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 dalla Dott.ssa Francesca Zampone nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia dell'Impresa dell'Università di Roma "La Sapienza" (https://dei.web.uniroma1.it/it/ogid - jodi.deap@uniroma1.it).

SOMMARIO

* 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.

ISSN 2239-8570

ISSN 2239-8570

2026/2(19)IG Il (video)gioco è una cosa seria! Il documento di raccomandazioni e buone pratiche per la protezione dei dati personali nei videogiochi emanato dalle autorità per la protezione dei dati personali spagnola e belga nel giugno 2026 – **Chiara Di Somma**

2026/2(20)AG Le Linee guida del Garante privacy italiano del 17.4.2026 sull'utilizzo di tracking pixel nelle comunicazioni di posta elettronica – **Antonio Gorgoni**

2026/2(21)GD La Corte di giustizia UE conferma in via definitiva la maxi-sanzione da 4,1 miliardi di euro inflitta a Google per abuso di posizione dominante nel caso Android (sentenza del 2.7.2026, causa C-738/22 P, Google e Alphabet c. Commissione – Google Android) – **Giorgia Diotallevi**

2026/2(22)GB La sentenza della Corte di giustizia UE nelle cause riunite C-188/24 (WebGroup Czech Republic e NKL Associates) e C-190/24 (Coyote Systems) su servizi della società dell'informazione: gli Stati membri possono esigere la verifica dell'età degli utenti di siti pornorafici e vietare la diffusione di informazioni relativi a determinati controlli operati, per motivi di ordine pubblico, sicurezza o incolumità pubblica, sul traffico stradale – **Giorgia Bincoletto**

2026/2(23)RMa-MCG Il provvedimento del Garante privacy italiano n. 342 del 14.5.2026 di avvertimento nei confronti di Myndoor s.r.l. per possibile violazione del GDPR e del Codice privacy in relazione a un componente aggiuntivo per le piattaforme di messaggistica aziendale Slack e Teams finalizzato a rilevare linguaggio, emozioni e livello di stress psicologico dei lavoratori – **Riccardo Maraga/Maria Chiara Garofalo**

2026/2(24)AGa Il provvedimento sanzionatorio n. 419 del 28.5.2026 adottato dal Garante privacy italiano nei confronti di AgID per violazione del GDPR in relazione alla migrazione da INI-PEC a INAD – **Andrea Gabrielli**

2026/2(25)CI Il provvedimento sanzionatorio dell'AGCM di 2 milioni di euro a Deghi S.p.A. per pratica commerciale scorretta per promozioni e sconti a termine sollecitati con "contatori alla rovescia" – **Cecilia Isola**

2026/2(26)AR L'ordinanza della Cassazione n. 20945/2026 sul requisito della sottoscrizione a parte e con firma digitale ai sensi dell'art. 1341 c.c. – **Alfredo Rocchi**

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, del 2025 e del 2026 non ancora raccolti nell'Atlante) sono facilmente consultabili nella sezione OGID del sito web della Rivista.

ISSN 2239-8570

2026/2(1)LC
La lettera enciclica del 15.5.2026 "*Magnifica humanitas*" del Santo Padre Leone XIV sulla custodia della persona umana nel tempo dell'intelligenza artificiale

Il 25 maggio 2026 la Santa Sede ha pubblicato la prima lettera enciclica di Papa Leone XIV, intitolata *Magnifica Humanitas*, firmata il 15 maggio, in occasione del 135° anniversario della storica *Rerum Novarum* di Leone XIII. Il documento affronta in modo organico il tema della transizione digitale globale, ponendo al centro la tutela della persona nell'era dell'intelligenza artificiale (IA). Fin dall'introduzione, è subito evidente come l'enciclica non rappresenti soltanto un manifesto morale, ma tenda a delineare una vera e propria architettura di "**algoretica**" (neologismo nato dalla crasi tra algoritmo ed etica), destinata ad influenzare i futuri dibattiti di politica del diritto, nazionali e sovranazionali. Da questa prospettiva, l'enciclica di Papa Leone XIV pone nuove sfide regolatorie, inserendosi nelle intercapedini del controverso rapporto tra persona umana e intelligenza artificiale. Ad una prima lettura del testo emerge in modo chiaro un'analisi diversificata attorno a molteplici profili di stretta rilevanza non solo per la dottrina sociale della Chiesa, ma anche per la dottrina e la prassi giuridica del nostro tempo: dal dominio della tecnica al binomio dignità-lavoro, dalla "normalizzazione della guerra", che passa dalla crisi del multilateralismo internazionale, alla polarizzazione della forza "senza limiti". Per ragioni di sintesi, si accennerà di seguito solo ad alcuni di tali profili. Il primo attiene alla **centralità della dignità umana**, punto di partenza e filo conduttore dell'intero messaggio pastorale, elevata a criterio per orientare il progresso tecnico. **La lettera papale rigetta fermamente ogni tipo di deriva tecnocratica volta a considerare la persona come un mero dataset, oggetto di profilazione e ottimizzazione algoritmica**. Al contrario, il Santo Padre sottolinea come le **debolezze umane** non devono essere considerate come bug di un sistema da correggere in vista di obiettivi transumanisti, ispirati da una sorta di darwinismo tecnologico, ma come **elementi costitutivi della dignità umana** stessa. Di conseguenza, viene fortemente sostenuto il principio di **non-discriminazione algoritmica** e la necessità di garantire che ogni decisione automatizzata (specialmente in ambiti sensibili come welfare, giustizia e sanità) mantenga sempre una **supervisione umana** (human in the loop). Un secondo tema di grande rilevanza e impatto sociale attiene alla **disinformazione** e alla **manipolazione** del consenso tramite l'IA. In questo ambito, si invoca una regolamentazione più stringente contro la proliferazione incontrollata di contenuti falsi o mistificati - deepfake - anche al fine di contrastare i fenomeni di **polarizzazione** indotti dai **meccanismi di raccomandazione**. Occorre, invece, configurare l'accesso a un'informazione attendibile e veritiera come un vero e proprio diritto fondamentale e un bene comune dell'umanità. Altro aspetto d'interesse, specialmente se posto in parallelo con lo spirito dalla *Rerum Novarum*, è quello relativo all'impatto

ISSN 2239-8570

dell'automazione sul mercato occupazionale. Qui il lavoro non viene inteso semplicemente come mezzo di sostentamento economico, ma come cardine della realizzazione della persona, ponendosi così in linea con il dettato costituzionale (cfr., in particolare, quanto alla Carta italiana, gli artt. 1, 4, 35 e 37 cost.). In quest'ottica vengono inquadrate alcune auspicate politiche attive volte ad implementare gli **ammortizzatori sociali** e la **riqualificazione professionale** per contrastare le crescenti asimmetrie di potere, economico e tecnologico, generate dalle **nuove forme di monopolio** che dominano i mercati digitali. Un altro passaggio chiave, questa volta sotto il profilo del diritto internazionale umanitario, riguarda i sistemi militari avanzati e le c.d. **armi autonome**. Leone XIV lancia un **appello per l'imposizione di un divieto assoluto di delega alla macchina di decisioni fondamentali riguardanti la vita e la morte** dell'essere umano e denuncia il fallimento irresponsabile di quella realpolitik, quale «forma di "realismo" politico, che semina nelle coscienze e nella cultura la rassegnazione a una guerra ineluttabile, e qualifica la pace e il dialogo come posizioni utopiche o irrazionali, che ignorano i rischi in campo». Per il Pontefice occorre, invece, «**disarmare l'IA**» che «non significa rinunciare alla tecnologia, ma impedirle di dominare l'umano. Significa sottrarla ai monopoli, renderla discutibile, contestabile, e quindi abitabile, restituendola alla pluralità delle culture umane e delle forme di vita». Significa, in definitiva, contrapporre alla «cultura della potenza» la «civiltà dell'amore». L'antidoto auspicato per un ritorno alla pace (che «non è una speranza ingenua né soltanto un'assenza di guerra: è frutto, sempre possibile, della giustizia e della carità) è, dunque, un rinnovato **multilateralismo** ispirato ad una governance globale giusta e condivisa. Solo in questa chiave è immaginabile un superamento della logica della «forza senza limiti» e dei blocchi geopolitici contrapposti. Aspetto quest'ultimo su cui, recentemente, la Santa Sede ha osservato come la crescente facilità con cui possono essere impiegati i sistemi d'arma ad autonomia operativa basati sull'IA renda la guerra più facilmente "praticabile" e dunque meno soggetta al controllo umano, in aperto contrasto con il principio secondo il quale il ricorso alla forza armata debba avvenire come *extrema ratio*, ovvero quale ultima risorsa in caso di legittima difesa (nel nostro ordinamento, cfr. art. 11 cost., a mente del quale: «L'Italia ripudia la guerra come strumento di offesa alla libertà degli altri popoli e come mezzo di risoluzione delle controversie internazionali […]»). Ad uno sguardo d'insieme e in prospettiva diacronica, ogni questione trattata nel testo si lascia apprezzare per lo stretto legame tra l'enciclica di Leone XIII e quella di Leone XIV, che non risulta essere unicamente celebrativo, ma risponde ad una precisa metodologia dottrinale. In entrambi i casi, infatti, la Chiesa interviene in un momento di vuoto regolatorio (1891) o di forte «**asimmetria epistemica, economica e politica**» (2026), proponendo criteri che ambiscono a ridefinire e attualizzare le categorie tradizionali nel segno di una ritrovata *magnifica humanitas*.

