrelazione tra il regolamento (UE) 2022/2065 (**Digital Services Act** o **DSA**) e il regolamento (UE) 2016/679 (**GDPR**). La consultazione pubblica resterà aperta fino al 31 ottobre 2025.

Le Linee guida hanno l'obiettivo di contribuire a un'interpretazione coerente del DSA e del GDPR, focalizzandosi su specifiche disposizioni del DSA che concernono il trattamento di dati personali da parte dei prestatori dei servizi di intermediazione (*mere conduit, caching e hosting*).

Le attività di rilevazione e rimozione di contenuti illegali ai sensi dell'art. 7 DSA possono comportare il trattamento di dati personali mediante diverse tecniche. L'EDPB chiarisce a quali condizioni l'adempimento a un obbligo legale o il legittimo interesse possano costituire un'idonea base giuridica per l'adozione di misure volte a identificare e disabilitare contenuti illegali, fornendo anche degli esempi.

I meccanismi di segnalazione e rimozione (cd. *notice and action*), così come i sistemi di gestione dei reclami richiesti dal DSA (artt. 16, 17, 20 e 23 DSA) possono comportare anch'essi il trattamento di dati personali degli individui che segnalano contenuti illegali o contestano le decisioni adottate dall'intermediario. A tal fine, il prestatore del servizio è tenuto a raccogliere solo i dati personali necessari e il meccanismo di notifica dovrebbe consentire, ma non imporre, l'identificazione del segnalante, a meno che sia necessaria per stabilire se un contenuto sia qualificabile come "illegale". Qualora sia necessario rivelare l'identità del segnalante ai destinatari del servizio interessati, il segnalante dovrebbe esserne debitamente informato. Dopo la presentazione di un reclamo ex art. 20 DSA, le conseguenti decisioni devono essere adottate dal prestatore del servizio sotto la supervisione di personale qualificato e non solamente sulla base di mezzi automatizzati. L'EDPB evidenzia che la sospensione di un *account* (art. 23 DSA) avviene senza pregiudizio rispetto ai diritti e ai rimedi previsti dal GDPR, incluso il diritto alla portabilità.

Il DSA sancisce un divieto generale per i fornitori di servizi di piattaforme online di ricorrere a *design* ingannevoli nelle loro interfacce (art. 25, par. 1 DSA), ad eccezione di quelle rientrano nell'ambito di applicazione del GDPR (art. 25, par. 2 DSA). L'EDPB illustra i principali elementi da valutare per stabilire se un *design* ingannevole rientri nel GDPR, come la presenza di un trattamento di dati personali o la modifica comportamentale dell'interessato dovuta a tale attività.

I fornitori dei servizi di piattaforme online sono tenuti a garantire la trasparenza rispetto agli annunci pubblicitari mostrati sulle loro interfacce e non devono trattare dati di natura particolare per presentare i messaggi pubblicitari profilati (art. 26 DSA). L'EDPB chiarisce che mentre l'informativa prevista dall'art. 26 DSA sarebbe resa agli interessati soltanto a trattamento già avvenuto, gli obblighi di trasparenza di cui agli artt. 13-14

GDPR prevedono che le informazioni siano fornite all'interessato al momento della raccolta di dati personali. Il divieto speciale di profilare gli utenti sulla base di dati particolari stabilito dall'art. 26, par. 3 DSA è complementare rispetto alle disposizioni degli artt. 22, par. 4 e 9, par. 2 GDPR. Il DSA vieta di profilare gli interessati sulla base di dati particolari anche qualora il fornitore della piattaforma online si avvalga di una base giuridica idonea ai sensi dell'art. 6, par. 1 GDPR e di una deroga elencata all'art. 9, par. 2 GDPR.

Nei sistemi di raccomandazione (cfr. artt. 27 e 38 DSA), i fornitori delle piattaforme online possono trattare i dati personali degli utenti per personalizzare l'ordine o la rilevanza dei contenuti loro mostrati. Si tratta di sistemi che sollevano preoccupazioni in relazione all'accuratezza, alla trasparenza delle inferenze e delle combinazioni di dati personali, oltre ai potenziali rischi associati al trattamento su larga scala e di dati particolari. L'EDPB osserva che non si può escludere che la presentazione di contenuti specifici agli utenti di una piattaforma online tramite un sistema di raccomandazione costituisca una "decisione" ai sensi dell'art. 22, par. 1 GDPR, in particolare quando può avere gravi conseguenze per gli individui. Per quanto concerne, in particolare, le grandi piattaforme online, i fornitori dovrebbero presentare agli utenti almeno un'opzione tra i diversi sistemi di raccomandazione non basata sulla profilazione. Finché l'opzione non basata sulla profilazione è attiva, il fornitore non dovrebbe continuare a raccogliere e trattare dati personali per profilare l'utente. Inoltre, qualora l'utente utilizzi sia la versione del sistema di raccomandazione basata sulla profilazione sia quella priva, il fornitore dovrà astenersi dal profilare l'utente durante l'uso della versione senza profilazione.

L'EDPB accoglie positivamente l'intento del DSA di garantire un livello elevato di tutela della riservatezza, della sicurezza e della protezione per i minori utenti delle piattaforme online. Le Linee guida riconoscono che l'art. 28, par. 1 e 2 del DSA può costituire un "obbligo legale" ai sensi dell'art. 6, par. 1 lett. c) GDPR e, dunque, un valido presupposto di liceità per il trattamento dei dati personali effettuato per finalità di tutela dei minori online, a condizione che tale trattamento necessario e proporzionato. Proteggere i minori nel contesto delle piattaforme online è una preoccupazione crescente, da bilanciare con la tutela del diritto fondamentale alla protezione dei dati personali di tutti gli utenti di tali servizi. Pertanto, l'EDPB ritiene che i fornitori di piattaforme online debbano evitare di adottare meccanismi di verifica dell'età che consentano un'identificazione online univoca dei loro utenti e non dovrebbero stimare o verificare e conservare permanentemente l'età o la fascia d'età del destinatario del servizio come risultato del processo di stima dell'età. Gli artt. 34 e 35 DSA impongono ai fornitori di piattaforme e motori online di dimensioni molto grandi di valutare e mitigare i rischi sistemici dei loro servizi, compresa la diffusione di contenuti illegali e la compromissione di diritti fondamentali, inclusa la protezione dei dati personali. L'EDPB interpreta e ritiene che la verifica dell'età dovrebbe essere effettuata in funzione del rischio per i minori, tenendo conto dei principi di necessità e proporzionalità del GDPR secondo una lettura congiunta degli artt. 28 e 35 DSA e delle regole generali del GDPR. Pertanto, se il fornitore

del servizio ritiene che sussistano soltanto rischi modesti per gli utenti minorenni e non siano disponibili altri mezzi per accertarsi della minore età con ragionevole certezza, l'EDPB ritiene sufficiente chiedere una semplice conferma sull'età all'utente e, nel caso di dubbi, effettuare ulteriori verifiche o, in alternativa, adottare misure a beneficio di tutti gli utenti, senza operare alcuna distinzione in base all'età. Nel caso in cui siano identificati rischi sistemici, il fornitore è tenuto a effettuare la valutazione d'impatto prevista dall'art. 35 GDPR. Sul tema della verifica dell'età, l'EDPB rinvia allo Statement 1/2025 on Age Assurance.

L'EDPB ritiene importante chiarire il rapporto tra i codici di condotta sviluppati ai sensi del DSA e quelli sviluppati ai sensi del GDPR, e garantire il coinvolgimento delle autorità di protezione dei dati nello sviluppo dei primi, ove opportuno. Idealmente, i codici di condotta adottati ai sensi dell'una e dell'altra normativa sono, infatti, complementari tra di loro.

Infine, viene evidenziata la centralità della cooperazione tra i Coordinatori dei servizi digitali, la Commissione europea e le Autorità di protezione dei dati personali per assicurare un'applicazione coerente del DSA e del GDPR. Il principio di leale cooperazione impone a tali Autorità di cooperare, il che significa che esse dovrebbero consultarsi reciprocamente quando sono chiamate a esaminare se la condotta di un prestatore di servizi di intermediazione, di un titolare o di un responsabile del trattamento sia conforme alle disposizioni del quadro normativo soggetto alla vigilanza dell'altra. La consultazione reciproca è funzionale a rafforzare la certezza del diritto, evitare incoerenze regolatorie e prevenire eventuali violazioni del principio di *ne bis in idem*.

ELISABETTA STRINGHI

https://www.edpb.europa.eu/system/files/2025-09/edpb_guidelines_202503_interplay-dsa-gdpr_v1_en.pdf

2025/3(6)TB

Le Linee guida EDPB 2/2025 aperte alla consultazione pubblica sul trattamento di dati personali attraverso tecnologie blockchain (versione 1.1 dell'8 aprile 2025)

L'8 aprile 2025 il Comitato Europeo per la Protezione dei Dati (EDPB) ha pubblicato la versione 1.1 delle Linee guida 02/2025 sui trattamenti di dati personali tramite tecnologie blockchain, rimaste aperte alla consultazione pubblica fino al 9 giugno 2025.

Le Linee guida si propongono di fornire indicazioni utili ad affrontare l'elevato livello di tecnicità ed incertezza sotteso al trattamento dei dati personali nell'ambito delle blockchain, in ragione della natura distribuita e dei complessi calcoli matematici connessi a questa tecnologia.

In linea di principio, le blockchain – o più in generale le tecnologie a registro distribuito (*Distributed Ledger Technologies*, o “DLT”) - sono caratterizzate dai seguenti elementi:

- hanno una struttura nodale distribuita di tipo *peer-to-peer*, basata su catene di blocchi interconnessi crittograficamente tra loro, che permettono un sistema di conservazione dei dati decentralizzato;
- prevedono una validazione dei dati disintermediata, basata cioè su un accordo tra i partecipanti alla blockchain stessa (ad esempio, un determinato algoritmo) e che prescinde in genere dall'approvazione di un'autorità centrale;
- sono coerenti e a prova di manomissione, in quanto qualsiasi aggiornamento o rimozione dalla catena può essere agevolmente rilevato;
- sono trasparenti, poiché tutti i partecipanti possono accedere ai dati e verificarli.

Le blockchain, di cui esistono diverse tipologie e che possono essere utilizzate per fornire diversi tipi di servizi, offrono in genere forti garanzie tecniche di integrità e disponibilità in ragione degli strumenti crittografici che utilizzano, nonché del sistema decentralizzato di conservazione.

Poiché ogni transazione è registrata nella catena e destinata a rimanervi per dimostrarne l'integrità, essa non può essere individualmente rimossa o modificata, in quanto ciò evidenzerebbe un'anomalia nella catena.

Ciò comporta, nei casi in cui tali transazioni includano dati personali, delle criticità significative in un'ottica di conformità ad alcuni principi fondamentali del regolamento (UE) 2016/679 (**GDPR**): su tutti, il **principio di limitazione della conservazione** e il rispetto dei diritti degli interessati, con particolare riferimento al **diritto alla correzione** dei dati ed al **diritto alla cancellazione**.

Le Linee Guida forniscono quindi indicazioni con riferimento alle diverse possibili architetture delle blockchain e le loro implicazioni sul trattamento dei dati personali, e chiariscono i ruoli e le responsabilità che i differenti attori possono assumere nei trattamenti tramite blockchain e gli aspetti che questi devono valutare nel progettare il trattamento.

In questo contesto, secondo l'EDPB, i rischi per i diritti e le libertà degli interessati devono essere attentamente soppesati anzitutto tramite una valutazione di fatto che tenga conto di diversi elementi, quali la **natura del servizio** fornito, i **meccanismi di governance**, le **misure tecniche e organizzative** adottate, le **relazioni tra i differenti attori** coinvolti.

Dopodiché, andrebbero attentamente valutati i **rischi** per i diritti e le libertà degli interessati connessi al trattamento che si intende condurre tramite blockchain. Tale valutazione dovrebbe ponderare (i) se i dati presenti sulla blockchain includono dati personali; (ii) in tale caso, **se la tecnologia blockchain è necessaria per il trattamento**; (iii) che **tipologia** di blockchain dovrebbe essere utilizzata; (iv) quali misure tecniche e organizzative vengono utilizzate.

Quanto alle salvaguardie da applicare per evitare il caricamento di dati direttamente identificativi degli interessati, l'EDPB suggerisce una serie di misure tecniche, tra cui l'**encryption** e l'**hashing** dei dati.

L'EDPB enfatizza poi l'importanza della corretta implementazione dei **principi di cui all'art. 5 del GDPR**, evidenziandone la variabilità a seconda dei contesti e dei livelli di rischio, con particolare riferimento ai principi di

trasparenza, limitazione della finalità, minimizzazione, correttezza, integrità e limitazione della conservazione.

In particolare, ove quest'ultimo principio non venga preso in considerazione sin dalla progettazione, **secondo l'EDPB potrebbe – in alcuni casi - essere necessario cancellare l'intera blockchain**, in caso il titolare del trattamento non fosse in grado di dimostrare e documentare che un periodo di *retention* pari alla vita della blockchain è adeguato in relazione alla finalità del trattamento perseguita.

Con riferimento alla **base giuridica** del trattamento, l'EDPB sottolinea che essa vada individuata sulla base della specifica finalità per cui la blockchain viene utilizzata, nonché in relazione alla natura dei dati che vengono trattati. In particolare, **ove venga scelto il consenso, deve essere garantito che i dati possano essere cancellati o resi anonimi in caso di revoca dello stesso**.

Inoltre, l'EDPB sottolinea la necessità di implementare in modo effettivo i principi di *privacy by design e by default*, con valutazioni e misure basate sugli specifici contesti di applicazione, che potrebbero richiedere una combinazione di diverse *privacy enhancing technologies*.

le Linee guida sottolineano poi l'importanza di condurre una **valutazione d'impatto** sulla protezione dei dati prima di cominciare un trattamento che preveda l'utilizzo di una tecnologia blockchain.

Infine, l'EDPB osserva che **potrebbe essere tecnicamente impraticabile accogliere richieste di cancellazione od opposizione** al trattamento quando i dati personali sono conservati direttamente sulla blockchain. Pertanto, i titolari dovrebbero prendere in considerazione questa problematica fin dalla progettazione del trattamento, in modo da poter **rendere effettivamente anonimi** i dati in caso di ricezione di tali richieste.

Da ultimo, l'Allegato A delle Linee Guida fornisce una serie di concise **raccomandazioni** destinate ad organizzazioni intenzionate a strutturare un trattamento basato sulla blockchain.

TIMOTEO BUCCI

https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf

2025/3(7)GD

Le sanzioni irrogate il 23.4.2025 dalla Commissione europea a Meta (€ 200 milioni) e ad Apple (€ 500 milioni) per violazioni del DMA in relazione alla formula “consent or pay” di Meta per i dati raccolti su Facebook e Instagram, e alla pratica di Apple di imporre vincoli agli operatori commerciali nel presentare informazioni ed offerte alternative all'App Store di Apple

Con due distinti provvedimenti adottati entrambi in data 23 aprile 2025 la Commissione europea (la **Commissione**) ha contestato a Meta Platforms Inc. (**Meta**) (caso DMA.100055) ed Apple Inc. (**Apple**) (caso DMA.100109) di aver violato alcuni obblighi sanciti dal regolamento (UE) 2022/1925 sui

mercati digitali (**Digital Markets Act** o **DMA**). La Commissione ha di conseguenza inflitto una sanzione pecuniaria di 200 milioni di euro a Meta e di 500 milioni di euro ad Apple.

Giova premettere che Apple e Meta sono obbligate a conformarsi alle norme del DMA in quanto sono considerate *gatekeeper*, ossia imprese che, ai sensi dell'art. 2 DMA, forniscono almeno un "servizio di piattaforma di base" e che, secondo l'art. 3, cumulativamente: (i) hanno un impatto significativo sul mercato interno; (ii) gestiscono piattaforme che mettono in contatto imprese e consumatori; (iii) e occupano una posizione consolidata e duratura sul mercato.

Nel **caso Meta**, la Commissione ha rilevato la non conformità del modello c.d. *pay or consent* utilizzato da Meta all'art. 5(2) DMA, a tenore del quale il gatekeeper:

- a) non deve trattare, ai fini della fornitura di servizi pubblicitari online, i dati personali degli utenti finali che utilizzano servizi di terzi che si avvalgono di servizi di piattaforma di base del gatekeeper;
- b) non deve combinare dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi;
- c) non deve utilizzare in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa; e
- d) non deve fare accedere con registrazione gli utenti finali ad altri servizi del gatekeeper al fine di combinare dati personali, a meno che sia stata presentata all'utente finale la scelta specifica e quest'ultimo abbia dato il proprio consenso ai sensi dell'articolo 4, punto 11), e dell'articolo 7 del regolamento (UE) 2016/679 (**GDPR**), e, laddove l'utente finale abbia negato o revocato il consenso, il gatekeeper non deve ripetere la sua richiesta di consenso per la stessa finalità più di una volta nell'arco di un anno, impregiudicata in ogni caso la possibilità per il gatekeeper di avvalersi delle previsioni di cui all'articolo 6(1) lettere c), d) ed e) GDPR.

La Commissione ha rilevato che, secondo il modello *pay or consent*, agli utenti Meta viene proposta una scelta alternativa tra: (1) sottoscrivere un abbonamento mensile per utilizzare i servizi delle piattaforme senza pubblicità, e (2) acconsentire al trattamento combinato dei dati per ottenere pubblicità personalizzate. La Commissione ha contestato che offrire un modello del genere non equivale a garantire una vera possibilità di scelta ai consumatori. Gli utenti, infatti, sono sostanzialmente obbligati ad acconsentire al trattamento dei dati, salvo che non scelgano un'alternativa a pagamento. In sintesi, secondo la Commissione, Meta ha omesso di rendere disponibile agli utenti un'alternativa effettivamente equivalente in caso di diniego del consenso al trattamento per finalità di profilazione, limitandosi a prevedere un'opzione a pagamento come unica modalità per sottrarsi a tale trattamento, con ciò esercitando una pressione indiretta suscettibile di condizionare la libera espressione del consenso da parte dell'utente.

Tale condotta ha inoltre determinato, di conseguenza, una violazione della normativa in materia di protezione dei dati personali, con particolare

riferimento ai requisiti di validità del consenso ai sensi degli artt. 4 n. 11 e 7 GDPR, secondo cui il consenso deve essere libero, specifico, informato e inequivocabile e non può ritenersi tale ove condizionato da elementi di natura economica o da un'asimmetria contrattuale.

Nel **caso Apple**, invece, la Commissione ha accertato che le condizioni commerciali di Apple disponibili nell'UE non sarebbero conformi all'articolo 5(4) DMA, a tenore del quale, il gatekeeper deve consentire agli utenti commerciali, a titolo gratuito, di comunicare e promuovere offerte, anche a condizioni diverse, agli utenti finali acquisiti attraverso il proprio servizio di piattaforma di base o attraverso altri canali, e di stipulare contratti con tali utenti finali, a prescindere dal fatto che, a tal fine, essi si avvalgano dei servizi di piattaforma di base del gatekeeper.

Si premette che il servizio di piattaforma di base offerto da Apple prevede la vendita di applicazioni software (App Store). Gli utenti commerciali di tale servizio sono, quindi, gli sviluppatori di applicazioni che mettono le loro app e i loro beni e servizi digitali a disposizione degli utenti finali attraverso l'App Store. In tale contesto, i gatekeeper come Apple dovrebbero consentire agli sviluppatori di applicazioni che distribuiscono le app tramite il loro app store di orientare gli utenti finali e di concludere poi contratti con loro (all'interno o all'esterno dell'app) a titolo gratuito.

Stando a quanto accertato dalla Commissione sembrerebbe che gli sviluppatori delle app siano obbligati a rispettare rigide restrizioni riguardanti le informazioni che possono dare agli utenti Apple e le modalità con cui possono informarli.

La Commissione ritiene che l'imposizione di questi vincoli sia contrario al DMA sia dal punto di vista degli sviluppatori delle app (che sarebbero svantaggiati dall'esclusività sulle piattaforme Apple) sia da quello dei consumatori (che potrebbero perdere l'accesso alle offerte più vantaggiose a causa della mancanza di informazioni).

A luglio 2025 sia Apple che Meta hanno impugnato le decisioni della Commissione davanti al Tribunale dell'Unione Europea. Secondo Apple, la Commissione sta imponendo regole su come gestire l'App Store e condizioni commerciali che confondono gli sviluppatori e penalizzano gli utenti. Secondo Meta, la decisione della Commissione sarebbe viziata da errori di fatto e di diritto.

A questo punto non resta che attendere l'esito delle predette impugnazioni per scoprire se e in che modo Apple e Meta saranno tenute a conformarsi al DMA.

GIORGIA DIOTALLEVI

https://ec.europa.eu/competition/digital_markets_act/cases/202523/DMA_100109_929.pdf

https://ec.europa.eu/competition/digital_markets_act/cases/202525/DMA_100055_528.pdf

<https://curia.europa.eu/juris/document/document.jsf?text=apple%2Bcommissione%2Bregolamento%2B2022%252F1925&docid=304952&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=1435132#ctx1>

<https://curia.europa.eu/juris/document/document.jsf?text=meta%2Bcommissione%2Bregolamento%2B2022%252F1925&docid=304951&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=1437018#ctx1>

2025/3(8)FZ

La sanzione di €2.95 miliardi irrogata dalla Commissione europea a Google il 5 settembre 2025 per condotte anticoncorrenziali tese a favorire i propri servizi di tecnologia per pubblicità online (Google ADTECH)

Con decisione del 5 settembre 2025, la Commissione europea (la **Commissione**) ha accertato e sanzionato un abuso di posizione dominante posto in essere da Google nel settore del *display advertising* – comunemente noto come settore *adtech* – in violazione dell'art. 102 del Trattato sul funzionamento dell'Unione europea (TFUE) e dell'art. 54 dell'Accordo sullo Spazio economico europeo (Accordo SEE).

A termine del procedimento, avviato nel giugno 2021, la Commissione ha inflitto al colosso americano una ammenda di €2,95 miliardi.

L'attività di Google nel settore pubblicitario di riferimento si articola su due direttrici principali: da un lato, la vendita diretta di spazi pubblicitari sui propri siti e applicazioni; dall'altro, l'intermediazione tra inserzionisti e editori terzi, attraverso una serie di strumenti digitali. In particolare, l'ecosistema *adtech stack* – l'insieme coordinato di strumenti che consente la compravendita in tempo reale di spazi pubblicitari digitali – si compone di tre categorie di servizi: (i) *Ad server* per editori, destinati alla gestione degli spazi pubblicitari; (ii) *Buying tools - Demand-Side Platforms (DSP)*, strumenti di acquisto programmatico sull'*open web*; (iii) *Ad exchange*, ossia piattaforme d'asta in cui si incontrano in tempo reale domanda e offerta.

L'azienda informatica statunitense Google non solo opera in maniera integrata lungo l'intera filiera tramite, rispettivamente, il server "*DoubleClick for Publishers*" (DFP), gli strumenti di acquisto "Google Ads" e "DV360", nonché l'*Ad exchange* "AdX", ma, alla luce dell'indagine approfondita condotta dalla Commissione, gode anche di una posizione dominante sia nel mercato degli *Ad server* per editori, sia nel mercato per gli strumenti di acquisto programmatico sull'*open web*.

La Commissione ha osservato in merito che, a partire almeno dal 2014, Google ha attuato pratiche discriminatorie suscettibili di falsare significativamente la concorrenza nel comparto *adtech*, determinando abuso di posizione dominante attraverso la realizzazione di pratiche di *self-preferencing* dirette a favorire AdX lungo l'intera filiera. Da un lato, infatti, il server DFP informava sistematicamente AdX del valore delle migliori offerte concorrenti, consentendogli di prevalere nelle aste; dall'altro, gli strumenti di acquisto di Google privilegiavano in via selettiva AdX, evitando di collocare offerte su piattaforme rivali. Tali condotte hanno inevitabilmente rafforzato il

ruolo centrale di AdX nella catena del valore, incrementando la capacità di Google di imporre commissioni elevate e producendo effetti di esclusione nei confronti degli operatori concorrenti.

La decisione della Commissione ha imposto a Google l'obbligo di porre immediatamente fine alle condotte contestate e di presentare, entro il termine di sessanta giorni, misure idonee ad eliminare i conflitti di interesse insiti nella gestione integrata della propria filiera pubblicitaria.

È bene notare come la rilevanza della decisione vada oltre i confini europei, collocandosi in un contesto internazionale più ampio, già richiamato in questa Rubrica (v. in questa Rubrica [notizia n. 12 del numero 3/2024 \[2024/3\(12\)GD\]](#) e [notizia n. 52 del numero 4/2024 \[2024/4\(52\)GD\]](#)), relativo ai procedimenti antitrust avviati negli Stati Uniti nei confronti di Google.

In una simile prospettiva, l'intervento della Commissione contribuisce a delineare un quadro transnazionale di contrasto al potere di mercato di Google nell'*adtech*, riaffermando il ruolo delle autorità antitrust nel garantire condizioni di concorrenza effettiva e parità di accesso al mercato per inserzionisti e editori.

Momentaneamente, dunque, non resta che attendere, sia all'interno del perimetro nazionale che oltre oceano, la proposta di Google.

Nel frattempo, sia la Commissione che il *Department of Justice* statunitense (**DOJ**) hanno già sostenuto, nei rispettivi pareri preliminari, che solo la dismissione di una porzione dei servizi di Google consentirebbe di risolvere il conflitto di interessi intrinseco.

FRANCESCA ZAMPONE

https://ec.europa.eu/commission/presscorner/detail/it/ip_25_1992

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207

2025/3(9)ST

Gli accertamenti preliminari della Commissione europea del 28 luglio 2025 nei confronti di Temu per violazione del DSA relativamente alla valutazione del rischio sistemico di prodotti illegali offerti al pubblico nella sua piattaforma e l'indagine sui *dark patterns*

La Commissione europea (la **Commissione**) ha accusato il colosso dell'*e-commerce* Temu di aver violato l'articolo 34 del regolamento (UE) 2022/2065 (**Digital Services Act** o **DSA**), che impone ai fornitori di piattaforme *online* di dimensioni molto grandi di individuare, analizzare e valutare con diligenza gli eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi.

Ai sensi dell'art. 34 DSA, la valutazione del rischio deve essere specifica e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità.

A Temu, nello specifico, viene contestata la violazione dell'obbligo di "valutare correttamente i rischi di prodotti illegali in diffusione sulla sua piattaforma di vendita", trascurando il rischio sistemico derivante dalla massiccia circolazione di tali prodotti.

L'analisi preliminare di Bruxelles ha rivelato che la valutazione di rischio presentata da Temu nell'ottobre 2024 era imprecisa, basata su "informazioni generiche sul settore" anziché su dati specifici e dettagliati del proprio mercato. Ciò ha comportato misure di mitigazione inadeguate contro la diffusione di prodotti illegali.

A corroborare la tesi accusatoria, la Commissione cita prove raccolte tramite un'operazione di c.d. *mystery shopping*. Questa attività investigativa ha dimostrato che i consumatori che acquistano su Temu hanno un'alta probabilità di imbattersi in articoli pericolosi. Esempi di prodotti non conformi, che circolano sulla piattaforma, includono **giocattoli per neonati e piccoli dispositivi elettronici che comportano rischi significativi per la salute e la sicurezza**.

La non conformità dei prodotti è una minaccia diretta alla sicurezza dei consumatori nel mercato digitale europeo e, al fine di contrastarla, il DSA mira a disegnare i confini della responsabilità delle piattaforme nell'era del commercio elettronico globale.

La vicenda che vede coinvolta la piattaforma Temu rappresenta una delle prime prove di applicazione rigorosa del DSA per garantire la sicurezza del consumatore online e la lotta alla contraffazione.

L'incremento continuo delle vendite *online* nell'Unione europea ha portato con sé un aumento di merci pericolose, false o che non rispettano le normative. Questi prodotti costituiscono una minaccia non solo per la salute e la sicurezza dei consumatori e per l'ambiente, ma anche per la concorrenza leale all'interno del mercato unico digitale.

Per affrontare questi pericoli, il Digital Services Act introduce obblighi specifici di contrasto ai contenuti illegali, prevedendo in particolare:

- a) il potenziamento degli strumenti che permettono agli utenti di segnalare i contenuti illegali e di ricorrere contro le decisioni di rimozione;
- b) obblighi di tracciabilità per i *marketplace online*, che sono tenuti a raccogliere informazioni dettagliate sui commercianti che operano sulle loro piattaforme.

Temu ha ora il diritto di esercitare la sua difesa, esaminando il fascicolo e fornendo una risposta scritta alla Commissione.

Se le conclusioni preliminari dovessero essere confermate, la Commissione adotterebbe una decisione di non conformità che potrebbe portare a sanzioni estremamente severe:

- multe: fino al 6% del fatturato annuo totale mondiale dell'azienda.
- misure correttive: ordine di adottare misure specifiche per risolvere le violazioni, potenzialmente seguito da un periodo di vigilanza rafforzata.

L'indagine, avviata a ottobre 2024 nei confronti di Temu, non si esaurisce con la questione della sicurezza dei prodotti. La Commissione sta infatti proseguendo gli accertamenti su altri profili di potenziale non conformità al *DSA*, tra cui:

- i. l'efficacia complessiva delle misure di mitigazione dei rischi;
- ii. l'uso di funzionalità di *design* ingannevoli che manipolano le scelte degli utenti;
- iii. la trasparenza dei sistemi di raccomandazione dei prodotti e la loro influenza sul consumatore;
- iv. l'effettivo accesso ai dati da parte dei ricercatori abilitati, cruciale per un'analisi indipendente dei rischi.