LUCIO CASALINI

Testo lettera enciclica

ISSN 2239-8570

2026/2(2)ES
Approvato il Digital Omnibus sulla IA: regolamento (UE) 2026/1744 dell'8.7.2026 che modifica i regolamenti (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (Omnibus digitale sull'IA)

In esito a procedura legislativa ordinaria avviata su impulso della Commissione europea (la **Commissione**) con la proposta di regolamento COM(2025)836, cd. *Digital Omnibus on AI* (su cui v. in questa Rubrica il contributo n. 6 nel numero 4/2025 in *PeM* 2025, p. 1036 e il contributo n. 1 nel numero 1/2026 in *PeM* 2026, p. 272), il Parlamento europeo e il Consiglio dell'Unione europea hanno adottato l'8 luglio 2026 il **regolamento (UE) 2026/1744** che modifica i regolamenti (UE) 2024/1689 (**AI Act** o **AIA**), (UE) 2018/1139 (in materia di aviazione civile) e (UE) 2023/1230 (**regolamento macchine**) per quanto riguarda la semplificazione dell'attuazione di regole armonizzate sull'intelligenza artificiale (Omnibus digitale sull'IA), pubblicato nella Gazzetta Ufficiale dell'UE il 24 luglio 2026 (il **Regolamento**).
La riforma dell'AI Act (sull'AI Act v. in questa Rubrica il contributo n. 2 del numero 2/2024 [2024/2(2)SO], in *PeM* 2024, p. 650) apportata dal Regolamento (la **Riforma dell'AI Act** o la **Riforma**) si inserisce in un più ampio processo di novellazione del diritto digitale dell'Unione, al dichiarato fine di apportarvi una razionalizzazione per rendere più sostenibile l'applicazione degli obblighi gravanti sugli operatori economici attivi nel settore dell'economia digitale, senza compromettere un adeguato livello di tutela dei diritti fondamentali.
Le modifiche all'AI Act sono contenute nell'art. 1 del Regolamento, che consta di 43 punti.
Riportiamo di seguito le principali modifiche, seguendo l'ordine della numerazione degli articoli dell'AI Act modificati dal Regolamento.
L'art. 1, punto 1) del Regolamento ha modificato l'**art. 1(2)(g) AIA**, estendendo le misure di sostegno già previste per le piccole e medie imprese (**PMI** o **SME**: acronimo inglese da Small Medium Enterprises), come definite all'articolo 2 dell'allegato della raccomandazione 2003/361/CE, anche alle piccole imprese a media capitalizzazione (**SMC**: acronimo inglese da Small Mid-Cap Companies), come definite al punto 2 dell'allegato della raccomandazione (UE) 2025/1099, comprese le start-up. In particolare, alle SMC vengono estese le agevolazioni regolatorie già previste per le PMI in materia di documentazione tecnica e di predisposizione di un sistema di gestione della qualità proporzionato alle dimensioni dell'impresa.
L'art. 1 punto 2) lett. a) e c) del Regolamento modificano l'art. 2 AIA, apportando **importanti modifiche all'applicazione degli obblighi previsti dagli artt. 9-15 e 17-25 AIA**, che costituiscono il cuore dell'AI Act.
Le modifiche riguardano l'applicazione di tali obblighi ai sistemi di IA ad alto rischio destinati a essere incorporati come componenti di sicurezza in un

ISSN 2239-8570

prodotto, ovvero costituenti essi stessi un prodotto o disciplinati dalla normativa armonizzata dell'Unione in qualità di componenti di sicurezza o prodotti *stand-alone*.

Per comprendere tali modifiche bisogna ricordare l'assetto previsto dall'AI Act prima della Riforma relativamente ai sistemi di IA ad alto rischio (**sistemi ad alto rischio**) la cui definizione è affidata alle disposizioni dell'art. 6 AIA che individuano due categorie di sistemi ad alto rischio attraverso il riferimento agli allegati I e III del medesimo regolamento. Segnatamente: nel paragrafo 1 dell'art. 6 AIA, viene delineata una prima categoria di sistemi ad alto rischio attraverso il riferimento all'allegato I dell'AIA contenente 20 normative di armonizzazione dell'Unione; mentre l'altra categoria di sistemi ad alto rischio è individuabile attraverso le norme dei successivi paragrafi 2 e 3, tramite l'allegato III dell'AIA, contenente un elenco di 8 settori di impiego dei sistemi di IA.

La Riforma ha toccato entrambe le categorie di sistemi ad alto rischio.

Quanto ai sistemi individuabili attraverso il riferimento all'allegato I dell'AI Act (normative di armonizzazione), già prima della Riforma era previsto un diverso trattamento venendo in rilievo a tal fine la distinzione tra le 12 fonti contenute nella sezione A di tale allegato, recante l'«elenco della normative di armonizzazione dell'Unione in base al nuovo quadro legislativo» e le 8 fonti contenute nella sezione B, recante l'«elenco di altre normative di armonizzazione dell'Unione». In particolare, l'art. 2(2) AIA già sottraeva i sistemi relativi a prodotti disciplinati dalla normativa elencata nella sezione B al regime applicabile alla generalità dei sistemi ad alto rischio, disponendo che a tali sistemi si applica unicamente la norma definitoria dell'art. 6(1), l'art. 57 (in materia di spazi di sperimentazione normativa) e gli artt. 102-109 AIA. Questi ultimi articoli dispongono che gli essenziali requisiti *ex-ante* per i sistemi di IA di alto rischio previsti nella Sezione 2 del Capo III AIA (artt. 8-15 AIA) debbano essere presi in considerazione quando si adotteranno normative attuative o delegate della medesima legislazione, e dunque prevedono una sorta di applicazione indiretta o programmatica delle norme che fissano tali requisiti attraverso la previsione di un futuro adeguamento normativo.

La Riforma è intervenuta su molti punti.

Innanzitutto, il Regolamento ha **"spostato" il regolamento macchine nella sezione B dell'allegato I dell'AI Act** assoggettandolo al regime dedicato ai sistemi relativi ai prodotti disciplinati dalle normative elencate in tale sezione, sopra richiamato: art. 1, punto 41) del Regolamento. La *ratio* di questo primo intervento si trova dichiarata nel cons. 42 del Regolamento, dove si legge che l'applicazione del reg. macchine e dell'AI Act «potrebbe portare a sovrapposizioni», e si soggiunge: «[d]ata la natura specifica delle macchine e del settore delle macchine, e al fine di rispondere alla necessità di semplificare il quadro normativo per le macchine basate sull'IA, è opportuno passare a un approccio settoriale spostando il regolamento (UE) 2023/1230 [reg. macchine] dalla sezione A alla sezione B dell'allegato I del regolamento (UE) 2024/1689 [AI Act]».

In secondo luogo, è stato **modificato l'art. 2(2) AIA** come segue «Ai sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1,

ISSN 2239-8570

relativo a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, si applicano unicamente l'articolo 6, paragrafo 1, l'articolo 60 bis e gli articoli da 102 a 112. Gli articoli 57, 58 e 59 si applicano solo nella misura in cui i requisiti per i sistemi di IA ad alto rischio a norma del presente regolamento siano stati integrati in tale normativa di armonizzazione dell'Unione». Il **nuovo art. 60 bis AIA** ivi richiamato - introdotto dall'art. 1, punto 25) del Regolamento - contiene una nuova disciplina *ad hoc* per la prova di tali sistemi in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA.

La terza modifica è molto importante. Essa riguarda, come anticipato, **l'applicazione degli obblighi previsti dagli artt. 9-15 e 17-25 AIA** ai sistemi di IA ad alto rischio di cui all'art. 6(1) AIA. Per i motivi sopra esposti, la Riforma investe pertanto sia i sistemi ad alto rischio identificabili attraverso l'elenco di cui alla sezione A dell'allegato I AIA – ai quali quelle norme si applicano direttamente - quanto i sistemi ad alto rischio identificabili attraverso l'elenco di cui alla sezione B del medesimo allegato, cui quelle norme non si applicano direttamente ma possono indirettamente condizionarne il trattamento a cagione del meccanismo di adeguamento sopra ricordato.