L'indagine che la Commissione sta conducendo su Temu non è isolata, ma svolta in collaborazione con una serie di enti, tra cui i supervisori nazionali per i servizi digitali, le autorità che si occupano di dogane e quelle che vigilano sul mercato. Questa attività segue le linee guida stabilite nella [European Commission's e-Commerce Communication](#) del 5 febbraio 2025. Inoltre, l'indagine della Commissione procede contemporaneamente ad altre due verifiche separate:

- 1) un'indagine della [Consumer Protection Cooperation \(CPC\) Network](#)
- 2) [la prima indagine generale sulla sicurezza dei prodotti](#)

In questo modo, le autorità stanno adottando un approccio coordinato e completo per affrontare tutte le preoccupazioni relative alle pratiche commerciali di Temu.

Questo *iter* procedurale rappresenta una pietra di paragone per il futuro dell'applicazione del Digital Services Act, consolidando il ruolo del diritto europeo nella regolamentazione dei giganti del digitale e nella tutela dei diritti fondamentali dei cittadini nell'ambiente online. Il verdetto finale su Temu contribuirà a delineare i confini della responsabilità delle piattaforme nell'era del commercio elettronico globale.

SARA TOMMASI

<https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-temu-breach-digital-services-act-relation-illegal-products-its>

<https://digital-strategy.ec.europa.eu/en/library/e-commerce-communication-comprehensive-eu-toolbox-safe-and-sustainable-e-commerce>

https://ec.europa.eu/commission/presscorner/detail/fi/ip_24_5707

<https://ec.europa.eu/safety-gate/#/screen/pages/SafetyProductsOnline>

2025/3(10)AG

La prima relazione annuale dell'AGCOM quale Coordinatore dei servizi digitali ai sensi del DSA

L'Autorità per le Garanzie nelle Comunicazioni (**AGCOM** o l'**Autorità**), a cui sono state attribuite in attuazione dell'art. 49(1) del regolamento (UE) 2022/2065 (**Digital Services Act** o **DSA**) dal decreto legge n. 123/2023 (recante «*Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale*») conv. in l. 159/2023, le funzioni di Coordinatore nazionale dei Servizi Digitali (**Digital Services Coordinator** o **DSC**), ha pubblicato la prima relazione annuale sull'attività svolta nel 2024 (la **Relazione**), il primo anno di applicazione in Italia del DSA (sul d.l. 123/2023 e la designazione di AGCOM quale DSC v. in questa Rubrica la notizia n. 24 nel [numero 2/2024 \[2024/2\(24\)MVT\]](#)).

L'art. 55 DSA prevede l'obbligo di redigere tale relazione - che deve essere resa disponibile al pubblico in un formato leggibile meccanicamente - e ne prescrive l'oggetto:

1) il numero dei reclami ricevuti ai sensi dell'art. 53 DSA;

2) «a) il numero e l'oggetto degli ordini di contrastare contenuti illegali e degli ordini di fornire informazioni emessi in conformità degli articoli 9 e 10 da qualsiasi autorità giudiziaria o amministrativa nazionale dello Stato membro del coordinatore dei servizi digitali interessato; b) il seguito dato a tali ordini, quale comunicato al coordinatore dei servizi digitali ai sensi degli articoli 9 e 10».

Queste prescrizioni contenutistiche sono significative perché volte non soltanto a far acquisire contezza del grado di sicurezza, prevedibilità e affidabilità dell'ambiente digitale, quanto soprattutto alla tutela dei diritti fondamentali, ma anche a incentivare in funzione general-preventiva i prestatori di servizi intermediari e i fornitori di piattaforme online e di motori di ricerca molto grandi all'utilizzo responsabile della tecnologia digitale nel rispetto dello Stato di diritto. Sotto quest'ultimo profilo è importante, ad esempio, che i prestatori e i fornitori conoscano il numero e l'esito dei reclami proposti all'AGCOM dai destinatari del servizio e quale seguito è stato dato sempre dall'Autorità alla comunicazione effettuata alla medesima dei predetti ordini di contrasto e ordini di fornire informazioni.

La relazione dell'AGCOM prescritta dall'art. 55 DSA non è, dunque, solo una fotografia fine a se stessa di ciò che è accaduto, ma è uno strumento utile al raggiungimento del fine perseguito dal legislatore europeo di rendere l'ambiente digitale sempre più sicuro per il singolo individuo. Un insieme di elementi concorrono allo scopo, come emerge dal testo della Relazione, la quale si sofferma sui seguenti aspetti: **i)** sui reclami ricevuti dal DSC; **ii)** sugli ordini e richieste di informazioni emanati da un'autorità giudiziaria o amministrativa nazionale; **iii)** sull'attività del DSC di certificazione degli organismi che si occupano della risoluzione stragiudiziale delle controversie (**ODS** Out-of-court dispute settlement) insorte tra il prestatore dei servizi intermediari e il destinatario del servizio (art. 21 DSA); **iv)** sul rilascio da parte del DSC della qualifica di segnalatore attendibile (art. 22 DSA); **v)** sulle richieste da parte dei ricercatori accreditati stabiliti in Italia di poter accedere ai dati delle piattaforme online di dimensioni molto grandi (VLOP) e di motori di ricerca online di dimensioni molto grandi (VLOSE); **vi)** sull'attività nazionale e internazionale dell'AGCOM come DSC.

Si noterà, sintetizzando questi sei punti, come le funzioni del DSC siano complesse e di grande rilievo, perché volte a individuare e a sanzionare le violazioni del DSA e a prevenire lesioni dei diritti fondamentali, rischi sistemici, abusi da parte dei prestatori del servizio nei confronti dei destinatari dei servizi. Come pure l'attenzione del DSC si è concentrata sulle condotte illecite degli stessi destinatari dei servizi, i quali versano in rete contenuti illegali.

Di seguito si esplicitano, in sintesi, questi sei aspetti.

i) Sul diritto al reclamo. Ai sensi dell'art. 53 DSA, i destinatari del servizio e gli organismi, le organizzazioni o le associazioni incaricati di esercitare per loro conto i diritti conferiti dal DSA, in caso di supposta violazione del DSA, hanno diritto di presentare reclamo al DSC dello Stato membro in cui il destinatario del servizio è situato o stabilito. Quindi l'utente residente in Italia che ritenga di aver subito una violazione del DSA da parte del fornitore dei servizi può rivolgersi al DSC.

Quanto alla competenza di quest'ultimo a decidere sul reclamo, occorre distinguere. Il luogo di stabilimento del prestatore di servizi intermediari è l'elemento fondamentale per stabilire la competenza del DSC. Solo se il prestatore di servizi ha lo stabilimento principale in Italia, è competente a decidere il DSC italiano. Diversamente, il DSC italiano deve trasmettere il reclamo al DSC del luogo di stabilimento del prestatore di servizi intermediari, unitamente, ove lo ritenga appropriato, a un parere sulla fattispecie concreta oggetto del reclamo.

Come ci si aspettava, nella Relazione si dà atto che degli otto reclami ricevuti dal DSC nel 2024, solo in un caso è risultata la competenza dell'Autorità italiana; negli altri, si è provveduto ad inoltrare i reclami al DSC competente. Si fa presente, inoltre, che l'Italia non è sede di stabilimento di VLOP/VLOSE e che il nostro Paese «ha una struttura produttiva costituita da un gran numero di imprese di dimensioni ridotte, per cui anche le piattaforme stabilite in Italia godono, nei casi in cui siano micro e piccole imprese, dell'esenzione di cui all'art. 19 DSA». Ciò comporta che dette imprese non sono assoggettate alla sezione 3 («Disposizioni aggiuntive applicabili ai fornitori di piattaforme online») del Capo III («Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro») del DSA.

A tale proposito, il DSC ha avvertito la necessità di implementare la mappatura dei soggetti ricadenti nell'ambito di applicazione del DSA, soprattutto in caso di gruppi societari operanti in più Stati membri o di servizi ibridi (in parte ricadenti nell'ambito del DSA e in parte esclusi). Inoltre, nella Relazione si afferma che qualora si tratti - com'è per lo più - di fornitori non stabiliti in Italia occorre, in particolare, rafforzare la cooperazione con gli altri DSC, attraverso la sottoscrizione di protocolli d'intesa e con la Commissione europea.

L'avvio e il procedimento del reclamo sono ispirati ai criteri della semplicità e della rapidità, in applicazione delle regole contenute nella [delibera n. 25/25/CONS](#), contenente l'«Adozione di un regolamento di procedura per la gestione dei reclami ai sensi dell'art. 53 del Regolamento sui servizi digitali» (il **Regolamento Reclami AGCOM**).



Per presentare un reclamo occorre utilizzare l'apposito modello disponibile nel sito web dell'AGCOM, da trasmettere all'Autorità secondo le modalità previste dall'art. 3 co. 4 del Regolamento Reclami AGCOM (<https://www.agcom.it/competenze/piattaforme-online/digital-service-act/reclami-articolo-53-regolamento-servizi-digitali-DSA>).

Se il reclamo riguarda prestatori di servizi intermediari stabiliti in Italia, l'Autorità, ove ne ricorrano i presupposti, avvia il procedimento sanzionatorio entro 45 giorni dalla ricezione del reclamo. Di tale avvio è data comunicazione al reclamante e al trasgressore. Il provvedimento finale dovrà essere emesso entro 90 giorni decorrenti dalla notifica dell'avvio del procedimento (art. 6 co. 3. Regolamento Reclami AGCOM); tale termine, però, è sospeso, «informandone le parti, fino a un massimo di 60 giorni nel caso in cui sia necessario svolgere ulteriori specifici approfondimenti istruttori» (art. 6, co. 8, Regolamento Reclami AGCOM).

Se, invece, il reclamo riguarda prestatori di servizi intermediari stabiliti in un altro Stato membro, l'Autorità entro 60 giorni trasmette il reclamo al coordinatore dei servizi digitali del luogo di stabilimento del prestatore. Tuttavia, in tale caso, l'Autorità italiana dà comunicazione dell'avvenuto riscontro della ricezione del reclamo e soprattutto «comunica ogni informazione sullo stato dello stesso, resa disponibile dal coordinatore dei servizi digitali del luogo di stabilimento» (art. 5 co. 3, reg. Agcom).

Si afferma nella Relazione che degli otto reclami ricevuti, su uno soltanto il DSC si è dichiarato competente, sebbene all'esito degli accertamenti svolti si sia pronunciato il non luogo a procedere.

L'esiguo numero dei reclami dipende dalla difficoltà della materia e dalla scarsa conoscenza tra i cittadini italiani del DSA. Sempre più oggi c'è la necessità di diffondere tra tutti la conoscenza quanto meno delle normative più vicine alla vita delle persone. Nonostante questo dato, è utile sottolineare che l'oggetto dei reclami ha riguardato prevalentemente: a) la mancata o non adeguata comunicazione delle motivazioni in caso di adozione da parte del prestatore dei servizi di misure di sospensione o limitazione dell'account (art. 17 DSA; b) la difficoltà di accedere a un sistema interno (al prestatore di servizi) di gestione dei reclami o di ricevere una comunicazione chiara e argomentata in caso di esito negativo del reclamo (art. 20 DSA). Ci si riferisce, rispettivamente, a quei provvedimenti restrittivi del servizio di cui all'art. 17(1) DSA, adottati dai prestatori di servizi in ragione di contenuti illegali o incompatibili con le proprie condizioni generali e all'obbligo di istituire un sistema interno di gestione dei reclami, proposti dal destinatario del servizio a fronte di decisioni assunte contro di lui nella tipologia di quelle indicate dal par. 1 dell'art. 20 DSA. Questo sistema di reclamo deve essere attivo per almeno sei mesi dalla decisione assunta dal fornitore di piattaforme online.

ii) Sugli ordini di contrasto e di richieste di informazioni.

L'art. 9 DSA contiene la disciplina delle attività che devono essere poste in essere nell'eventualità che le autorità giudiziarie o amministrative nazionali competenti sulla base del diritto dell'Unione o nazionale emettano ordini di contrastare specifici contenuti illegali. In particolare, l'art. 9 DSA, tra le altre disposizioni, prevede al par. 3 che l'autorità che emette un simile ordine

debba trasmetterlo, unitamente alle informazioni ricevute dai prestatori dei servizi intermediari a seguito dell'ordine stesso, al coordinatore dei servizi digitali dello Stato membro della medesima autorità emittente, ossia, nel caso dell'Italia, all'AGCOM.

Una disciplina analoga è contenuta nell'art. 10 DSA a proposito degli ordini di fornire informazioni specifiche su uno o più singoli destinatari del servizio, sempre emessi dalle autorità giudiziarie o amministrative competenti sulla base del diritto dell'Unione o nazionale. Anche in questo caso è previsto, tra l'altro, l'obbligo di trasmettere l'ordine al DSC dello Stato membro dell'autorità emittente l'ordine (art. 10(3) DSA).

Nella Relazione si fa presente che nel 2024 non è stato notificato all'AGCOM alcun ordine di questi tipi (contrasto o informazione) ai sensi del DSA, e che con le autorità amministrative e giudiziarie è stata avviata un'attività volta ad elaborare protocolli d'intesa.

iii) Sulla certificazione degli organismi che si occupano della risoluzione stragiudiziale delle controversie.

L'art. 21 DSA attribuisce ai destinatari del servizio il diritto di scegliere qualunque organismo, certificato in conformità al par. 3, di risoluzione stragiudiziale delle controversie (**ODS**, da *Out-of-court dispute settlement*) insorte con il prestatore di servizi che abbia adottato una delle decisioni di cui all'art. 20(1) DSA; sono comprese anche quelle controversie oggetto dei reclami, di cui si diceva sopra, «che non è stato possibile risolvere mediante il sistema interno di gestione». Queste decisioni possono consistere nella rimozione di informazioni o nella disabilitazione dell'accesso alle stesse, in limitazioni della visibilità, nella sospensione o cessazione dell'account dei destinatari, della fornitura del servizio o dei meccanismi di monetizzazione della piattaforma.

Si segnalano anzitutto tre aspetti: *a)* i destinatari del servizio devono essere informati agevolmente e con immediatezza sulla loro interfaccia online della possibilità di avere accesso a una risoluzione extragiudiziale delle controversie; *b)* il diritto di adire un organismo "ODS" lascia impregiudicato il diritto del destinatario del servizio di rivolgersi, in qualsiasi fase, all'organo giurisdizionale competente per contestare quelle decisioni di cui all'art. 20, par. 1, DSA (art. 21 par. 1 DSA); *c)* l'organismo "ODS" non può «imporre una risoluzione della controversia vincolante per le parti»; ciò significa che le parti devono essere in grado di trovare un accordo sul modello della mediazione.

Nella Relazione si fa presente che il DSC deve certificare l'organismo di risoluzione extragiudiziale delle controversie, su richiesta di quest'ultimo, il che può avvenire solo se vengono soddisfatte tutte le condizioni di cui al par. 3 dell'art. 21 DSA. Tra queste si indicano qui, tra le altre, l'imparzialità, l'indipendenza dai fornitori di piattaforme online e dai destinatari del servizio, compresi le persone e gli enti che hanno presentato segnalazioni e l'essere in grado di risolvere le controversie in modo rapido, efficiente ed efficace sotto il profilo dei costi e in almeno una delle lingue ufficiali dell'Unione.

L'AGCOM fa presente altresì che, con la delibera n. 282/24/CONS, ha approvato il Regolamento di procedura per la certificazione degli organismi

di risoluzione stragiudiziale delle controversie e che, nel 2024, ha certificato un unico organismo “ODS”.

iv) Sul rilascio da parte del DSC della qualifica di segnalatore attendibile.

L’art. 22 DSA prevede la figura del «segnalatore attendibile», particolarmente importante ai fini della tutela dei diritti, perché l’attributo della specificazione – «attendibile» – fa sì che il fornitore della piattaforma online debba assicurare priorità alla segnalazione ricevuta da tali soggetti e dunque trattarla e deciderla senza indebito ritardo. Si badi però: resta fermo l’obbligo di trattare tutte le segnalazioni pervenute secondo i meccanismi di notifica prescritti dal DSA in modo tempestivo, diligente e non arbitrario (cons. 61 DSA).

Spetta all’AGCOM quale DSC dello Stato membro attribuire la qualifica di «segnalatore attendibile» (*trusted flagger*) su richiesta di qualunque ente stabilito nel medesimo Stato, a condizione che il richiedente dimostri di soddisfare le seguenti condizioni: «a) dispone di capacità e competenze particolari ai fini dell’individuazione, dell’identificazione e della notifica di contenuti illegali; b) è indipendente da qualsiasi fornitore di piattaforme online; c) svolge le proprie attività al fine di presentare le segnalazioni in modo diligente, accurato e obiettivo» (art. 22(2) DSA).

Anche con riguardo a questo potere dell’Agcom, con delibera n. 283/24/CONS è stato emanato il «Regolamento di procedura per il riconoscimento della qualifica di segnalatore attendibile ai sensi dell’art. 22 DSA».

La Relazione riporta che delle quattro istanze di riconoscimento della qualifica di segnalatore attendibile una è stata archiviata nel 2024, mentre nel 2025, delle tre restanti, solo in un caso si è pervenuti al riconoscimento. Non stupisce questo esito perché il segnalatore attendibile svolge una funzione particolarmente delicata che coinvolge, da un lato, la libertà di espressione del destinatario del servizio, dall’altro, i diritti fondamentali degli utenti che entrano in contatto con un determinato contenuto. Non a caso nel cons. 63 DSA si indicano quali criteri di valutazione di un contenuto online la manifesta illegalità dell’informazione o la manifesta infondatezza della segnalazione (cons. 63 DSA). Questo per sottolineare che l’attribuzione della qualifica di segnalatore attendibile deve essere molto rigorosa.

v) Sulle richieste da parte dei ricercatori accreditati stabiliti in Italia di poter accedere ai dati delle piattaforme online di dimensioni molto grandi (VLOP) e di motori di ricerca online di dimensioni molto grandi (VLOSE).

Nell’ambito della disciplina di cui all’art. 40 DSA sull’accesso ai dati e sul controllo da parte del DSC delle piattaforme e dei motori di ricerca molto grandi, è consentito anche ai ricercatori di accedere a tali dati «al solo scopo di condurre ricerche che contribuiscano al rilevamento, all’individuazione e alla comprensione dei rischi sistemici nell’Unione, come stabilito a norma dell’articolo 34, paragrafo 1, così come per la valutazione dell’adeguatezza, dell’efficienza e degli impatti delle misure di attenuazione dei rischi a norma dell’articolo 35».

I ricercatori abilitati, quindi, possono essere di supporto al DSC nell’individuare un rischio sistemico, ossia un effetto fortemente negativo su

vasta scala, che coinvolge molti utenti online e che può arrecare gravi danni ai singoli, alla società, all'economia e al corretto funzionamento della democrazia (cfr. art. 34(1) DSA nella parte in cui sono indicati i 4 gruppi di rischi sistemici).

Spetta al DSC del luogo di stabilimento conferire lo status di «ricercatori abilitati» per la specifica ricerca menzionata nella domanda di accesso ai dati, a condizione che i ricercatori dimostrino di soddisfare tutte le condizioni di cui all'art. 40(8) DSA (art. 40(9) DSA). I fornitori di piattaforme online e di motori di ricerca molto grandi sono tenuti a condividere i dati in forza di una richiesta motivata del DSC (art. 40(4) DSA), salvo nei casi di cui al par. 5 dell'art. 40 DSA.

Nella Relazione si rileva che nel 2024 non sono pervenute richieste di accesso da parte di ricercatori stabiliti in Italia. Inoltre, si fa presente che nel primo anno di applicazione del DSA l'AGCOM si è dedicata soprattutto alla preparazione dell'emanazione degli atti delegati di cui al par. 13 dell'art. 40 DSA sulle modalità di condivisione dei dati, sul rapporto col GDPR, tenendo conto anche dei diritti e degli interessi dei fornitori di piattaforme e di motori di ricerca molto grandi.

vi) Sull'attività nazionale e internazionale dell'AGCOM.

L'ultimo punto della Relazione, prima delle conclusioni, è dedicato alle azioni e iniziative nazionali e internazionali volte ad attuare il DSA, a promuoverne il rispetto degli obblighi e a rafforzare la cooperazione tra i DSC dei diversi Stati membri.

Come primo atto scaturito dalle nuove funzioni dell'AGCOM come DSC, è stato modificato il Regolamento di organizzazione e funzionamento dell'AGCOM come segue: alla *Direzione Servizi Digitali e Tutela dei Diritti Fondamentali* dell'Agcom è stata attribuita la competenza dello svolgimento delle attività preparatorie e istruttorie per le funzioni di regolamentazione, vigilanza, ispettive e sanzionatorie per l'applicazione del DSA. Invece l'*Ufficio Digital Services Coordinator*, istituito nell'ambito di tale Direzione, è stato incaricato di svolgere le attività proprie del Coordinatore dei servizi digitali con i relativi poteri previsti dal DSA nonché di collaborare con la Direzione relazioni esterne e istituzionali nello svolgimento delle attività necessarie al coordinamento dell'Agcom con la Commissione Europea, con i Coordinatori dei Servizi Digitali degli Stati membri e con le autorità nazionali competenti (delibera n. 382/24/CONS del 30 settembre 2024).

Quanto all'attività nazionale, la Relazione segnala un'attività informativa per i destinatari del servizio e per i fornitori di servizi intermediari, stante la necessità di attuare il DSA nella sua fisiologia, con particolare riferimento agli obblighi di cui agli artt. 11 («Punti di contatto per le Autorità degli Stati membri, la Commissione e il Comitato»), 12 («Punti di contatto per i destinatari del servizio») e 13 DSA («Rappresentanti legali»).

Quanto all'attività internazionale, nella Relazione si dà atto che con essa l'AGCOM ha perseguito il duplice intento di: 1) assicurare la piena collaborazione con la Commissione, gli altri DSC e il Comitato europeo dei servizi digitali (il **Comitato DSA**); 2) promuovere i valori e i principi del DSA, anche rispetto a Stati non europei.

In estrema sintesi, l'AGCOM ha partecipato a tutte le riunioni plenarie organizzate dal Comitato DSA (composto dai coordinatori dei servi digitali dei diversi Stati membri rappresentati da funzionari di alto livello, art. 62(1) DSA) al fine di «sviluppare una comprensione condivisa delle problematiche emergenti e garantire un'applicazione del DSA calibrata sulle esigenze di ogni singolo Stato».

Nella Relazione si segnala altresì la partecipazione di AGCOM agli incontri organizzati dalla Commissione europea per la formazione del personale dei DSC e tutta l'attività svolta presso gli organismi internazionali di cui è membro con l'obiettivo di promuovere l'adozione del DSA anche al di fuori dei confini dell'UE, il che garantirebbe una risposta più efficace ai problemi generati dalla circolazione di contenuti in piattaforme “globali”.

In conclusione. Dalla Relazione emerge soprattutto la necessità di mappare i soggetti che ricadono nell'ambito del DSA, di rafforzare la cooperazione con gli altri DSC, con la Commissione europea e anche con le altre Autorità nazionali coinvolte nell'applicazione del DSA e non ultimo di coinvolgere la società civile «per diffondere una maggiore consapevolezza dei diritti dei destinatari del servizio e degli obblighi dei fornitori che scaturiscono dal DSA».

ANTONIO GORGONI

<https://www.agcom.it/relazione-annuale-dellautorita-le-garanzie-nelle-comunicazioni-ai-sensi-dellarticolo-55-dsa>

<https://www.agcom.it/sites/default/files/media/allegato/2025/Digital%20Services%20Act%20-%20Relazione%20annuale.pdf>

2025/3(11)CAT

Il protocollo d'intesa del 29.7.2025 tra il Garante privacy italiano e l'AGCM

Negli ultimi anni, il confine tra le competenze delle autorità indipendenti nazionali. L'economia digitale, infatti, si fonda sulla circolazione e sull'analisi dei dati, personali e non, che rappresentano una risorsa strategica per gli operatori del mercato. Anche in virtù della recente implementazione del quadro normativo europeo in materia, gli interventi provvedimenti delle autorità indipendenti nazionali, in particolare l'Autorità garante della concorrenza e del mercato (AGCM) e il Garante per la protezione dei dati personali (Garante privacy), tendono talvolta a intersecarsi, generando problemi di coordinamento e di certezza per i differenti stakeholders.

L'esigenza di delimitare e armonizzare le rispettive sfere d'intervento delle due predette autorità non è nuova. Diversi casi recenti hanno mostrato come la condotta di un'impresa possa essere valutata sotto profili differenti: come violazione della disciplina *antitrust*, da un lato, e come trattamento illecito di dati personali, dall'altro. La questione è emersa in particolare con riferimento alle grandi piattaforme digitali, dove l'abuso di posizione dominante si

intreccia con pratiche di raccolta e utilizzo dei dati non trasparenti o sproporzionate rispetto ai fini dichiarati. Emblematici sono i procedimenti avviati dall'AGCM nei confronti di operatori come Facebook, Google e Amazon, nei quali la stessa Autorità Antitrust ha riconosciuto che l'uso improprio dei dati degli utenti può costituire una leva anticoncorrenziale, incidendo sulla libertà di scelta dei consumatori. In tali contesti, la collaborazione con il Garante Privacy si è rivelata essenziale, ma finora priva di un quadro stabile di riferimento.

Sul piano sovranazionale, la Corte di Giustizia dell'Unione Europea, con la sentenza del 4 luglio 2023 nella causa C-252/21 (sulla quale v. in questa Rubrica la notizia n. 7 nel [numero 3/2023](#) [2023/3(7)CAT] e in *Atlante*, p. 381) ha affrontato proprio il tema della possibile sovrapposizione tra competenze antitrust e privacy. La vicenda riguardava il procedimento dell'Autorità antitrust tedesca nei confronti di Meta (già Facebook) accusata di abuso di posizione dominante per aver subordinato l'accesso al servizio social alla raccolta e combinazione di dati provenienti da piattaforme terze.

La Corte ha chiarito che le Autorità garanti della concorrenza possono valutare la conformità di un trattamento di dati rispetto al GDPR, ma non sostituirsi alle Autorità di protezione dei dati. Devono, pertanto, agire nel rispetto del principio di leale cooperazione previsto dall'art. 4(3) del Trattato sull'Unione europea (TUE), informando e coordinandosi con le Autorità privacy competenti. La decisione rappresenta un punto di equilibrio importante poiché riconosce la legittimità di un approccio collaborativo nella valutazione delle pratiche di mercato, ma riafferma il ruolo centrale delle Autorità di protezione dati nella tutela dei diritti fondamentali.

In Italia, la giurisprudenza amministrativa ha avuto occasione di pronunciarsi su questioni analoghe. Con la [sentenza n. 497 del 15 gennaio 2024](#), il Consiglio di Stato ha annullato la precedente decisione del TAR Lazio che aveva escluso la competenza dell'AGCM nel sanzionare Telepass per pratiche commerciali scorrette collegate al trattamento dei dati dei consumatori. I giudici di Palazzo Spada hanno invece riconosciuto che l'AGCM può legittimamente valutare anche gli aspetti di trasparenza e correttezza informativa nel trattamento dei dati, qualora tali condotte incidano sulla libertà di scelta del consumatore. Ciò, tuttavia, non elide la competenza del Garante privacy, imponendo piuttosto un necessario coordinamento tra le due Autorità.

Proprio in questa cornice, nel tentativo di rispondere alle suesposte esigenze di chiarezza e cooperazione, il 29 luglio 2025 i Presidenti Pasquale Stanzone (Garante privacy) e Roberto Rustichelli (AGCM) hanno sottoscritto un Protocollo d'intesa che definisce il quadro operativo della collaborazione tra le due istituzioni.

L'accordo, della **durata di tre anni**, mira a garantire una più efficace azione congiunta nei casi in cui il trattamento dei dati personali assuma rilievo anche sotto il profilo concorrenziale o consumeristico e prevede una serie di disposizioni quali: **segnalazioni reciproche** tra le Autorità nei casi in cui emergano violazioni di norme di competenze trasversali; **scambio periodico di informazioni** sulle linee di intervento e sui procedimenti di comune interesse; **collaborazione in indagini conoscitive e segnalazioni congiunte**

al Parlamento e al Governo; consultazioni reciproche durante le istruttorie che presentano profili condivisi; l'istituzione di un tavolo tecnico permanente, composto dai responsabili degli uffici competenti, incaricato di coordinare le attività e proporre eventuali modifiche o integrazioni del Protocollo e, infine, l'organizzazione di incontri periodici e attività formative volte a promuovere una cultura comune della tutela del consumatore digitale e della protezione dei dati.

La sottoscrizione del Protocollo rappresenta un passo significativo verso una maggiore certezza del diritto, in linea con le tendenze europee che mirano a superare le logiche settoriali e a promuovere un approccio sistemico alle sfide dell'economia digitale.