Il Regolamento ha introdotto un **nuovo paragrafo 13 dell'art. 2 AIA** nel quale si stabilisce che **la Commissione possa prevedere limitazioni all'applicazione degli obblighi previsti dagli artt. 9-15 e 17-25 dell'AI Act**. Il Regolamento non ha meglio individuato le tipologie di limitazioni né ha specificato di quali obblighi si tratti, ma ha richiesto alla Commissione di **adottare entro il 2 agosto 2027 atti delegati per individuare i sistemi di IA interessati, gli obblighi suscettibili di limitazione e l'estensione di tali deroghe**. In ogni caso, il nuovo paragrafo 13 dell'art. 2 AIA prevede che ogni siffatta limitazione sia condizionata alla circostanza che la normativa di armonizzazione applicabile garantisca un livello di tutela della salute, della sicurezza e dei diritti fondamentali dei consumatori equivalente o superiore e che non determini una riduzione dello *standard* complessivo di protezione.

In materia di **alfabetizzazione all'IA**, il Regolamento - art. 1, punto 5) – ha modificato **l'art. 4 AIA.** Ai fornitori e ai *deployer* di sistemi di IA è richiesto di adottare misure adeguate affinché dipendenti e collaboratori acquisiscano competenze e conoscenze in materia di IA, senza tuttavia prescrivere il conseguimento di uno specifico livello di formazione. La Commissione europea e gli Stati membri sono tenuti a sostenere gli operatori nell'adempimento di tali obblighi, anche mediante la pubblicazione di casi pratici. Il Consiglio per l'IA europeo dovrà inoltre adottare raccomandazioni, tenendo conto dei quadri europei delle competenze, al fine di supportare la Commissione e gli Stati membri nella promozione dell'alfabetizzazione all'IA e nella definizione di obiettivi comuni.

Di particolare rilievo è l'introduzione del nuovo art. 4 bis dell'AI Act - in sostituzione del paragrafo 5 dell'art. 10 AIA - che estende i casi di applicazione della **base giuridica** per il trattamento di categorie particolari di dati personali ex art. 9(1) regolamento (UE) 2016/679 (**GDPR**) per lo sviluppo e il funzionamento di sistemi di IA, come riflesso coerentemente nel **nuovo testo dell'art. 2(7) AIA.**

ISSN 2239-8570

Il primo paragrafo del nuovo art. 4 bis AIA innanzitutto ammette un simile trattamento – in continuità con quanto già previsto dalla disposizione dell'abrogato paragrafo 5 dell'art. 10 AIA - per consentire ai **fornitori di sistemi di IA ad alto rischio** di trattare «eccezionalmente» categorie particolari di dati personali quando ciò sia «strettamente necessario» per assicurare la rimozione di *bias* dai *dataset* di addestramento e/o funzionamento dei sistemi: «nella misura strettamente necessaria a garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio in conformità dell'articolo 10, paragrafo 2, lettere f) e g)». Tale facoltà è subordinata a una serie di condizioni, previste nel paragrafo 1 dell'art. 4 bis, tra cui l'impossibilità di conseguire il medesimo risultato mediante dati anonimi o sintetici, l'adozione di adeguate misure tecniche di protezione e di limitazione del riutilizzo dei dati, comprese la pseudonimizzazione e le misure di sicurezza, l'assenza di comunicazione o accesso ai dati da parte di terzi e la puntuale motivazione della stretta necessità del trattamento nel registro del titolare.

In aggiunta a ciò, e questa è la novità sostanziale introdotta dalla Riforma, **i fornitori e *deployer* di sistemi e modelli di IA non ad alto rischio («altri sistemi e modelli di IA») nonché i *deployer* dei sistemi di IA ad alto rischio**, possono eccezionalmente trattare categorie particolari di dati personali qualora ciò sia strettamente necessario per individuare ed eliminare *bias* («distorsioni») suscettibili di incidere sulla salute, sulla sicurezza o sui diritti fondamentali delle persone ovvero di determinare esiti discriminatori ai sensi del diritto dell'Unione, «specie laddove gli output di dati influenzano gli input per operazioni future», purché siano rispettate tutte le citate garanzie previste dal paragrafo 1. Il paragrafo 2 dell'art. 4 bis AIA specifica che **le disposizioni del medesimo paragrafo 2 non introducono alcun obbligo di effettuare tali trattamenti**. La specificazione è limitata alla previsione del secondo paragrafo (trattamenti da parte di fornitori e deployer relativi a sistemi non ad alto rischio, trattamenti dei deployer relativi a sistemi ad alto rischio) e non anche alla previsione del primo paragrafo, posto che per quest'ultima, come chiarito dal **cons. 9 del Regolamento** il relativo trattamento ha una base giuridica legata all'obbligo dei fornitori di sistemi ad alto rischio di stabilire pratiche relative al rilevamento, alla prevenzione e alla correzione delle distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione.

Il Regolamento modifica altresì il Capo II dell'AI Act introducendo attraverso le **nuove lettere b bis) e b ter) del paragrafo 1 dell'art. 5 AIA, nuovi divieti di immissione sul mercato, messa in servizio e uso di sistemi di IA destinati alla creazione di materiale pedopornografico ovvero di immagini sessualmente esplicite riferite a una persona identificabile senza il suo consenso libero, specifico, informato ed esplicito**, rafforzando così le tutele poste a presidio della dignità umana (art. 1, punto 7) del Regolamento).

Il **nuovo paragrafo 1 bis dell'art. 5 AIA** circoscrive tali divieti, mentre il **nuovo paragrafo 1 ter dell'art. 5 AIA** specifica il concetto di manipolazione di cui alla lettera b bis) dell'art. 5(1) AIA.

ISSN 2239-8570

Il Regolamento introduce altresì alcuni **nuovi paragrafi dell'art. 6 AIA** ai fini della qualificazione dei sistemi di IA come componenti di sicurezza dei prodotti e ai fini della disposizione di cui all'art. 6(1)(b) AIA. Si tratta, rispettivamente dei **nuovi paragrafi 1 bis**, **1 ter e 1 quater dell'art. 6 AIA**.
Un'importante modifica riguarda i sistemi di IA che ai sensi dell'**art. 6(4) AIA** sono **considerati non ad alto rischio dal fornitore** e per i quali ai sensi di quell'articolo il fornitore documenta la relativa valutazione, mettendola a disposizione delle autorità nazionali competenti su richiesta, ed è tenuto all'obbligo di registrazione ai sensi dell'art. 49(2) AIA, dovendo fornire in sede di registrazione e poi tenere aggiornate alcune informazioni elencate nella **sezione B dell'allegato VIII dell'AIA**. La Riforma non ha modificato né l'art. 6(4) AIA né l'art. 49(2) AIA ma **ha espunto dall'elenco delle informazioni** di cui alla sezione B dell'allegato VIII dell'AI Act quelle di cui ai punti 7 e 9 del medesimo allegato, ossia il breve riassunto dei **motivi posti alla base della valutazione del fornitore** per i quali questi considera non a rischio il sistema di IA (in particolare, in applicazione dell'art. 6(3) AIA), e l'indicazione degli **Stati membri** nei quali il sistema di IA è stato immesso sul mercato, messo in servizio o messo a disposizione. La *ratio* di questo intervento è dichiarata nel **cons. 22** del Regolamento.
Relativamente alla procedura di notifica di cui all'**art. 30 AIA** e all'attività e agli adempimenti degli organismi di valutazione della conformità ivi previsti, ed in particolare per consentire di specificare l'ambito di applicazione della designazione degli organismi di valutazione, il Regolamento ha introdotto un **nuovo allegato all'AI Act, l'allegato XIV** intitolato «Elenco dei codici, delle categorie e dei corrispondenti tipi di sistemi di IA ai fini della procedura di notifica di cui all'articolo 30, che specifica l'ambito di applicazione della designazione degli organismi notificati». La *ratio* dell'introduzione dell'allegato XIV è dichiarata estensivamente nel **cons. 43 del Regolamento**, dove si trova una spiegazione dei diversi tipi di **«codici AIP»** per i sistemi di IA disciplinati dalla normativa sui prodotti di cui all'allegato I all'AI Act, **«codici AIB»** per i sistemi di IA biometrici di cui al primo punto dell'allegato III all'AI Act, e **«codici AIH»** riguardano i tipi e le tecnologie alla base dei sistemi di IA e sono definiti come **«codici orizzontali»** per i sistemi di IA perché possono essere utilizzati in combinazione con i codici AIP e AIB, questi ultimi qualificati, per questa funzione operativa, come **«codici verticali»**.
Con riferimento alle autorità di notifica e al coordinamento con la normativa europea sulla sicurezza dei prodotti, viene introdotta una procedura semplificata in base alla quale gli Stati membri devono garantire che gli organismi di valutazione della conformità che richiedano la designazione sia ai sensi dell'AI Act sia della legislazione armonizzata dell'Unione di cui alla sezione A dell'Allegato I possano avvalersi di **un'unica domanda** e di **un solo procedimento di valutazione**: modifiche agli **artt. 28, 29 e 30 AIA**.
Al paragrafo 2 dell'art. 40 AIA, in materia di **norme armonizzate e prodotti della normazione**, viene aggiunta la seguente disposizione: «Conformemente al regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio [sulla normazione europea] e senza indebito ritardo, la Commissione chiede alle organizzazioni europee di normazione di elaborare

ISSN 2239-8570

prodotti della normazione, comprese, se del caso, norme armonizzate, al fine di agevolare la conformità congiunta e la presunzione di conformità ai requisiti o agli obblighi di cui al capo III, sezioni 2 e 3, del presente regolamento e ai requisiti e agli obblighi pertinenti stabiliti nella normativa di armonizzazione dell'Unione elencata nell'allegato I del presente regolamento».