CARMINE ANDREA TROVATO

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10152658>

2025/3(12)VH

Il provvedimento dell'AGCM del luglio 2025 di avvio di istruttoria nei confronti di Meta per abuso di posizione dominante in relazione alla pratica di *tying* consistente nell'installazione automatica del servizio di intelligenza artificiale Meta AI nella app di messaggistica WhatsApp

Con il [provvedimento n. 31634 del 30 luglio 2025](#), adottato ai sensi dell'art. 14, l. 287/1990, l'Autorità garante per la concorrenza e il mercato (AGCM) ha aperto la fase istruttoria al fine di valutare la possibile violazione dell'art. 102 del Trattato sul Funzionamento dell'Unione europea (TFUE) da parte di Meta Platforms Inc e le società del suo gruppo, Meta Platforms Ireland Limited, WhatsApp Ireland Limited e Facebook Italy s.r.l. (di seguito indistintamente **Meta**) per effetto dell'installazione automatica del servizio di intelligenza artificiale Meta AI nell'applicazione di messaggistica WhatsApp. A partire dal mese di marzo 2025, in Italia e in altri Stati membri dell'Unione europea, Meta ha abbinato al servizio di messaggistica istantanea WhatsApp un proprio servizio di intelligenza artificiale denominato Meta AI. Il servizio di Meta AI è stato reso autonomamente disponibile agli utenti senza che questi si siano attivati in tal senso. In altri termini, la scelta di Meta è stata quella di preinstallare Meta AI e di porlo in posizione prominente sulla schermata, rendendo tale servizio immediatamente disponibile per tutti i propri utenti di WhatsApp. Nello specifico, l'utilizzo delle funzioni di Meta AI avviene cliccando sull'icona circolare; a quel punto si apre una nuova chat nell'ambito della quale è possibile porre domande di qualsiasi natura all'intelligenza artificiale di Meta alle quali verrà data una specifica risposta. Inoltre, il servizio Meta AI è stato integrato anche nella barra di ricerca di WhatsApp, in posizione prominente, permettendo agli utenti di interagire direttamente con l'assistente virtuale senza dover aprire una chat separata. Nello specifico è stata collocata la voce 'Chiedi a Meta AI' nello spazio che si trova all'interno della barra di ricerca, in cui si può digitare direttamente

una domanda o, in alternativa, si può selezionare uno dei suggerimenti proposti.

Sulla base di questi elementi, l'AGCM ha ritenuto di adottare il provvedimento in questione al fine valutare la potenziale sussistenza e consistenza di un abuso di posizione dominante da parte di Meta, in violazione dell'art. 102, TFUE. Più nel dettaglio, la pratica anticoncorrenziale presa in considerazione è quella del c.d. *tying*, ossia la decisione di un'impresa dominante di offrire, a determinate condizioni, un prodotto o servizio principale (nel caso di specie, WhatsApp) congiuntamente all'utilizzo di un prodotto o servizio abbinato (nel caso di specie il servizio Meta AI, integrato con WhatsApp).

Il ragionamento alla base delle valutazioni dell'Autorità muove dalla perimetrazione dei mercati rilevanti: da un lato, la condotta di Meta si colloca nel contesto del mercato dei servizi di comunicazione tra utenti via *app*, nella sua ulteriore articolazione dei servizi di messaggistica istantanea; dall'altro, la condotta di Meta è letta nella cornice del mercato dei servizi di AI di Chatbot o Assistenti AI che si caratterizzano per l'offerta ai consumatori finali di un servizio di intelligenza artificiale funzionale a rispondere a quesiti generalisti, di varia natura e offrire forme di interazione simili ai c.d. assistenti virtuali. Coerentemente a questa operazione *finium regondurum*, l'AGCM rileva la strutturale disomogeneità dei servizi di Whatsapp e Meta AI, qualificati da caratteristiche tecnologiche differenti e delle diverse esigenze di domanda a cui tali servizi rispondono. Di conseguenza, l'avvenuta preinstallazione di Meta AI sull'app WhatsApp, con possibilità di utilizzo nell'ambito di una chat dedicata e/o in alto nella barra degli strumenti (opzione questa disponibile solo per il servizio di AI di Meta), appare idonea a conferire a Meta, che detiene una posizione dominante nel mercato dei servizi di comunicazione per i consumatori via app, un vantaggio competitivo nel mercato dei servizi di AI Chatbot o Assistenti AI in quanto, con modalità pressoché istantanea, i milioni di utenti di WhatsApp (più di 120 milioni in Europa) sono diventati milioni di possibili utenti di Meta AI. Gli utenti, infatti, possono accedere, su WhatsApp, solo al servizio di Meta AI con modalità immediate e ben più agevoli rispetto a quanto si richieda loro per accedere ai servizi simili di altri operatori, trovando Meta AI già integrato nell'ambito del servizio WhatsApp. In altri termini, Meta appare in grado di trainare l'ingente numero dei propri clienti dal mercato in cui è dominante in quello nascente dei servizi di intelligenza artificiale, non già per mezzo di una concorrenza basata sui meriti, ma "imponendo" la disponibilità dei due servizi distinti agli utenti. Inoltre, è possibile che Meta addestri il proprio modello di AI sui dati e/o sulle interazioni con la base utenti del servizio in cui detiene una posizione dominante. Il possibile trascinarsi della user base ed il possibile utilizzo dei dati e delle interazioni con essa ai fini di addestramento del proprio modello di AI sono suscettibili di generare effetti escludenti anche considerato il rischio di lock-in o dipendenza funzionale degli utenti che potrebbero utilizzare meno le AI concorrenti, in quanto il servizio di Meta AI memorizza le informazioni fornite nel tempo e, dunque, le risposte diventano più utili e rilevanti al crescere dell'utilizzo di Meta AI.



[https://www.agcm.it/dotemsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/4A42216BF3C9F531C1258CDD0038CC8B/\\$File/p31634.pdf](https://www.agcm.it/dotemsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/4A42216BF3C9F531C1258CDD0038CC8B/$File/p31634.pdf)

| 1050

2025/3(13)OL

Il provvedimento di inibizione provvisoria del Garante privacy italiano dell'11.9.2025 relativo al sistema di riconoscimento facciale *FaceBoarding* utilizzato presso l'aeroporto di Milano Linate

Con [decisione dell'11 settembre 2025](#) (il **Provvedimento GPDP**) il Garante per la protezione dei dati personali (il **Garante** o l'**Autorità o GPDP**) ha disposto la limitazione provvisoria del trattamento dei dati biometrici operato da SEA S.p.A. (**SEA**) attraverso il sistema "*FaceBoarding*" presso l'aeroporto di Milano Linate. La determinazione si fonda sull'applicazione del [parere n. 11/2024](#) del Comitato europeo per la protezione dei dati (**EDPB o il Comitato**) del 24.5.2024 sull'uso delle tecnologie di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree per snellire il flusso dei passeggeri negli aeroporti (il **Parere EDPB**), che aveva individuato specifici scenari di conformità al regolamento (UE) 2016/679 (**GDPR**) (sul Parere EDPB v. in questa Rubrica il contributo n. 15 del [numero 2/2024](#) [2024/2(15)VR])

L'istruttoria ha accertato che il sistema implementato da SEA ricadeva nello "Scenario 3.1" del Parere EDPB, caratterizzato dalla conservazione centralizzata dei modelli biometrici sotto il controllo del gestore aeroportuale, configurazione giudicata dal Comitato intrinsecamente non conforme al GDPR. Le verifiche ispettive del Garante hanno inoltre rivelato una pluralità di violazioni: informativa contenente indicazioni inesatte, assenza di cifratura dei *template* biometrici, conservazione sproporzionata fino a 12 mesi e, più gravemente, generazione automatica di *template* biometrici anche per passeggeri non consenzienti ai varchi "ibridi".

La misura di limitazione provvisoria, adottata *ex art.* 58(2)(f) GDPR ha effetto immediato e rimarrà in vigore fino al completamento dell'istruttoria, interessando un trattamento che alla data del 31 luglio 2025 aveva coinvolto 24.550 soggetti.

Il Provvedimento GPDP, si configura quale *exemplum* di sicuro rilievo dell'**approccio preventivo nella governance delle tecnologie emergenti**. L'aspetto più significativo dell'intervento dell'Autorità risiede nel suo carattere proattivo: non si tratta di una mera sanzione *ex post*, ma di un paradigma di regolazione preventiva che delinea i confini entro cui l'innovazione tecnologica può legittimamente dispiegarsi nel rispetto dei diritti fondamentali della persona.

Il Provvedimento GPDP si pone in linea con il parere EDPB dove vengono riconosciuti conformi al GDPR solo due scenari architetture: la conservazione del modello biometrico unicamente sul dispositivo



dell'utente (scenario 1) e la conservazione centralizzata in forma cifrata con chiave segreta nota esclusivamente al passeggero (scenario 2). Entrambe le soluzioni condividono un principio cardine: il controllo effettivo ed esclusivo sui dati biometrici da parte dell'interessato (il Provvedimento GPDP ha richiamato in proposito la sez. 3.2.3.1 del Parere EDPB).

Il sistema *FaceBoarding* utilizzato da SEA, invece, è stato ritenuto “pienamente riconducibile allo scenario 3”, specificamente il 3.1, caratterizzato dalla “conservazione centralizzata dei modelli biometrici in una banca dati all'interno dell'aeroporto, sotto il controllo del gestore aeroportuale”. Questo schema è stato giudicato dall'EDPB, e di riflesso dal Garante, intrinsecamente non conforme ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita e di sicurezza del trattamento.

La questione si inserisce nel più ampio dibattito sulla natura dei dati biometrici, che costituiscono “dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca” (art. 4, n. 14 GDPR).

L'analisi delle violazioni accertate

L'istruttoria del Garante ha messo in luce non una singola criticità, ma un quadro di elementi che è stato ritenuto dall'Autorità indicativo di una non conformità diffusa e di una carente implementazione dei principi fondamentali del GDPR.

In primo luogo, l'Autorità ha accertato che l'informativa privacy fornita agli utenti conteneva “indicazioni inesatte”, asserendo che in caso di adesione tramite app il modello biometrico sarebbe rimasto conservato esclusivamente sullo smartphone del passeggero. Il Garante ha ritenuto questo riferimento in contrasto con la disposizione dell'art. 13 GDPR, che prescrive le informazioni da fornire qualora i dati personali siano raccolti presso l'interessato.

Nel Provvedimento GPDP si rileva inoltre che la società “non ha adottato misure di cifratura del *template* biometrico, all'atto della conservazione di quest'ultimo nei propri sistemi”. In un contesto che tratta dati biometrici, la cui compromissione ha conseguenze permanenti e irreversibili, l'assenza di una misura di sicurezza basilare come la cifratura a riposo costituisce una violazione di particolare gravità del principio di integrità e riservatezza sancito dall'art. 5(1)(f) GDPR.

Il Garante ha censurato la violazione delle previsioni dell'art. 25 GDPR in materia di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita, e dell'art. 32 GDPR, che prescrive al titolare del trattamento l'adozione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, contemplando espressamente “la pseudonimizzazione e la cifratura dei dati personali”. In breve, il Garante ha ravvisato la violazione delle norme del GDPR a tenore delle quali il titolare è tenuto ad implementare il principio di *privacy by design*, approntando *ab origine*, sin dalla fase progettuale di qualsivoglia sistema o servizio che implichi il trattamento di dati personali, l'intero apparato di

misure tecniche e organizzative necessarie ad assicurare un presidio di sicurezza commisurato al grado di rischio.

Il sistema prevedeva altresì la possibilità di conservare i *template* biometrici fino a 12 mesi per gli aderenti al “Programma a lungo termine”. Avuto riguardo alla “particolare natura dei dati biometrici oggetto di trattamento e gli elevati rischi di violazione dei dati correlati alla conservazione centralizzata”, l’Autorità ha ritenuto tale opzione di 12 mesi in contrasto con il principio di limitazione della conservazione, codificato nell’art. 5(1)(e) GDPR, per il quale i dati personali devono essere “conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati”.

Forse la criticità più allarmante rilevata dal Garante è stata – infine - quella relativa ai varchi “di natura ibrida”. L’Autorità ha accertato che anche per i passeggeri che non avevano aderito al sistema, e che quindi non avevano prestato alcun consenso, “viene comunque generato un *template* biometrico” al momento del passaggio. Questo trattamento, avvenendo in totale assenza di una base giuridica, rappresenta una violazione lampante dell’art. 6 GDPR e svela una progettazione del sistema fondamentalmente incurante dei più elementari principi di protezione dei dati.

L’intervento del Garante nel caso SEA si inserisce in un contesto normativo multilivello caratterizzato da un approccio marcatamente prudenziale verso le tecnologie di riconoscimento facciale.

A livello nazionale, tale orientamento è confermato dalla moratoria, prorogata fino al 31 dicembre 2025, che sospende “l’installazione e utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale in luoghi pubblici o aperti al pubblico” (art. 9, comma 9, D.L. n. 139/2021, come modificato dall’art. 8-ter, co. 1 del D.L. 10 maggio 2023, n. 51 convertito con modificazioni dalla L. 3 luglio 2023, n. 87).

È rilevante notare che il perimetro di tale divieto è specificamente circoscritto agli “impianti di videosorveglianza”, la cui finalità è il monitoraggio generalizzato di un’area. Il sistema *FaceBoarding*, concepito come un servizio ad adesione volontaria per la facilitazione delle procedure di imbarco, si configura piuttosto come un sistema di identificazione biometrica on-demand e, in linea di principio, non rientrerebbe in tale definizione.

Proprio per questo, l’intervento del Garante non si è fondato sulla violazione della moratoria, bensì sulle gravissime non conformità dell’implementazione tecnica del sistema rispetto al GDPR. L’Autorità ha sanzionato non l’idea di un servizio basato sul consenso, ma la sua concreta e illecita realizzazione, che includeva la conservazione centralizzata e non cifrata dei dati biometrici e, soprattutto, la generazione di *template* biometrici anche per i passeggeri non aderenti al servizio, in palese violazione dell’art. 6 del Regolamento.

L’azione del Garante, pur muovendo da presupposti giuridici distinti (il GDPR e non la legge sulla moratoria), è quindi espressione della medesima filosofia di tutela preventiva. Tale approccio trova piena coerenza nel più

recente quadro normativo europeo: il Regolamento (UE) 2024/1689 (c.d. AI Act) classifica infatti l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico come una pratica vietata, ammettendola solo in situazioni eccezionali e tassativamente elencate.

Pertanto, l'Autorità si allinea a un indirizzo normativo multilivello che, pur distinguendo tra diverse tipologie di sistemi, privilegia la protezione dei diritti fondamentali della persona, esigendo che ogni innovazione basata su dati biometrici si sviluppi entro parametri di conformità, necessità e proporzionalità rigorosamente definiti.

Il provvedimento inibitorio temporaneo

Su questa base, il Garante ha esercitato i poteri correttivi che l'art. 58 GDPR attribuisce alle autorità di controllo, tra cui quello di "imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento".

L'esercizio di tale potere nel caso in esame è stato ritenuto una misura cautelativa necessaria per tutelare i diritti di decine di migliaia di cittadini da un trattamento illecito e rischioso.