Si tratta di una **soluzione** che va nella direzione della ricerca di norme tecniche affidanti, ma **meno drastica di quella originariamente prevista dalla Commissione**, che proponeva di condizionare l'applicazione del capo III dell'AI Act alla disponibilità di standard (norme armonizzate) o altri strumenti a sostegno della conformità al medesimo capo III e ad una decisione della Commissione che confermasse tale disponibilità. La Riforma prevede invece una posizione più chiara: le date di applicazione non sono più legate alle norme armonizzate o ad altre misure di sostegno della conformità al capo III, ma avranno decorrenze fisse dal 2 dicembre 2027 per i sistemi *stand alone* classificati ad alto rischio ai sensi dell'art. 6(2) e dell'allegato III AIA, e a partire dal 2 agosto 2028 per i sistemi di IA classificati ad alto rischio ai sensi dell'art. 6(1) AIA relativi a prodotti assoggettati alle discipline di cui all'allegato I dell'AI Act.

L'art. 1, punto 18) del Regolamento chiarisce il coordinamento tra l'AI Act e il regolamento (UE) 2024/2847 (**regolamento sulla ciberresilienza**) quanto ai requisiti di cibersicurezza, disponendo, attraverso l'aggiunta di un paragrafo all'**art. 42 AIA** che, qualora i sistemi ad alto rischio rientrino nell'ambito di applicazione del regolamento sulla ciberresilienza e siano soddisfatte le condizioni di cui all'articolo 12(1) di tale regolamento, tali sistemi sono considerati conformi ai requisiti di cibersicurezza di cui all'articolo 15 AIA.

Viene inoltre chiarito il **coordinamento con la procedura di valutazione della conformità prevista dall'art. 43 AIA**, stabilendo che, qualora un sistema di IA ad alto rischio rientri nella legislazione armonizzata dell'Unione oppure sia classificato ad alto rischio sia ai sensi dell'Allegato I sia dell'Allegato III, la valutazione debba essere svolta tenendo conto delle pertinenti norme di armonizzazione e delle relative procedure.

Nella materia dei c.d. obblighi di trasparenza ai sensi dell'**art. 50 AIA**, la Riforma ha sottratto alla Commissione il compito di approvare con atti di esecuzione **i codici di buone pratiche**, , rimanendo in capo ad essa un ruolo promozionale e di incoraggiamento, e prevedendosi un potere di intervento ex post esercitabile eventualmente nel caso in cui la Commissione, dietro parere dell'ufficio per l'IA ritenga i Codici non adeguati. La modifica investe l'**art. 50(7) AIA** ed è spiegata nel **cons. 41 del Regolamento**.

Sono inoltre introdotte modifiche alla disciplina degli spazi di sperimentazione normativa per l'IA (**sandbox regolatorie** o **sandbox**) **di cui all'art. 57 AIA** dell'AI Act, precisando che ciascuno Stato membro è tenuto a istituire **almeno una sandbox nazionale, operativa entro il 2 agosto 2027**, tramite le proprie autorità competenti o congiuntamente ad altri Stati membri. La disposizione novellata attribuisce altresì al Garante europeo della protezione dei dati (**EDPS**) il potere di istituire una sandbox destinata alle istituzioni e agli organismi dell'Unione e conferisce all'ufficio per l'IA ex art.

ISSN 2239-8570

64 AIA (**AI Office**) la facoltà di creare una sandbox regolatoria a livello europeo per i sistemi di IA rientranti nella propria competenza esclusiva, imponendo contestualmente agli Stati membri di rafforzare la cooperazione transfrontaliera tra le rispettive sandbox.

Con il già citato nuovo **art. 60 bis AIA**, a supporto dell'innovazione, viene estesa la possibilità di sperimentare, anche al di fuori delle sandbox regolatorie, i sistemi di IA ad alto rischio disciplinati dalla sezione B dell'allegato I all'AI Act, al fine di verificarne la conformità agli obblighi previsti dagli artt. 8-15 dell'AI Act.

Il monitoraggio post-commercializzazione sui sistemi di IA continua a fondarsi su un apposito piano. A tal fine, nel novellato **art. 72(3) AIA** è previsto che entro il 2 settembre 2027 la Commissione europea dovrà adottare orientamenti corredati anche da un modello standard (template), destinati a supportare gli operatori economici nell'adempimento dei relativi obblighi.

Il Regolamento, inoltre, con la modifica, fin dal titolo, dell'**art. 75 AIA**, interviene anche sull'architettura istituzionale dell'enforcement, **rafforzando le competenze dell'AI Office in materia di vigilanza su specifiche categorie di sistemi di IA, tra cui quelli basati su modelli di IA per finalità generali realizzati dal medesimo fornitore del sistema** - salvo alcune esclusioni ivi previste- nonché **sui sistemi di IA integrati in piattaforme online molto grandi (VLOPs) e in motori di ricerca di dimensioni molto grandi (VLOSEs)** ai sensi del regolamento (UE) 2022/2065 (**Digital Services Act**): **nuovo art. 75(1) AIA**. La *ratio* dell'attribuzione alla Commissione, attraverso l'AI Office, di questo nuovo potere di vigilanza sui sistemi di IA integrati in VLOPs e VLOSEs è estensivamente dichiarata nel **cons. 32 del Regolamento**.

Il **nuovo art. 75(1 bis) AIA**, prevede che, in deroga all'art. 73 dell'AI Act, i fornitori dei sistemi di IA ad alto rischio sottoposti alla vigilanza dell'AI Office sono tenuti a notificare direttamente a quest'ultimo ogni incidente grave. Numerose nuove disposizioni disciplinano inoltre il **coordinamento tra l'AI Office e le autorità nazionali competenti**, imponendo obblighi di scambio di informazioni e di reciproca assistenza nello svolgimento delle attività ispettive e nell'attuazione delle misure correttive e sanzionatorie previste dall'AI Act e dal **regolamento (UE) 2019/1020 (regolamento sulla vigilanza del mercato e sulla conformità dei prodotti)**.

I nuovi articoli seguenti - **nuovi articoli 75 bis (Poteri di controllo ed esecuzione dell'ufficio per l'IA), 75 ter (Impegni), 75 quater (Non conformità, sanzioni pecuniarie e penalità di mora), 75 quinquies (Garanzie e ulteriori precisazioni)** - rafforzano le competenze dell'AI Office nell'ambito delle attività di valutazione della conformità dei sistemi di IA ad alto rischio soggetti alla propria vigilanza prima dell'immissione sul mercato. La riforma introduce una disciplina dettagliata dei poteri sanzionatori dell'AI Office, prevede le relative procedure e garanzie, richiamando in larga misura il modello previsto dal reg. (UE) 2019/1020 in materia di vigilanza del mercato. Nell'esercizio delle proprie funzioni, l'AI Office dispone delle prerogative riconosciute alle autorità di vigilanza del mercato dall'AI Act e dagli artt. 14(4) e 16(3) del reg. (UE) 2019/1020. Esso può, in particolare, esercitare poteri informativi, ispettivi, di accesso e di

ISSN 2239-8570

indagine, avvalersi di esperti indipendenti, revisori esterni o personale tecnico delle autorità nazionali e ordinare agli operatori economici di consentire l'accesso ai sistemi di IA, fornirne spiegazioni e conservare dati e documenti ritenuti necessari ai fini della verifica del rispetto dell'AI Act. Il nuovo art. 75 quinquies richiama l'art. 18 del reg. (UE) 2019/1020 e riconosce agli operatori diverse **garanzie procedurali nel procedimento sanzionatorio**, quali il diritto di difesa, l'accesso agli atti istruttori, la pubblicazione dei provvedimenti e gli eventuali oscuramenti necessari a tutela della riservatezza. Il nuovo art. 75 ter AIA introduce infine l'istituto degli **impegni vincolanti**, attribuendo efficacia cogente agli impegni assunti dagli operatori e qualificandone espressamente come sanzionabile l'eventuale violazione.

Al fine di assicurare un'applicazione armonizzata dell'AI Act e del diritto dell'Unione, il **nuovo art. 77 AIA** impone alle autorità di vigilanza del mercato di mettere tempestivamente a disposizione delle autorità competenti per la tutela dei diritti fondamentali i documenti e le informazioni relativi ai sistemi di IA oggetto di indagine, nel rispetto delle rispettive competenze e dell'indipendenza istituzionale. Le due autorità sono pertanto chiamate a cooperare strettamente e a prestarsi reciproca assistenza.

All'**art. 111 AIA** è introdotto un **periodo transitorio** che consente ai fornitori di integrare retroattivamente nei propri sistemi di IA generativa le soluzioni tecniche necessarie affinché i contenuti prodotti risultino leggibili dalle macchine e identificabili come generati o manipolati artificialmente. Tali obblighi diverranno pienamente applicabili **dal 2 dicembre 2026**.

Infine, il Regolamento, pur lasciando immodificata la **data generale di applicazione dell'AI Act**, già prevista nell'art. 113, secondo comma - **2 agosto 2026** - e la data di applicazione delle "vecchie norme" dei capi I e II AIA – **2 febbraio 2025** -, modifica parzialmente il terzo comma del medesimo articolo ridefinendo il **calendario dell'entrata in vigore di alcune disposizioni dell'AI Act**:

- dal **2 dicembre 2026** troveranno applicazione le norme concernenti i nuovi divieti dell'art. 5 AIA (paragrafo 1, primo comma, lettere b bis e b ter, e paragrafi 1 bis e 1 ter);
- dal **2 dicembre 2027** per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6(2) e dell'allegato III dell'AI Act
- dal **2 agosto 2028** per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6(1) e dell'allegato I dell'AI Act
- dal **27 luglio 2026** gli articoli da 102 a 110 AIA.

ELISABETTA STRINGHI

Reg. (UE) 2026/1744

2026/2(3)FZ

Lo schema di d.lgs. n. 421 di adeguamento della normativa italiana all'AI Act approvato il 9.6.2026 in materia di poteri delle autorità nazionali e

ISSN 2239-8570

di utilizzo dell'intelligenza artificiale nella formazione. In particolare: le disposizioni sulla formazione

Il 10 giugno 2026, il Consiglio dei ministri ha approvato due schemi di decreto legislativo – con nn. atti di Governo 418 e 421 (di seguito lo **schema** e gli **schemi n. 418 e n. 421**) – volti ad adeguare la normativa nazionale al regolamento (UE) 2024/1689 (**AI Act**), in attuazione delle deleghe contenute nella l. n. 132/2025, recante «Disposizioni e deleghe al Governo in materia di intelligenza artificiale» (sull'AI Act v. in questa Rubrica il contributo n. 2 del numero 2/2024 [2024/2(2)SO], in *PeM* 2024, p. 650; sulla legge 132/2025 v. in questa Rubrica il contributo n. 1 nel numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016).

I testi dovranno ora essere sottoposti al vaglio delle Commissioni parlamentari, della Conferenza delle Regioni e delle *Authorities* competenti entro il 10 ottobre 2026, termine previsto dall'art. 24 della medesima legge.

In questo contributo e in quelli successivi da 4 a 7 riassumeremo i contenuti essenziali dello schema n. 421, mentre nei contributi da 8 a 10 riporteremo i contenuti principali dello schema n. 418.

Lo schema n. 421 disciplina i poteri delle autorità nazionali, la formazione in materia di intelligenza artificiale, ma anche altre materie non recate dal titolo, in particolare contenendo disposizioni di diritto di lavoro e sull'amministrazione della giustizia (su cui v. *amplius* i contributi seguenti in questo numero di questa Rubrica).

Dopo un **capo I** di carattere definitorio, il **capo II** individua i poteri delle autorità nazionali competenti nell'**Agenzia per l'Italia digitale** (**AgID**), con compiti di notifica, e dell'**Agenzia per la cybersicurezza nazionale** (**ACN**), quale autorità di vigilanza del mercato e solo punto di contatto con le istituzioni europee.

Sono inoltre previste competenze settoriali in capo alla **Banca d'Italia**, alla **CONSOB** e all'**IVASS** per i sistemi ad alto rischio usati dagli intermediari finanziari, nonché al **Garante per la protezione dei dati personali** per i sistemi impiegati in materia di contrasto ai reati, gestione delle frontiere, giustizia e democrazia.

Il capo III è dedicato alla formazione e prevede in percorsi di vera e propria alfabetizzazione sull'intelligenza artificiale rivolti a studenti, docenti, professionisti, pubbliche amministrazioni e magistrati.

In **ambito scolastico** sono previste, tra l'altro, l'integrazione nei **programmi** scolastici del secondo ciclo di studi delle tecnologie avanzate e IA generativa, l'inserimento dell'IA nell'insegnamento dell'educazione civica, il rafforzamento delle **competenze STEAM** (scienza, tecnologia, ingegneria, arte e matematica) e una **formazione stabile del personale** docente sui rischi, sui limiti, sulla tutela dei dati e sull'uso responsabile dei sistemi.

Ad accompagnare questa sperimentazione didattica sono previsti **comitati** tecnico-etici territoriali, organizzati in rete, pensati anche per contribuire all'aggiornamento dei regolamenti di istituto in modo rendere l'uso dell'IA sicuro e verificabile.

ISSN 2239-8570

È inoltre previsto uno **stanziamento** di 100 milioni di euro per un piano di formazione dei docenti volto a rafforzare il ruolo della scuola nella **prevenzione dei rischi digitali, delle dipendenze, dell'opacità algoritmica e delle forme di condizionamento dei minori, anche con il coinvolgimento delle famiglie**.
Anche **Università e istituzioni AFAM** dovranno integrare **attività formative sull'utilizzo sicuro e consapevole dei sistemi di IA**, secondo un approccio interdisciplinare e laboratoriale, volto a garantire la comprensione tecnica, giuridica e critica delle nuove tecnologie.
Per le **professioni**, lo schema introduce l'alfabetizzazione sull'IA nella formazione iniziale e continua, ribadendo che la responsabilità dell'attività svolta resta in capo al professionista e non si trasferisce allo strumento tecnologico.
Quanto alle **pubbliche amministrazioni**, il testo promuove l'**introduzione di sistemi di IA** nelle politiche di reclutamento, formazione e innovazione organizzativa, con l'obiettivo di **semplificare l'azione amministrativa e accelerare i procedimenti**. In questa cornice, il **Ministro per la Pubblica amministrazione** assume funzioni di indirizzo e coordinamento, anche al fine di evitare un'adozione frammentata o disomogenea dell'IA tra amministrazioni.
Particolare rilievo è attribuito alla **formazione dei dipendenti pubblici**, che devono essere messi nelle condizioni di comprendere il funzionamento dei sistemi, interpretarne correttamente gli output, riconoscerne limiti, errori e possibili bias, proteggere dati e sicurezza, e garantire una sorveglianza umana effettiva.
Per i **magistrati**, lo schema di d.lgs affida alla **Scuola superiore della magistratura** il compito di promuovere **percorsi formativi sui profili tecnici** dei sistemi di IA utilizzati nell'attività giudiziaria, sulla **disciplina giuridica** dell'intelligenza artificiale e sull'impatto di tali sistemi sull'**organizzazione giudiziaria** e sui **diritti delle persone**.
Invece, per la **formazione del personale di polizia**, la disciplina è contenuta nell'altro schema di decreto legislativo, lo schema n. 418 (art. 6), al cui contributo si rimanda (v. in questa Rubrica contributo n. 9, *infra* [2026/2(9)NA]).

FRANCESCA ZAMPONE

Comunicato stampa
Schema di decreto legislativo

2026/2(4)ME
(*segue)* Le disposizioni sulle autorità nazionali

Per quanto riguarda le disposizioni sulle autorità nazionali, lo schema di decreto legislativo n. 421 approvato il 9 giugno 2026 (di seguito **schema n. 421** o anche solo lo **schema**) (sul quale v. in generale *supra*, il contributo che precede) attua la delega conferita al Governo dalla legge 23 settembre 2025,

ISSN 2239-8570

n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale (sulla legge 132/2025 v. in questa Rubrica il contributo n. 1 del numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016) con particolare riguardo agli artt. 20 (Autorità nazionali per l'intelligenza artificiale) e 24 (Deleghe al Governo in materia di intelligenza artificiale). Sul piano sovranazionale, l'atto adegua l'ordinamento interno all'art. 70 del regolamento (UE) 2024/1689 (**AI Act**), che richiede a ciascuno Stato membro la designazione delle autorità nazionali competenti e di un punto di contatto unico (sull'AI Act v. in questa Rubrica il contributo n. 2 del numero 2/2024 [2024/2(2)SO], in *PeM* 2024, p. 650).

Lo schema n. 421 muove dalla designazione già operata dall'art. 20 della l. 132/2025 e ne definisce i poteri in coerenza con il regolamento europeo. La ripartizione delle funzioni tra le autorità è la seguente:

1) **l'Agenzia per l'Italia Digitale (AgID) è autorità di notifica**, cui competono le procedure di valutazione, designazione e notifica degli organismi di valutazione della conformità, nonché il relativo monitoraggio;
2) **l'Agenzia per la Cybersicurezza Nazionale (ACN) è autorità di vigilanza del mercato ed è designata punto di contatto unico** con le istituzioni dell'Unione europea;
3) la **Banca d'Italia**, la Commissione Nazionale per le Società e la Borsa (**CONSOB**) e l'Istituto per la Vigilanza sulle Assicurazioni (**IVASS**) **esercitano la vigilanza, nei rispettivi ambiti di competenza**, sui sistemi di IA ad alto rischio impiegati dagli intermediari finanziari;
4) il **Garante per la protezione dei dati personali** interviene, per i profili di propria competenza, sui sistemi di IA ad alto rischio utilizzati nei settori del contrasto, delle frontiere, della giustizia e della democrazia.