Così, il Garante, ravvisata la necessità di intervenire urgentemente per tutelare i diritti e le libertà degli interessati, in ragione dell'elevata gravità delle constatate violazioni, dell'elevato numero di interessati coinvolti e della particolare natura dei dati personali trattati nel caso di specie, e ritenuto, ai sensi dell'art. 58(2)(f) GDPR, di dover adottare, in via d'urgenza la misura della limitazione provvisoria del trattamento con effetto immediato ha disposto ai sensi della medesima norma nei confronti di SEA la misura della limitazione provvisoria del trattamento dei dati biometrici dei passeggeri posto in essere, per il tramite del sistema FaceBoarding, ai fini dell'identificazione di questi ultimi ai varchi di accesso all'area sterile e ai gate di imbarco presso l'aeroporto di Milano Linate, facendo salva ogni successiva ulteriore valutazione, per il tempo necessario a consentire il completamento dell'istruttoria e con effetto immediato (a decorrere dalla data di ricezione del provvedimento).

Controllo facciale e trattamento dei dati biometrici: la precisazione del comunicato stampa del 18.9.2025

Il provvedimento in esame non è il primo adottato dal Garante in materia di riconoscimento facciale (in materia, tra gli ultimi si ricorda l'istruttoria aperta nel maggio 2024 dal Garante per il progetto di videosorveglianza con riconoscimento facciale nelle stazioni metro di Roma, su cui v. in questa Rubrica la notizia n. 36 nel [numero 2/2024](#) [2024/2(36)VR]; il provvedimento del Garante del 22 febbraio 2024 adottato sulla base del reclamo di alcuni dipendenti di una s.r.l. – la Igiene Urbana Evolution s.r.l. – che lamentavano l'installazione in un cantiere situato in Ardea di un rilevatore biometrico basato sul riconoscimento utilizzato dal datore di lavoro per rilevare la presenza degli stessi sul luogo di lavoro: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995680>; il provvedimento del Garante dell'1.1.2024 adottato nei confronti del Comune di Trento relativamente a progetti di sperimentazione nell'ambito del programma "Trento Smart City", su cui

v. in questa Rubrica la notizia n. 13 del [numero 1/2024](#) [2024/1(13)VR]. Ancor prima, si ricordano il parere del Garante del 25.3.2021 sull'utilizzo da parte del Ministero dell'Interno del sistema di riconoscimento facciale SARI, sui cui v. in questa Rubrica la notizia n. 3 nel [numero 2/2021](#) [2021/2(3)CR] e in *Atlante*, p. 80; la decisione del 10.2.2022 del Garante sul trattamento dei dati biometrici da parte di Clearview AI su cui v. in questa Rubrica la notizia n. 8 sul [numero 1/2022](#) [2022/1(8)GDI] e in *Atlante*, p. 167; utilizzato; il comunicato del Garante del 14.11.2022 di avvio di istruttorie per i sistemi di videosorveglianza dei Comuni di Lecce e di Arezzo, su cui v. in questa Rubrica la notizia n. 12 nel [numero 4/2022](#) [2022/4(12)VR] e in *Atlante*, p. 269).

Per evitare che fossero diffusi equivoci sul suo ruolo e sulla natura e la funzione dei suoi provvedimenti, - e con particolare riferimento all'ultimo provvedimento qui esaminato, quello dell'11 settembre 2025 - il Garante ha voluto sottolineare con apposito [comunicato stampa del 18 settembre 2025](#), di non aver precluso a SEA l'impiego di sistemi di riconoscimento facciale in quanto tale, bensì di aver interdetto in via temporanea il trattamento di dati biometrici relativo ad una specifica modalità implementativa, manifestamente inadeguata sotto il profilo della sicurezza e della conformità normativa, sulla base del Parere EDPB e sottolineando in proposito che già nel dicembre 2024, il Garante aveva invitato SEA “a considerare le diverse soluzioni individuate come compatibili secondo la citata disciplina europea”. Nel medesimo comunicato stampa il Garante ha precisato che “il ricorso a tecnologie di riconoscimento facciale in aeroporto è, quindi, da considerarsi consentito ma ricorrendo a soluzioni tecnologiche diverse da quella adottata da SEA, idonee a bilanciare le esigenze di semplificazione nelle operazioni di imbarco con quelle di protezione dei dati personali nel rispetto della vigente disciplina europea, con particolare riferimento al trattamento dei dati biometrici. Tali soluzioni sono quelle specificatamente indicate nel citato parere dal Comitato”.

OLINDO LANZARA

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10167745>

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10167973>

2025/3(14)EF

La sentenza della Cassazione 24204/2025 del 29.8.2025 sulla inutilizzabilità a fini disciplinari delle email personali del lavoratore dipendente

Il caso. - Con la sentenza del 29 agosto 2025, n. 24204, la Cassazione fornisce ulteriori indicazioni in tema di tutela della riservatezza del lavoratore e potere di controllo del datore di lavoro.

Nel caso in esame la Suprema Corte è stata chiamata a pronunciarsi sull'accesso da parte del datore di lavoro, dopo la cessazione del rapporto, alle comunicazioni del dipendente **estratte da account privati e fatte confluire sul server aziendale.**

In particolare, la vicenda nasce da un'azione legale per concorrenza sleale che il datore di lavoro aveva intentato contro alcuni suoi ex dipendenti.

Per dimostrare le accuse, la società aveva prodotto in giudizio delle email provenienti dagli account personali dei lavoratori, acquisite tramite una consulenza tecnica sui server aziendali.

In primo grado il Tribunale aveva accolto parzialmente il ricorso della società, relativamente all'utilizzabilità in giudizio delle comunicazioni mail dei lavoratori, affermando che, sebbene fossero state estratte da account privati, erano state fatte confluire sul server aziendale, **per cui la corrispondenza doveva considerarsi aperta e non chiusa**; inoltre, il datore di lavoro sottolineava che la conoscenza dei dati era **finalizzata ad accertare comportamenti illeciti** posti in essere dagli ex dipendenti e **non per controllare l'attività lavorativa** degli stessi.

La Corte d'Appello di Milano aveva ribaltato la decisione, giudicando quelle prove inutilizzabili per violazione della disciplina in tema di privacy. La Cassazione, chiamata a pronunciarsi sul ricorso dell'azienda contro la sentenza di appello, ha ritenuto corretta la decisione di secondo grado affermando che "la posta acquisita dal datore di lavoro **proveniva da account personali, sebbene inseriti sul server aziendale, per accedere ai quali occorreva una password**" e che tale corrispondenza è tutelata dall'**art. 8 della Convenzione Europea dei diritti dell'uomo**, che al primo comma stabilisce il principio di diritto secondo cui "ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza" e, nel secondo, le condizioni richieste affinché uno Stato possa ingerirsi nel godimento del diritto protetto.

I criteri della CEDU e la tutela della privacy – Il dato da cui muovere per una corretta comprensione della sentenza che si annota è che la posta acquisita dal datore di lavoro proveniva da account personali, sebbene inseriti sul server aziendale, per accedere ai quali occorreva una p.w. e che le indagini compiute dalla società erano state espletate quando tutti i dipendenti coinvolti avevano già rassegnato le proprie dimissioni.

Per tale motivo, secondo la Suprema Corte, i giudici di appello hanno "correttamente applicato i principi" sanciti dalla sentenza della Corte Europea per i Diritti dell'Uomo (cfr. Grande Camera, sentenza 5 settembre 2017, ricorso n. 61496/08, Barbalescu), nella quale "è stato affermato che le comunicazioni trasmesse dai locali dell'impresa nonché dal domicilio di una persona possono essere comprese nella nozione di 'vita privata' e di 'corrispondenza'" contenuta all'articolo 8 della Convenzione Europea dei diritti dell'uomo".

Si applica lo stesso principio alle e-mail inviate dal luogo di lavoro, che godono di analoga tutela, anche in considerazione del fatto che la linea di confine tra l'ambito lavorativo e professionale e quello strettamente privato non può sempre essere tracciata in modo netto.

Il caso della sentenza Barbalescu riguardava il licenziamento di un ingegnere romeno intimato sulla base del controllo svolto dal datore di lavoro sulla chat dell'account aziendale Yahoo Messenger di cui era stato verificato l'utilizzo a fini privati in violazione del regolamento aziendale.

Ribaltando la pronuncia della sezione semplice, la Grand Chambre aveva accolto il ricorso del ricorrente, ritenendo non provato l'assolvimento dell'obbligo informativo in capo al datore di lavoro circa la possibilità che le comunicazioni che effettuava mediante l'account aziendale avrebbero potuto essere monitorate, né del carattere o della portata del monitoraggio o del livello di intrusività del controllo nella sua vita privata e nella sua corrispondenza.

Che il diritto al rispetto della "vita privata" sancito dall'art. 8 Cedu ricomprenda anche le attività professionali, sia che abbiano luogo in un contesto privato che pubblico, è un principio pacificamente accolto dalla Corte di Strasburgo, che in più occasioni ha verificato non solo se gli Stati membri si siano astenuti dal porre in essere comportamenti potenzialmente lesivi della vita privata degli individui, ma anche se questi abbiano adottato misure idonee a garantire l'effettivo rispetto della loro vita privata o familiare, anche ove i comportamenti illegittimi siano stati posti in essere dai datori di lavoro.

La sentenza che si annota ha inoltre rilevato che nel giudizio di appello si è giustamente tenuto in considerazione anche dei criteri fissati dalla Cedu "in tema di rispetto dei principi della finalità legittima (il controllo nelle sue varie forme deve essere giustificato da gravi motivi), della proporzionalità (il datore di lavoro deve scegliere, nei limiti del possibile, tra le varie forme e modalità di adeguato controllo, quelle meno intrusive) e della preventiva dettagliata informazione ai dipendenti sulle possibilità, forme e modalità del controllo.

In particolare, anche nell'ambito di controlli diretti all'accertamento di illeciti, il datore di lavoro non può accedere e/o usare la corrispondenza dei propri dipendenti (ivi incluse le comunicazioni e-mail), neppure dopo la cessazione del rapporto di lavoro e per accertare eventuali condotte illecite degli stessi se proveniente da un account protetto da password e senza fornire al dipendente un'esauritiva informativa ex art. 13 regolamento (UE) 2016/679 (GDPR).

Riservatezza della corrispondenza mail e inutilizzabilità per fini disciplinari. Nel caso di specie, inoltre, i dipendenti avevano dichiarato che "non avevano impostato alcuna opzione per ricevere le mail personali sul medesimo applicativo di posta elettronica utilizzato sul pc aziendale e di non avere concesso alcuna autorizzazione", mentre "la società non aveva dimostrato di avere impartito specifiche disposizioni finalizzate a regolamentare le modalità di controllo e/o di duplicazione della corrispondenza dei lavoratori".

Inoltre, anche a voler equiparare gli account dei lavoratori a quelli aziendali, la sentenza che si annota ha ribadito che sono illegittime la conservazione e la categorizzazione dei dati personali dei dipendenti, relativi alla navigazione in Internet, all'utilizzo della posta elettronica ed alle utenze telefoniche da essi chiamate, acquisiti dal datore di lavoro attraverso impianti e sistemi di controllo la cui installazione sia avvenuta senza il positivo esperimento delle procedure di cui all'art. 4, comma 2, della L. n. 300 del 1970 (**Statuto dei lavoratori**), nel testo anteriore alle modifiche apportate dal D.Lgs. n. 151 del 2015 vigente *ratione temporis* ed in assenza dell'acquisizione del consenso individuale e del rilascio delle informative previste dal D.Lgs. n. 196 del 2003 (**Codice privacy**) e dal GDPR.

Il trattamento di quei dati si traduce, inoltre, nella violazione dell'art. 8 dello Statuto dei lavoratori, che vieta lo svolgimento di indagini sulle opinioni e sulla vita personale del lavoratore, anche se le informazioni raccolte non siano in concreto utilizzate (Cass. n. 18302/2016).

Altrettanto significativo è il richiamo alla giurisprudenza penale: l'accesso abusivo a un account e-mail protetto da password integra non solo la violazione di corrispondenza (art. 616 del c.p.), ma anche il reato di accesso abusivo a sistema informatico (art. 615 ter del c.p.).

La sentenza, pur senza richiamare espressamente la disposizione muove dall'art. 15 Cost., che, come si sa, tutela la libertà e la segretezza di ogni forma di comunicazione, a partire da quella più classica della corrispondenza.

Si tratta di un diritto inviolabile della personalità, il cui contenuto “non può subire restrizioni o limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante” e “sempreché l'intervento limitativo posto in essere sia strettamente necessario alla tutela di quell'interesse” e nei limiti stabiliti dallo stesso art. 15 Cost. (Corte cost. sent. n. 366/1991).

L'art. 15 Cost. chiarisce che l'ambito oggettivo tutelato è quello della “corrispondenza e di ogni altra forma di comunicazione”: un'accezione ampia che, alla tradizionale formula della corrispondenza epistolare, affianca una formula aperta che consente di ricondurre nell'alveo della tutela costituzionale non solo i mezzi di comunicazione esistenti all'epoca dell'entrata in vigore della Carta costituzionale, ma anche quelli resi oggi disponibili dall'innovazione tecnologica.

Ed in questa formula aperta la giurisprudenza, sia quella della Corte europea dei diritti dell'uomo che costituzionale ha fatto rientrare, ad esempio, le comunicazioni telefoniche, elettroniche, informatiche, tra cui la posta elettronica e la messaggistica istantanea (cfr. Corte cost. n. 170 del 2023, secondo cui tali comunicazioni rientrano a pieno titolo nella sfera di protezione dell'art. 15 Cost., “apparendo del tutto assimilabili a lettere o biglietti chiusi”).

Ne deriva che la condotta datoriale di accesso abusivo a mail protette da password configura sia una violazione dell'art. 616 c.p. (violazione di corrispondenza) che dell'art. 615 ter c.p.c (accesso abusivo del sistema informatico), che disciplinano le conseguenze penali previste dalla legge per chi viola il diritto costituzionale alla segretezza della corrispondenza.

Correttamente, dunque, la sentenza che si annota ha ritenuto configurabili tali reati, in relazione all'acquisizione del contenuto delle "mail" custodite nell'archivio, e con il delitto di danneggiamento di dati informatici, nel caso in cui all'abusiva modificazione delle credenziali d'accesso consegua l'inutilizzabilità della casella di posta da parte del titolare (Cass. pen. n. 18284/2019).

Conclusioni. Anche in occasione della sentenza che si annota, la Cassazione sembra far prevalere i diritti fondamentali, di rango costituzionale e comunitario, di segretezza della corrispondenza e di dignità e riservatezza dei lavoratori rispetto al potere di controllo del datore di lavoro.

Il monitoraggio da parte del datore di lavoro del lavoratore, con raccolta e conservazione di suoi dati personali, deve essere sempre eseguito nel rispetto della normativa vigente, limitato a quanto consentito dall'ordinamento e non deve mai ledere i diritti fondamentali dell'uomo.

Ancora una volta, la Cassazione evidenzia la necessità di disciplinare dettagliatamente, a livello aziendale e con appositi regolamenti/policy, i casi, le modalità e le condizioni di qualsiasi tipo di controllo aziendale sull'utilizzo di strumenti – anche elettronici – impiegati dai lavoratori, siano essi personali od aziendali, ponendo attenzione tanto alle norme giuslavoristiche (in particolare, a quelle di cui allo Statuto dei Lavoratori (artt 4 e 8)), quanto alle norme sulla privacy.