Resta fermo il raccordo tra le due Agenzie e le altre autorità e amministrazioni interessate, secondo i meccanismi di coordinamento previsti dall'art. 20 della l. 132/2025. Più in particolare, il testo prevede forme di **coordinamento e cooperazione tra le autorità**, da attuarsi tramite **accordi e protocolli d'intesa**, e prevede la trasmissione di una **relazione annuale** alla Presidenza del Consiglio, per il tramite del **Comitato di coordinamento istituito presso il Dipartimento per la trasformazione digitale**.

Il comunicato precisa che lo schema si mantiene aderente alle disposizioni dell'AI Act, senza introdurre discipline alternative rispetto al quadro europeo. Trattandosi di esame preliminare, il testo non è definitivo. Lo schema sarà ora trasmesso alle Commissioni parlamentari competenti, alla Conferenza delle Regioni e alle Autorità interessate per i prescritti pareri; all'esito, il Consiglio dei Ministri procederà all'approvazione definitiva, cui seguirà la pubblicazione in Gazzetta Ufficiale. Con la definizione dei poteri delle autorità nazionali l'Italia dà seguito a uno degli adempimenti richiesti agli Stati membri in vista della piena applicazione dell'AI Act.

MICHELE EMPLER

Schema di decreto legislativo

ISSN 2239-8570

2026/2(5)EF
(segue) Le disposizioni sul diritto del lavoro

Lo schema di decreto legislativo n. 421 approvato il 9 giugno 2026 (di seguito anche solo lo **schema**) (sul quale v. in generale *supra*, il contributo n. 3) prevede all'articolo 40 alcune disposizioni intese a tutelare il lavoratore nei processi decisionali assistiti da intelligenza artificiale, e si compone di quattro commi, come segue.

«1. Fermo restando quanto previsto dall'art. 22 del regolamento (UE) 2016/679 [**GDPR**], nei processi decisionali concernenti il rapporto di lavoro, il datore di lavoro che si avvale di sistemi di intelligenza artificiale, quali definiti dall'art. 3, punto 1) del [regolamento (UE) 2024/1689 (**AI Act)**], assicura che le decisioni relative alla costituzione, alla modificazione o alla risoluzione del rapporto, ivi compresi i provvedimenti disciplinari, non siano adottate unicamente sulla base di un trattamento automatizzato, in conformità all'articolo 11 della [legge 23 settembre 2025, n. 132]. La decisione definitiva è in ogni caso riservata a una persona fisica, che eserciti un potere effettivo e autonomo.

2. L'utilizzo dei sistemi di cui al comma 1 avviene nel rispetto della dignità e della riservatezza del lavoratore e del principio di non discriminazione.

3. Prima dell'avvio del trattamento, il datore di lavoro assolve agli obblighi di informativa previsti dall'articolo 1-bis del decreto legislativo 26 maggio 1997, n. 152. Il lavoratore ha diritto di ottenere, a richiesta e mediante l'intervento di una persona fisica, una motivazione intelligibile della decisione che lo riguarda, comprensiva dell'indicazione dell'eventuale incidenza dei sistemi di intelligenza artificiale sul processo decisionale e dei principali parametri considerati. Restano fermi il diritto di accesso ai dati raccolti e i diritti riconosciuti dagli articoli 13, 15 e 22 del regolamento (UE) 2016/679.

4. Il licenziamento intimato in violazione del comma 1 è nullo».

L'utilizzo dell'avverbio **«unicamente»** nel primo comma richiama quanto stabilito dall'art. 22 GDPR, che già vieta le decisioni basate unicamente su trattamento automatizzato produttive di effetti giuridici significativi, in ordine al quale il dibattito europeo ha da tempo segnalato un limite strutturale della disposizione perché espone al rischio della cosiddetta *automation bias*.

È infatti sufficiente che la decisione algoritmica venga sottoposta a una ratifica formale da parte di una persona fisica — anche quando tale intervento umano si risolva in una firma apposta senza un effettivo riesame dei presupposti — perché la fattispecie non sia più qualificabile come decisione "esclusivamente" automatizzata, con conseguente uscita dal perimetro di applicazione della tutela.

Lo schema di decreto, nonostante l'utilizzo dell'avverbio in questione, sembra però abbandonare l'impostazione dell'art. 22 GDPR attraverso l'introduzione di un correttivo che richiede un effettivo intervento umano. La disposizione prevede infatti che «la decisione definitiva è in ogni caso riservata a una persona fisica **che eserciti un potere effettivo e autonomo**».

ISSN 2239-8570

In altri termini, l'algoritmo può concorrere a ordinare informazioni, evidenziare profili coerenti con i requisiti richiesti o segnalare criticità, ma la valutazione finale deve restare presidiata da una persona fisica, specie quando la decisione produce effetti concreti sulla vita lavorativa del lavoratore.

Si tratta della trasposizione, in chiave lavoristica, del principio di sorveglianza umana che l'AI Act pone quale requisito di progettazione e obbligo per i deployer dei sistemi ad alto rischio – cfr. artt. 14, 26(2) AI Act - e che nel contesto italiano si collega al divieto, come già rilevato, presente nell'ordinamento in materia di protezione dei dati personali, di sottoporre la persona a decisioni basate unicamente su un trattamento automatizzato che producano effetti giuridici che la riguardano o che incidano in modo analogo significativamente sulla sua persona.

Resta però, sul piano applicativo, la difficoltà di stabilire **quando la decisione umana sia sostanziale e quando solo apparente**.

Ed infatti, la qualificazione della decisione come «umana», verificabile solo *ex post* e in sede contenziosa, potrebbe porre significative **difficoltà probatorie a carico del lavoratore**, il quale, salvo prova contraria che dovrà spesso fondarsi su presunzioni, non dispone di strumenti agevoli per dimostrare che la firma del soggetto umano ha semplicemente ratificato un esito predeterminato dal sistema.

Peraltro, l'accesso del lavoratore ai parametri e ai criteri computazionali del sistema di IA utilizzato, necessario sia per verificare l'effettività dell'intervento umano, che per comprendere la **motivazione della decisione** ai sensi del comma 3 dell'art. 40 dello schema, potrebbe risultare limitato dalla qualificazione di tali elementi come segreto commerciale ai sensi dell'articolo 49 dello schema, con un possibile pregiudizio per l'effettività processuale della tutela riconosciuta dal predetto articolo 40.

L'art. 49 dello schema di decreto prevede infatti l'introduzione nel codice della proprietà industriale (art. 98, decreto legislativo n. 30 del 2005) di un nuovo comma 1 bis, qualificando come informazioni aziendali riservate — e dunque, ricorrendone i presupposti, come segreti commerciali — i dati, gli algoritmi e i metodi matematici per l'addestramento dei sistemi di intelligenza artificiale, comprese le architetture dei modelli, e le funzioni di ottimizzazione (v. *amplius infra* il contributo n. 7 in questo numero della Rubrica).

La qualificazione di segreto commerciale potrebbe, sul piano applicativo, incidere sulla possibilità per il lavoratore di comprendere, quantomeno nei suoi tratti essenziali, il funzionamento dei parametri che hanno concorso alla decisione, specie ove il datore di lavoro non sia il titolare originario del sistema ma un semplice licenziatario o utilizzatore di una soluzione fornita da terzi.

Né lo schema di decreto prevede alcunché in ordine ai profili procedurali e probatori e pertanto, in assenza di modifiche prima dell'approvazione definitiva del testo, tale accertamento resterà, probabilmente affidato alla giurisprudenza, chiamata a valorizzare, caso per caso, indici quali, ad esempio, la effettiva conoscibilità dei parametri computazionali da parte del decisore umano, il tempo dedicato alla valutazione, le modalità utilizzate e la possibilità di discostarsi dall'output del sistema.