Tale decisione non stupisce, anche perché sia la giurisprudenza che il Garante per la Protezione dei Dati Personali hanno in più occasioni e da tempo affrontato il tema relativo ai limiti di utilizzabilità da parte del datore di lavoro, ai più diversi fini, della corrispondenza privata del lavoratore, delineando un quadro sempre più preciso dei limiti ai poteri di controllo datoriale.

La Corte di cassazione ha infatti più volte ribadito che l'utilizzo, da parte del datore di lavoro, delle comunicazioni e conversazioni private del lavoratore – con qualsivoglia mezzo effettuate, quale Whatsapp, posta elettronica, etc. – viola il diritto alla libertà e segretezza della corrispondenza privata di cui all'art. 15 della Costituzione.

In particolare, con riferimento all'utilizzo di tali comunicazioni nell'ambito di procedimenti disciplinari, la Suprema Corte ha chiarito esplicitamente che i messaggi scambiati in chat e/o conversazioni private non possono essere usate dal datore di lavoro a tali fini, trattandosi di corrispondenza chiusa, inviolabile ed inutilizzabile da parte di soggetti terzi estranei alla conversazione, anche ove effettuata con strumenti aziendali (cfr. da ultimo Cass. 28 febbraio 2025, n. 5334, sulla quale v., in questa Rubrica la notizia n. 21 sul [numero 1/2025](#) [2025/1(21)EF]).

Il Garante per la Protezione dei Dati Personali, da sempre interessato al tema in esame (vedi le “Linee guida del Garante per posta elettronica e Internet” del 1° marzo 2007, n. 13, doc. web n. 1387522), ha anche adottato più di recente il “Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”, (provv. del 6 giugno 2024, n. 364, doc. web n. 10026277, sul quale v., in questa Rubrica la notizia n. 30 sul [numero 2/2024](#) [2024/2(30)EG]), affrontando il delicato tema della conservazione dei

metadati di posta elettronica e fornendo, indicazioni e chiarimenti volti ad orientare le scelte organizzative e tecniche dei datori di lavori.

In particolare, i metadati di posta elettronica, che corrispondono alle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica e dalle postazioni nell'interazione che avviene tra i diversi server interagenti, comprendono generalmente gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in alcuni casi, l'oggetto del messaggio spedito o ricevuto.

I metadati di posta elettronica risultano assistiti da garanzie di segretezza, tutelate anche costituzionalmente (artt. 2 e 15 Cost.), intese ad assicurare protezione al nucleo essenziale della dignità della persona e al pieno sviluppo della sua personalità nelle formazioni sociali.

Ciò comporta che, anche nel contesto lavorativo, sussista una legittima aspettativa di riservatezza in relazione alla corrispondenza e, analogamente, agli elementi ricavabili dai dati esteriori della stessa, che ne definiscono i profili temporali (come la data e l'ora di invio/ricezione) nonché gli aspetti quali-quantitativi anche in ordine ai destinatari e alla frequenza di contatto, in quanto anche questi dati sono, a propria volta, suscettibili di aggregazione, elaborazione e di controllo (v. punto 2 del predetto Documento di indirizzo; punto 5.2 lett. b), delle Linee guida citate).

EMANUELA FIATA

www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20250829/snciv@sL0@a2025@n24204@tS.clean.pdf

2025/3(15)BG

Le sentenze del 16.9.2025 del Tribunale di Torino e del 23.9.2025 del Tribunale di Latina di condanna per responsabilità aggravata ex art. 96 c.p.c. per uso improprio del supporto di sistemi di intelligenza artificiale nella redazione di difese giudiziali

Dopo i rilevanti precedenti del Tribunale di Firenze di marzo e giugno 2025 (su cui v. in questa Rubrica la notizia n. 22 del [numero 2/2025](#) [2025/2(BG)]), due recenti pronunce dei Tribunali di Latina e di Torino, hanno affermato il principio della responsabilità aggravata per l'impiego negligente di risultati (output) di sistemi di IA nella redazione di scritti difensivi.

Le decisioni in oggetto confermano che l'utilizzo di strumenti di IA per la ricerca giurisprudenziale e la redazione degli atti è ammesso solo per attività strumentali o di supporto e non può sostituire l'elaborazione critica del professionista, il quale rimane tenuto all'obbligo di supervisione e verifica dei risultati generati.

In particolare, il **Tribunale di Torino, con sentenza del 16 settembre 2025**, ha ritenuto sussistenti i presupposti per la condanna ai sensi dell'articolo 96,

co 3 c.p.c. in un caso in cui una parte aveva proposto ricorso in opposizione nei confronti di avvisi di addebito già notificati e fatti oggetto di plurimi atti di esecuzione, anch'essi regolarmente notificati. Il ricorso presentato è stato giudicato manifestamente infondato.

L'elemento di responsabilità aggravata è stato individuato nel fatto che la ricorrente avesse agito con malafede o “*quantomeno con colpa grave*”, presentando eccezioni tutte manifestamente infondate tramite un atto risultato redatto con il supporto di strumenti di intelligenza artificiale. L'atto era costituito da un “*coacervo di citazioni normative e giurisprudenziali astratte, prive di ordine logico e in larga parte inconferenti*”. Anche le allegazioni risultavano astratte e non concretamente riferibili alla situazione oggetto del giudizio. Ad esempio, le doglianze relative al merito della pretesa creditoria e alla validità formale degli avvisi di addebito erano prive di connessione con gli specifici titoli impugnati. Inoltre, per contestare la notifica non poteva ritenersi sufficiente un mero elenco astratto di ipotesi di invalidità, ma si sarebbe dovuto contestare specificamente il mancato ricevimento dell'atto e indicare i vizi concreti, cosa non avvenuta.

Il Tribunale di Torino ha condannato quindi la ricorrente al pagamento di € 500 in favore di ciascuna delle parti convenute ex art. 96, comma 3, c.p.c., e a versare una somma equitativamente determinata di € 500 in favore della cassa delle ammende, ai sensi del comma 4 dello stesso articolo.

Analogamente, il **Tribunale di Latina con sentenza del 23 settembre 2025**, ha riscontrato i presupposti per l'applicazione della responsabilità aggravata ai sensi dell'articolo 96, comma 3, c.p.c.. La condanna è stata motivata in ragione del rilievo che il ricorso giudiziario – e, come rilevato dalla Giudice, anche “*tutti gli altri centinaia di giudizi patrocinati dal medesimo difensore*” – risultava “*evidentemente redatto con strumenti di intelligenza artificiale*”, tanto da poterlo definire “*a stampone*”.

I difetti riscontrati nell'atto erano numerosi e rilevanti. Gli scritti difensivi si distinguevano per la scarsa qualità redazionale e per la totale assenza di pertinenza rispetto alle questioni oggetto del giudizio. L'atto era composto, anche in questo caso, da un “*coacervo di citazioni normative e giurisprudenziali astratte, prive di ordine logico ed in gran parte inconferenti rispetto al thema decidendum*”. Tutte le argomentazioni risultavano manifestamente infondate.

Nella valutazione della Giudice, inoltre, la redazione con strumenti di IA risultava evidente non solo dalla qualità dell'atto, ma anche dalla “*gestione del procedimento*” e dal contegno del difensore. Difatti, questi aveva depositato le note scritte il giorno successivo al deposito del decreto di fissazione di udienza, prima ancora della notifica del ricorso e, più volte invitato a comparire per rendere chiarimenti in relazione al contegno processuale e alla duplicazione dei giudizi, non aveva ritenuto di presentarsi e spiegare le proprie ragioni.

L'azione è stata, pertanto, ritenuta introdotta in malafede o, quantomeno, con grave negligenza, tale da giustificare la condanna ex art. 96 co. 3 c.p.c.. Per tali ragioni, il ricorrente è stato condannato al pagamento della somma di € 1.000,00 in favore della controparte e € 1.000,00 in favore della cassa delle ammende.

I casi di Latina e Torino, in linea con il dibattito emerso a seguito dei provvedimenti del Tribunale di Firenze (relativamente all'utilizzo di sentenze inesistenti, frutto di c.d. "allucinazioni" di sistemi di IA), dimostrano che l'abuso o l'uso negligente di strumenti di intelligenza artificiale per la redazione degli atti processuali costituisce una condotta processuale scorretta e può integrare i presupposti della responsabilità aggravata.

Mentre in uno dei due precedenti fiorentini la condotta non fu sanzionata ai sensi dell'art. 96 c.p.c. solo perché le citazioni errate erano state utilizzate *ad colorandum* e a supporto di una tesi difensiva già valida, nei casi di Latina e Torino l'assenza di elaborazione critica e la scarsa qualità degli atti sono state considerate quali elementi integranti la malafede o la colpa grave, dimostrando che l'azione era stata temeraria o negligente fin dalla sua introduzione.

Questi precedenti confermano che nell'impiego di output di sistemi di IA il professionista debba osservare i doveri fondamentali di diligenza, competenza tecnica e verifica umana, obblighi che sono presidi imprescindibili per la corretta amministrazione della giustizia.

L'articolo 13 co.1 della Legge 23 settembre 2025, n. 132, entrata in vigore il 10 ottobre 2025, recante "*Disposizioni e deleghe al Governo in materia di intelligenza artificiale*" (su cui v. sopra la prima notizia in questo numero della Rubrica [2025/3(1)AA]), definisce i confini entro cui i sistemi di intelligenza artificiale possono essere utilizzati nell'ambito delle professioni intellettuali. Nello specifico, la norma prevede che l'utilizzo di tali sistemi nelle professioni intellettuali debba essere «**finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale** e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera». Questa disposizione si pone in linea con l'esigenza di assicurare il primato dell'apporto intellettuale del professionista e dei doveri di diligenza e competenza tecnica. Sebbene sistemi di IA possano dunque essere impiegati per attività ausiliarie, come la ricerca giurisprudenziale, tale impiego **non può sostituire l'elaborazione critica del professionista**, il quale rimane imprescindibilmente tenuto all'obbligo di supervisione e verifica dei risultati generati. I recenti arresti dei Tribunali di Latina e Torino hanno affermato pertanto un principio che può dirsi ormai anche normativamente espresso dalla nuova legge n. 132/2025 per cui il professionista resta il presidio essenziale di controllo e responsabilità, e l'IA può costituire supporto, e non surrogato della sua attività intellettuale.

BEATRICE GALLUCCI

Trib. Torino 16.9.2025, <https://urly.it/31cqps>

Trib. Latina 23.9.2025, <https://urly.it/31cqpV>

2025/3(16)FG

La storica transazione da 1,5 miliardi di dollari della class-action americana tra Anthropic e gli autori approvata in via preliminare in sede giudiziale il 25.9.2025

Ad inizio 2024, tre scrittori, Andrea Bartz, Charles Graeber e Kirk Wallace Johnson, hanno citato in giudizio Anthropic PBC (**Anthropic** o la **Società**), sostenendo che la Società avesse utilizzato illegalmente le loro opere per addestrare la sua famiglia di modelli linguistici di intelligenza artificiale "Claude" senza le dovute licenze o il consenso. A giugno 2024, il tribunale distrettuale della California ha emesso una decisione parziale, accogliendo in parte le argomentazioni di Anthropic e in parte quelle degli autori; il giudice William Alsup, nella sua analisi sul fair use, in relazione alla formazione di Large Language Models (LLM) per l'uso in sistemi di intelligenza artificiale generativa, ha distinto tra la copia da parte di Anthropic di milioni di materiali protetti da copyright allo scopo di addestrare i propri modelli e la conservazione da parte dell'azienda di copie di libri e testi per la creazione della propria biblioteca digitale. In particolare, il tribunale ha concluso che l'uso dei libri in questione da parte di Anthropic per addestrare i modelli di linguaggio allo scopo di restituire nuovi output testuali è trasformativo e quindi consentito dalla dottrina del fair use, poiché l'addestramento ha lo scopo di creare qualcosa di diverso e non di sostituire le opere originarie. La digitalizzazione da parte di Anthropic dei libri acquistati in formato cartaceo per utilizzarli come parte della propria biblioteca centrale è stata ritenuta un uso corretto, in quanto le copie digitali sostituivano quelle cartacee distrutte dopo la scansione. Diversa invece la conclusione per quanto riguarda le copie piratate: poiché Anthropic non ha mai pagato per tali copie, il tribunale ha ritenuto che queste avessero sostituito la domanda delle opere degli autori, copia per copia. Il giudice Alsup ha chiarito che "nessun danno derivante dalla pirateria può essere annullato dal successivo pagamento delle stesse opere" e ha stabilito che gli autori potevano procedere in una class action per pirateria delle loro opere. I danni legali per questo tipo di violazione, secondo la legge statunitense sul copyright, partono da 750 dollari per ogni opera violata e, considerato che la biblioteca digitale di Anthropic conteneva milioni di titoli, l'azienda ha rischiato sanzioni nell'ordine di miliardi di dollari. Proprio nell'ambito di questa class action si è sviluppata la trattativa che ha portato a uno storico accordo tra gli autori e Anthropic. Il 7 settembre 2025 il giudice Alsup ha inizialmente respinto la proposta di settlement da 1,5 miliardi di dollari, definendola "nowhere close to complete" poiché priva di una chiara definizione della classe, di un piano di notifica e di termini equi per la ripartizione dei fondi e delle spese legali. Solo dopo la presentazione di una lista completa delle opere coinvolte e di un piano di claims administration dettagliato, il 25 settembre 2025 il giudice ha concesso l'approvazione preliminare dell'accordo. Nella stessa sede, il giudice ha concesso anche l'approvazione preliminare al Plan of Distribution e al Plan for Notice, ossia al piano di ripartizione dei risarcimenti e al sistema di notifica ai titolari dei diritti, ordinando alle parti di conformarsi alle sue direttive. L'accordo, del valore di 1,5 miliardi di dollari, copre **482.460 opere letterarie** comprese nelle versioni dei dataset Library Genesis (LibGen) e Pirate Library Mirror (PiLiMi) scaricate da Anthropic e registrate presso lo U.S. Copyright Office con un ISBN o ASIN valido. Per essere incluse, le opere devono essere state registrate prima del relativo download e comunque non oltre agosto 2022.

L'intesa libera Anthropic da ogni responsabilità per gli usi passati fino al 25 agosto 2025, ma non concede alcuna licenza per utilizzi futuri, e prevede inoltre l'impegno dell'azienda a distruggere i dataset pirata oggetto della controversia. Secondo un affidavit del settlement administrator, sono stati identificati **367.824 autori e 16.237 editori**; di questi, **sono stati reperiti contatti per circa il 66% degli autori e il 97% degli editori**, e oltre 49.000 soggetti hanno già fornito informazioni di contatto tramite il sito ufficiale AnthropicCopyrightSettlement.com. Il piano di ripartizione prevede una divisione predefinita (default option) del 50% dell'importo tra autori ed editori, salvo prova documentale di accordi contrattuali differenti. Nel caso di opere con più autori, la quota autoriale viene suddivisa in parti uguali tra di loro, mentre l'editore riceve l'altra metà. Per i libri didattici (Education Works), i titolari possono deviare da questa regola anche senza documentazione, salvo conflitti che verranno risolti dal Settlement Administrator. Il sistema di notifica dispone che, se un co-titolare presenta una richiesta di pagamento, gli altri vengano automaticamente avvisati; se l'assegno inviato non viene incassato entro 18 mesi, l'importo torna al richiedente originario. I membri della classe possono scegliere di escludersi (opt-out) entro 104 giorni dall'approvazione preliminare; se anche uno solo esercita l'opt-out, l'intero libro viene escluso dal settlement. **Il valore teorico dell'accordo è di 3.000 dollari per opera**, circa quattro volte il minimo legale previsto per i danni da violazione del copyright. Tuttavia, gli importi effettivamente percepiti potrebbero aggirarsi sui 1.000-1.500 dollari per libro per gli autori tradizionali, dopo la deduzione delle spese legali e la ripartizione con gli editori, mentre gli autori indipendenti o titolari esclusivi dei diritti potranno trattenere la quota intera. Il giudice Alsup ha chiarito che non metteva in discussione l'importo complessivo dell'accordo, ma era preoccupato che il processo fosse del tutto trasparente e che non si verificassero comportamenti opportunistici, come l'uscita e il rientro strategico di alcuni autori dalla class action. **L'approvazione preliminare del 25 settembre 2025**, concessa dopo mesi di esame e 34 quesiti della Corte, segna il superamento del principale ostacolo procedurale; Alsup ha definito l'accordo "equo, ragionevole e adeguato" ai sensi della Rule 23(e)(2) delle Federal Rules of Civil Procedure, la norma che impone ai giudici di verificare che ogni accordo collettivo rispetti criteri di equità, trasparenza e adeguatezza nei confronti di tutti i membri della classe. **L'udienza per l'approvazione definitiva è prevista nel primo semestre 2026**, e i pagamenti ai membri della classe dovrebbero iniziare circa due mesi dopo la final approval. Pur non vincolando altri procedimenti, il caso Bartz v. Anthropic è considerato un modello di riferimento per le numerose class action pendenti negli Stati Uniti contro OpenAI, Meta, Stability AI e altre aziende accusate di aver utilizzato shadow libraries e database pirata per addestrare modelli generativi. Dopo la decisione della Corte Suprema in Trump v. CASA, che ha eliminato le ingiunzioni di portata nazionale, le class action restano l'unico strumento efficace per ottenere rimedi sistemici contro pratiche di addestramento illecito. Per essere valide, devono rispettare i criteri della Rule 23, rappresentanza adeguata, assenza di conflitti interni e trasparenza del processo, come ribadito nei precedenti Amchem e Ortiz. Anthropic, nel



frattempo, è ancora coinvolta in altre controversie per violazione del copyright, tra cui una promossa da Universal Music Group e altre etichette discografiche, che sostengono che l'azienda abbia utilizzato illegalmente testi musicali scaricati tramite BitTorrent. Il caso Bartz v. Anthropic rappresenta dunque un punto di svolta nel diritto d'autore dell'era dell'intelligenza artificiale, fissando standard procedurali e sostanziali destinati a orientare le future controversie collettive sull'addestramento dei modelli generativi.

FRANCESCO GROSSI

<https://assets-us-01.kc-usercontent.com/1eeb16db-4934-006e-40a6-38fa91285ebb/d8578720-9fd0-4c27-9c7f-041bac826869/Class%20Action%20Settlement%20Agreement.pdf>

2025/3(17)SR

La proposta legislativa danese del giugno 2025 per la tutela autoriale delle “repliche” digitali delle persone

La vertiginosa accelerazione dello sviluppo tecnologico, in particolare nell'ambito delle intelligenze artificiali generative, ha sollevato interrogativi profondi e trasversali circa l'adeguatezza degli strumenti giuridici tradizionali nel proteggere l'identità individuale, la creatività umana e l'integrità soggettiva dell'individuo. In questo scenario, il fenomeno dei *deepfake*, ovvero delle rappresentazioni sintetiche e iperrealistiche di volti, voci e comportamenti, sollecita una riflessione giuridica inedita, intersecando problematiche proprie del diritto d'autore, del diritto alla riservatezza e, più in generale, dei diritti della personalità.

In tale contesto, si situa una proposta di legge danese, presentata nel giugno 2025, volta a modificare la *Lovbekendtgørelse nr. 1093 af 20. august 2023* e la *lov nr. 676 af 11. juni 2024*, che mira a riconoscere un vero e proprio diritto esclusivo sulla riproduzione digitale dell'aspetto e della voce delle persone. Tale proposta è sintomatica della molteplicità delle opzioni legislative che possono immaginarsi nel tentativo di riconfigurare l'assetto assiologico della protezione giuridica dell'individuo nell'ecosistema digitale.

La proposta, si legge, ha come obiettivo principale quello di “garantire una difesa chiara contro l'abuso dei tratti personali altrui e assicurare che lo sviluppo tecnologico, specialmente l'uso dell'intelligenza artificiale per creare riproduzioni realistiche di persone e delle loro prestazioni, non comprometta integrità, credibilità, fiducia e trasparenza” (“*Hovedformålet med lovforslaget er at skabe et tydeligt værn mod misbrug af andres personlige kendetegn og sikre, at den teknologiske udvikling, herunder særligt muligheden for ved hjælp af kunstig intelligens at skabe virkelighedsnære gengivelser af personer og disses præstationer mv., ikke ender med at ske på bekostning af integritet, troværdighed, tillid og gennemsigtighed*”).

La proposta legislativa prevede l'introduzione di una normativa innovativa che attribuirebbe ai soggetti un diritto esclusivo assimilabile al *copyright* sull'utilizzazione della propria immagine, voce e “performance” digitale. Si tratta di una legislazione che, pur ancorata all'impianto del diritto d'autore,

ne estende la portata ontologica sino a ricomprendere elementi normalmente riconducibili alla sfera dei diritti della personalità. In particolare, il testo prevede che nessuna persona possa essere digitalmente “replicata” attraverso software generativi o tecniche di sintesi senza il previo consenso dell’interessato, con una tutela estesa fino a cinquant’anni *post mortem* (cfr. il nuovo § 73 a – “§ 73 a. *Virkelighedsnære digitalt genererede efterligninger af en fysisk persons personlige, fysiske kendetegn må ikke tilgængeliggøres for almenheden uden den efterlignede persons samtykke*. Stk. 2. Stk. 1 *omfatter ikke efterligninger, der hovedsagelig er udtryk for karikatur, satire, parodi, pastiche, magtkritik, samfundskritik o.l., medmindre efterligningen udgør misinformation, som konkret kan medføre alvorlig fare for andres rettigheder eller væsentlige interesser*. Stk. 3. *Beskyttelsen i stk. 1 varer, indtil 50 år er forløbet efter den efterlignede persons dødsår*”).

Il tentativo normativo, di portata paradigmatica, punta a colmare quel vuoto regolatorio che ha permesso finora una sostanziale impunità nell’uso strumentale e lesivo di identità altrui in ambiti che vanno dalla pornografia non consensuale alla disinformazione politica.

L’impostazione normativa danese appare, dunque, come una contaminazione strutturale tra le categorie del diritto d’autore e quelle del diritto della personalità, segnando un processo evolutivo che potrebbe condurre alla formalizzazione di un “diritto d’autore identitario”. Tale ibridazione trova ragione nella consapevolezza che l’elemento creativo, una volta considerato esclusivo appannaggio dell’opera dell’ingegno, possa oggi risiedere anche nell’unicità fisiognomica o vocale di un soggetto, specie se soggetto pubblico o artista.

In ambito europeo, tuttavia, tale proposta solleva non poche problematiche circa la compatibilità con la libertà di espressione sancita dall’art. 11 della Carta dei diritti fondamentali dell’UE (CDFUE), nonché con i principi del regolamento (UE) 2022/2065 (**Digital Services Act** o **DSA**), il quale disciplina in chiave sistemica la responsabilità delle piattaforme e la trasparenza nell’uso dei contenuti generati dall’IA. A ciò si aggiunge la tensione con l’AI Act, il quale distingue tra sistemi a rischio inaccettabile e sistemi a rischio limitato, introducendo obblighi di etichettatura e tracciabilità dei contenuti, ma senza ancora definire un perimetro chiaro di protezione dei diritti dell’identità personale.

Sul punto, però, è lo stesso legislatore danese a ritenere che la proposta risulti conforme agli obblighi internazionali assunti dalla Danimarca, in particolare alla Convenzione europea dei diritti dell’uomo (CEDU), con specifico riferimento all’articolo 10 sulla libertà di espressione e all’articolo 8 sulla tutela della vita privata e familiare e che si colloca inoltre nel solco del Digital Services Act, il quale introduce obblighi per i fornitori di servizi online riguardo alla rimozione dei contenuti illegali e alla trasparenza delle procedure di moderazione. Inoltre, ritiene che il contenuto della proposta si armonizzi con il quadro normativo dell’Unione europea in materia di diritto d’autore, in particolare con la direttiva (UE) 2019/790, pur non rappresentandone una diretta attuazione. Gli strumenti giuridici previsti dalla legge, viene affermato, hanno carattere autonomo, ma risultano complementari a quelli disciplinati dal diritto europeo e, infine, non

determinano conflitti con gli accordi internazionali sulla proprietà intellettuale, come la Convenzione di Berna o gli accordi TRIPS, né incidono sulla disciplina del diritto internazionale privato.

Tale proposta, come poc'anzi si accennava, si inserisce nell'alveo dell'evoluzione della categoria giuridica dei diritti della personalità volta a proteggere congiuntamente identità fisica e digitale e presenta degli elementi di unicità giuridica. Attraverso il disegno di legge, si tratta di associare e tutelare la persona (fisica quindi umana), tra le altre cose, ad una voce dalla quale se ne possono trarre caratteristiche descrittive uniche e peculiari. Un aspetto assolutamente rilevante, tenuto conto che, ad oggi, della voce dell'essere umano se ne fa ampiamente uso nelle dinamiche quotidiane interattive che avvengono attraverso l'uso di strumenti tecnologici di ultima generazione.

L'impianto della proposta danese solleva, però, una pluralità di nodi concettuali e applicativi. In primo luogo, emerge la difficoltà nel definire l'ambito oggettivo e soggettivo della tutela: se da un lato si rivendica il diritto all'identità anche da parte di cittadini stranieri (rafforzando il principio di universalità della personalità), dall'altro il legislatore si confronta con il problema della definizione della "realistica imitazione" e del grado di somiglianza richiesto perché un contenuto possa dirsi lesivo.

È altresì problematica la formulazione delle eccezioni di parodia, critica o satira, le quali, per quanto richiamate nel testo, rischiano di collidere con criteri interpretativi eccessivamente indeterminati, generando incertezza applicativa e aprendo la strada a un potenziale *chilling effect*. L'equilibrio tra tutela identitaria e libertà espressiva rappresenta, in tale ottica, un delicato esercizio di bilanciamento di valori e principi di ordine anche costituzionale. Quanto alla disciplina dei rimedi, la proposta si orienta su un sistema prevalentemente civilistico, che attribuisce ai titolari della nuova posizione giuridica soggettiva un diritto di rimozione e risarcimento, escludendo tuttavia sanzioni penali dirette per l'utente finale.

Interessante è il ruolo affidato alle piattaforme, chiamate a vigilare attivamente sulla diffusione di contenuti lesivi, pena l'irrogazione di sanzioni amministrative, in una logica che richiama il regime di responsabilità previsto dal DSA.

Sul piano della durata, come si è già anticipato, la previsione di una tutela estesa per cinquant'anni *post mortem* introduce un elemento che tende a trasformare alcuni aspetti di questi diritti in diritti a contenuto patrimoniale, simili a quelli d'autore, in controtendenza rispetto alla tradizionale prospettiva giuridica. Pertanto, la voce, il volto o l'"identità digitale" diventano beni giuridici che possono essere sfruttati economicamente, ceduti, ereditati, e tutelati anche *post mortem* per un determinato periodo. Tutto ciò in controtendenza rispetto alla tradizionale intangibilità della dignità postuma. Infatti, nella tradizione giuridica europea continentale, la dignità della persona dopo la morte non è mai stata considerata un bene su cui poter esercitare diritti patrimoniali o economici. I diritti della personalità si estinguono con la morte della persona, proprio perché sono strettamente legati all'individuo; ciò che resta è una tutela morale o simbolica della memoria e del rispetto verso il defunto, garantita ai familiari o alla collettività, ma senza

possibilità di sfruttamento economico diretto. La proposta danese rompe con questa concezione, perché stabilisce che la tutela contro i deepfake possa continuare per 50 anni dopo la morte. Ciò significa, quindi, che l'immagine o la voce di una persona diventano protetti non solo per tutelarne la dignità, ma anche come beni patrimoniali ereditabili, che i discendenti possono gestire e sfruttare economicamente.

La proposta impone, infine, obblighi tecnici di trasparenza per gli sviluppatori di modelli generativi, delineando un embrionale diritto alla tracciabilità dell'origine digitale dell'identità simulata, quale sviluppo del diritto all'informazione e alla verità.

Nella sua modernità, il modello normativo danese assume rilievo nel dibattito sull'evoluzione dei diritti della personalità in un'era digitale in cui l'identità è continuamente esposta, manipolata, riprodotta: da entità statica e inalienabile, essa si trasforma in bene fluido, da proteggere tanto contro l'appropriazione indebita quanto contro l'autosfruttamento non consapevole. In conclusione, l'esperienza danese testimonia la crescente esigenza di ripensare i fondamenti assiologici del diritto nell'epoca dell'intelligenza artificiale generativa, in cui l'identità dell'individuo diviene al contempo dato, simbolo, risorsa e vulnerabilità. La tensione tra creatività tecnologica e integrità personale impone una riflessione profonda sul ruolo del diritto come strumento di garanzia e di limite. La proposta di estendere una forma di *copyright* all'identità fisica e vocale non rappresenta tanto un'estensione del diritto d'autore, quanto la nascita di un nuovo paradigma di tutela della persona: un diritto che protegge la dignità nella sua proiezione digitale, fondato su un'inedita sinergia tra diritti della personalità, libertà di espressione e sovranità algoritmica. Solo attraverso un approccio multilivello, armonizzato e consapevole delle sfide tecnologiche, sarà possibile restituire all'individuo il controllo della propria rappresentazione nell'era delle simulazioni perfette.

SAMUELE FRANCESCO ROSA

<https://www.ft.dk/samling/20241/almdel/kuu/bilag/232/3050901.pdf>