ISSN 2239-8570

L'art. 40 dello schema, oltre a prevedere, nel comma 2, che l'utilizzo dei sistemi di intelligenza artificiale «avviene nel rispetto della dignità e della riservatezza del lavoratore e del principio di non discriminazione», nel comma successivo, ribadendo quanto previsto dall'art. 11 della legge 132/2025, rinvia agli obblighi informativi previsti dall'**art. 1 bis del d.lgs. 26 maggio 1997, n. 152** (introdotto in materia di sistemi decisionali e di monitoraggio automatizzati dal d.lgs. n. 104/2022, di recepimento della direttiva UE 2019/1152 relativa a condizioni di lavoro trasparenti e prevedibili) il cui comma 8 statuisce la non applicabilità degli obblighi informativi previsti dal medesimo articolo «ai sistemi protetti da segreto industriale e commerciale».
Inoltre, come detto, il comma 3 dell'art. 40 dello schema stabilisce che «il lavoratore ha diritto di ottenere, a richiesta e mediante l'intervento di una persona fisica, una motivazione intelligibile della decisione che lo riguarda, comprensiva dell'indicazione dell'eventuale incidenza dei sistemi di intelligenza artificiale sul processo decisionale e dei principali parametri considerati», fermi restando il diritto di accesso ai dati e i diritti di cui agli articoli 13, 15 e 22 GDPR.
L'art. 40, comma 4, stabilisce infine che «il licenziamento intimato in violazione del comma 1 è nullo», ovvero l'aver adottato la risoluzione del rapporto di lavoro unicamente sulla base di un trattamento automatizzato, senza che la decisione finale sia stata riservata a una persona fisica dotata di un potere effettivo e autonomo.
La formulazione testuale della disposizione appare chiara nel prevedere la **sanzione della nullità per il solo licenziamento**, sebbene il comma 1 riferisca il divieto di decisione integralmente automatizzata a un più ampio novero di decisioni datoriali tra cui anche la costituzione, la modificazione del rapporto e i provvedimenti disciplinari.
Ne deriva che, allo stato del testo, la illegittimità di una decisione di assunzione o un provvedimento disciplinare diverso dal licenziamento, anche se assunti in violazione del comma 1, dovrà essere fatta valere secondo gli ordinari rimedi previsti dall'ordinamento.
Allo stesso modo, **la violazione dell'obbligo di motivazione intelligibile prevista dal comma 3 della disposizione è un inadempimento azionabile in via ordinaria**, ad esempio ai fini risarcitori o come elemento di prova dell'illegittimità della decisione sottostante.
L'ipotesi della nullità del licenziamento prevista dall'art. 40, comma 4 dello schema, si aggiunge, ovviamente, come **autonoma e nuova causa di nullità al catalogo già esistente nell'ordinamento lavoristico** (nullità per motivo illecito determinante, per motivo discriminatorio, per motivo ritorsivo, etc) e alla disciplina generale di tutela in caso di licenziamento illegittimo, **con conseguente applicazione della tutela reale piena, prevista** dall'articolo 18, comma 1, dello Statuto dei lavoratori (come riformulato dalla legge n. 92 del 2012) **per il licenziamento** discriminatorio o «**riconducibile agli altri casi di nullità espressamente previsti dalla legge**», e dall'articolo 2, comma 1, del decreto legislativo n. 23 del 2015 (c.d. tutele crescenti, applicabile ai lavoratori assunti dopo il 7 marzo 2015), che utilizza una formula sostanzialmente analoga.

ISSN 2239-8570

EMANUELA FIATA

Schema di decreto legislativo

2026/2(6)LP
(segue) Le disposizioni sull'equo compenso ai sensi della legge professionale

L'art. 46 dello schema di decreto legislativo n. 421 approvato il 9 giugno 2026 (di seguito anche solo lo **schema**) (sul quale v. in generale *supra*, il contributo n. 3) introduce alcune norme in materia di equo compenso, attuando una delle deleghe conferite dalla legge 23 settembre 2025, n. 132 (sulla quale v. in questa Rubrica il contributo n. 1 del numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016].

In particolare, **l'art. 24(2)(f) della legge 132/2025** aveva specificato che, nell'adottare i decreti di adeguamento della normativa nazionale al regolamento (UE) 2024/1689 (**AI Act**), **il Governo potesse prevedere una modulazione dell'equo compenso del professionista «sulla base delle responsabilità e dei rischi connessi all'uso dei sistemi di intelligenza artificiale»**.

Va premesso che, ai sensi della legge 21 aprile 2023, n. 49 (Disposizioni in materia di equo compenso delle prestazioni professionali), la quale viene espressamente richiamata dall'art. 46(1) dello schema, **per "equo compenso" si intende un compenso proporzionato alla quantità e alla qualità del lavoro svolto, al contenuto e alle caratteristiche della prestazione professionale, nonché conforme ai compensi previsti dai decreti ministeriali per talune categorie professionali che offrono prestazioni intellettuali (avvocati, professionisti iscritti agli ordini e ai collegi, e professionisti non organizzati in ordini e collegi)**.

L'art. 46 dello schema si articola in due commi.

Il primo comma stabilisce che, qualora il professionista utilizzi sistemi di intelligenza artificiale, ciò potrà comportare una modulazione dell'equo compenso ai sensi della legge 21 aprile 2023, n. 49, «secondo parametri che tengono conto della classificazione di rischio del sistema di intelligenza artificiale utilizzato». La norma esclude pertanto qualsivoglia automatismo, limitandosi a indicare il parametro di riferimento per operare, eventualmente, una simile modulazione: la classe di rischio del sistema utilizzato, secondo la classificazione prevista dall'AI Act.

La lettera del primo comma, del pari, non specifica se una simile modulazione possa tradursi in un aumento o in una diminuzione del compenso del professionista. Tuttavia, nella **relazione illustrativa** che accompagna lo schema di decreto, si specifica che ancorare la modulazione alla classe di rischio del sistema «riflette la considerazione che l'impiego di sistemi a rischio più elevato richiede al professionista competenze aggiuntive, attività di verifica e sorveglianza più onerose e una maggiore assunzione di responsabilità, che giustificano un adeguamento del compenso». **La**

ISSN 2239-8570

modulazione sembra pertanto orientata in senso incrementale, in ragione del binomio "rischio-responsabilità" già individuato nella delega di cui all'art. 24(2)(f) legge132/2025.
Tale interpretazione risulta inoltre coerente con la collocazione della norma, inserita nel Capo III dello schema di decreto ("intelligenza artificiale per i percorsi formativi, le professioni, il lavoro, la sanità e la pubblica amministrazione") e immediatamente dopo l'art. 45, relativo alla formazione dei professionisti in materia di intelligenza artificiale.
L'art. 46(1) individua dunque un criterio su cui basare la modulazione dell'equo compenso – la classe di rischio del dispositivo di IA –, senza però definire come debba essere applicato, né quali altri elementi possano venire in rilievo e quale sia il peso da attribuirvi.
La questione viene affrontata dal **comma 2** dell'art. 46, che **rimette integralmente la determinazione dei parametri concreti su cui basare la modulazione del compenso** del professionista che usi un sistema di IA **ai decreti ministeriali che definiscono i parametri per la liquidazione dei compensi professionali**.
Difatti, il comma 2 dell'art. 46 stabilisce che, entro dodici mesi dalla data di entrata in vigore del decreto legislativo, tali decreti debbano venire integrati mediante l'indicazione dei parametri utili alla modulazione dell'equo compenso, creando quindi una nuova delega.
Nello specifico, i decreti da integrare in base alla delega prevista dall'art. 46, comma 2, sono i decreti adottati ai sensi dell'articolo 9 del decreto-legge 24 gennaio 2012, n. 1 (parametri generali per le professioni regolamentate in ordini o collegi), il decreto di cui all'articolo 13, comma 6, della legge 31 dicembre 2012, n. 247 (parametri forensi) nonché i decreti adottati ai sensi dell'articolo 1, comma 1, lettera c), della legge 21 aprile 2023, n. 49, concernente le professioni non organizzate in ordini o collegi.

LAURA PIVA

Schema di decreto legislativo

2026/2(7)LF
(segue) Le disposizioni sulla modifica del codice di proprietà industriale in materia di informazioni aziendali e sulla competenza delle sezioni specializzate in materia di impresa

Gli articoli 49 e 50 dello schema di decreto legislativo n. 421 approvato il 9.6.2026 (di seguito anche solo lo **schema**) (sul quale v. in generale *supra*, il contributo n. 3) intervengono, rispettivamente, sulla disciplina dei segreti commerciali e sulla competenza delle sezioni specializzate in materia di impresa. Le due disposizioni perseguono un obiettivo di coordinamento tra il quadro regolatorio europeo dell'intelligenza artificiale e la disciplina nazionale dei segreti commerciali.
L'art. 49 dello schema **modifica l'art. 98 del codice della proprietà industriale** (d.lgs. 10 febbraio 2005, n. 30, di seguito anche c.p.i.) mediante

ISSN 2239-8570

l'introduzione di un **nuovo comma 1 bis**, **che ricomprende espressamente tra le informazioni aziendali e le esperienze tecnico-industriali anche i dati, gli algoritmi e i metodi matematici impiegati nell'addestramento dei sistemi di intelligenza artificiale, precisando che per tali ultimi devono intendersi «le architetture dei modelli, le funzioni di ottimizzazione, le procedure e le configurazioni di addestramento, nonché ogni altro elemento tecnico-computazionale funzionale allo sviluppo dei sistemi di IA»**.

La disposizione subordina anche tali componenti informative alla **ricorrenza dei requisiti già previsti dal comma 1: la segretezza dell'informazione, il valore economico derivante dalla sua riservatezza e l'adozione di misure ragionevolmente adeguate a mantenerla segreta**.

La modifica si innesta sulla disciplina dei segreti commerciali introdotta dal d.lgs. n. 63/2018, attuativo della **direttiva (UE) 2016/943**, che ha armonizzato a livello europeo la tutela del **know-how riservato** e delle **informazioni commerciali riservate** contro l'acquisizione, l'utilizzo e la divulgazione illeciti. La direttiva muove dal presupposto che la tutela dei segreti commerciali abbia ad oggetto la protezione di informazioni che, in quanto segrete, economicamente rilevanti e adeguatamente protette, conferiscono al loro legittimo detentore un **vantaggio competitivo**.

In tale prospettiva, la disciplina dei segreti commerciali assume un ruolo centrale nella tutela del patrimonio informativo dell'impresa, **consentendo di proteggere algoritmi non brevettati o non brevettabili, dataset non generalmente accessibili, modelli di machine learning, tecniche di addestramento, processi produttivi, metodi organizzativi e know-how operativo che, pur non beneficiando della tutela brevettuale o autoriale, rappresentano un essenziale fattore di innovazione e di vantaggio competitivo**.

L'espresso riferimento ai dati, agli algoritmi e ai metodi matematici non introduce, peraltro, una nuova categoria di beni immateriali, ma chiarisce che anche gli elementi impiegati nello sviluppo e nell'addestramento dei sistemi di intelligenza artificiale possono essere ricondotti nell'ambito delle informazioni aziendali tutelate dal codice della proprietà industriale. In tale prospettiva, assume particolare rilievo il requisito del **valore economico dell'informazione**, che non coincide con un autonomo valore patrimoniale del bene, bensì con il vantaggio concorrenziale che il legittimo detentore consegue proprio in ragione della sua segretezza, riconducibile agli asset immateriali di cui al nuovo comma 1 bis dell'art. 98 del codice della proprietà industriale, previsto dallo schema di decreto in commento. Il patrimonio conoscitivo dell'impresa costituisce, infatti, un fattore competitivo il cui valore risiede nella possibilità di conservarne l'esclusiva disponibilità; la divulgazione delle informazioni comporterebbe, per converso, la perdita di tale vantaggio competitivo.

L'intervento attua il quadro delineato dal regolamento (UE) 2024/1689 (**AI Act** o **AIA**), che, accanto agli obblighi di trasparenza e documentazione gravanti sui fornitori di modelli di IA per finalità generali, riconosce l'esigenza di salvaguardare le informazioni commerciali riservate e i segreti commerciali. In particolare, l'**art. 53 AI Act** impone ai fornitori di predisporre

ISSN 2239-8570

e mantenere aggiornata la documentazione tecnica del modello (art. 53(1)(a) AIA), di mettere a disposizione le informazioni necessarie ai fornitori di sistemi che intendano integrarlo (art. 53(1)(b) AIA) e di pubblicare una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento (art. 53(1)(d) AIA). Tali obblighi rispondono alle esigenze di tracciabilità e spiegabilità dei sistemi di IA, esplicitate dal **cons. 27 dell'AI Act** a proposito del principio della trasparenza, e devono, tuttavia, essere adempiuti nel rispetto dei diritti di proprietà intellettuale, delle informazioni commerciali riservate e dei segreti commerciali.

Il medesimo equilibrio emerge dall'**art. 78 AIA**, rubricato «Riservatezza», il quale impone alla Commissione, alle autorità di vigilanza del mercato, agli organismi notificati e agli altri soggetti coinvolti nell'applicazione del regolamento di garantire la riservatezza delle informazioni e dei dati acquisiti nello svolgimento delle rispettive funzioni, tutelando, in particolare, i diritti di proprietà intellettuale, le informazioni commerciali riservate, i segreti commerciali e il codice sorgente. Nella stessa direzione si collocano i **cons. 107 e 167 dell'AI Act**, che ribadiscono come gli obblighi di trasparenza previsti dall'AI Act debbano essere attuati senza compromettere la protezione del patrimonio informativo delle imprese.

In tale contesto, la modifica dell'art. 98 del codice della proprietà industriale chiarisce che anche gli elementi informativi impiegati per l'addestramento dell'intelligenza artificiale possono beneficiare della tutela riconosciuta alle informazioni aziendali riservate, **purché ricorrano i requisiti richiesti dalla disciplina generale**. La novella si inserisce così nel più ampio processo di **coordinamento tra il diritto interno e l'AI Act**, assicurando che l'accresciuta circolazione delle informazioni richiesta dal regolamento non pregiudichi la protezione del patrimonio informativo delle imprese.

L'**art. 50 dello schema** interviene sul piano processuale, disponendo che **le controversie relative all'art. 98 c.p.i., come modificato dall'art. 49 dello schema, restino devolute alla competenza delle sezioni specializzate in materia di impresa ai sensi dell'art. 134, comma 1, lett. b), c.p.i.** La disposizione non introduce un nuovo criterio di riparto della competenza tra giudice ordinario e sezione specializzata, ma conferma l'operatività del sistema già delineato dal codice della proprietà industriale, chiarendo che anche le controversie aventi ad oggetto i dati, gli algoritmi e i metodi matematici richiamati dal nuovo comma 1 bis dell'art. 98 c.p.i. rientrano nella cognizione del giudice specializzato. Si tratta, dunque, di una disposizione di coordinamento processuale, funzionale ad assicurare continuità tra l'ampliamento dell'oggetto della tutela operato dall'art. 49 dello schema e il sistema di tutela giurisdizionale già previsto dal codice della proprietà industriale.

LAURA FABIANI

Schema di decreto legislativo

ISSN 2239-8570

2026/2(8)FZ
Lo schema di d.lgs. n. 418 di adeguamento della normativa italiana all'AI Act approvato il 9.6.2026 in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale: inquadramento

Come dianzi detto (v. contributo n. 3 *supra*), il 10 giugno 2026 il Consiglio dei ministri ha approvato con atti di Governo nn. 418 e 421 due schemi di decreti legislativi di adeguamento alle disposizioni del regolamento (UE) 2024/1689 (**AI Act**), il n. 418 «in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia e di responsabilità civile e penale» (lo **schema n. 418** o **lo schema**).
Lo schema n. 418 è stato adottato ai sensi dell'articolo 24, comma 1, comma 2, lett. h), comma 3 e comma 5 della legge 23 settembre 2025, n. 132 , ed è finalizzato all'adeguamento dell'ordinamento nazionale all'AI Act (sull'AI Act v. in questa Rubrica il contributo n. 2 del numero 2/2024 [2024/2(2)SO], in *PeM* 2024, p. 650; sulla legge 132/2025 v. in questa Rubrica il contributo n. 1 del numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016).
Lo schema n. 418 si compone di 22 articoli suddivisi in due titoli.
Il **titolo I** (sul quale v. *amplius* in questa Rubrica il contributo seguente per un esame degli articoli) è dedicato all'utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia. Esso dà attuazione all'articolo 24(2)(h) della legge 132/ 2025, che delega il Governo a prevedere una «apposita disciplina in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia». Secondo la relativa **Relazione illustrativa**, lo schema si colloca nel quadro di adeguamento nazionale all'AI Act e «persegue l'obiettivo di **coniugare l'efficacia dell'azione di prevenzione e contrasto dei reati con la piena tutela dei diritti fondamentali e della protezione dei dati personali**».
Si tratta di un obiettivo dichiarato anche all'art. 3 dello schema, che contiene i principi a dell'uso dell'IA che si vuole vengano realizzati da parte delle Forze di polizia: centralità dell'uomo, logica "*risk-based*", ruolo sussidiario dell'IA, valorizzazione della responsabilità degli operatori, conformità alla normativa sull'IA e sulla *privacy*. In particolare, il comma 1 dell'art. 3 dello schema di decreto n. 418, afferma che l'impiego dell'IA nelle attività di polizia deve essere improntato a un approccio antropocentrico, proporzionato e fondato sulla valutazione del rischio, in coerenza con l'AI Act, e che tenga conto della classificazione dei sistemi (con particolare riguardo a quelli ad alto rischio) e delle diverse categorie di interessati.
Il **titolo II** dello schema n. 418 si compone di due capi, contenenti, rispettivamente, **disposizioni penali sostanziali e processuali** in materia di realizzazione e impiego illeciti di sistemi di IA (**capo I**), e **disposizioni processuali civili in materia di risarcimento** dei danni cagionati dall'utilizzo di tali sistemi (**capo II**). Con queste disposizioni, il Governo intende dare attuazione alla delega di cui all'articolo 24(3) della legge 132/2025, a mente del quale il Governo è delegato ad

ISSN 2239-8570

«adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale», con le modalità e nei limiti previsti dai successivi commi 4 e 5 del medesimo articolo.

FRANCESCA ZAMPONE

Comunicato stampa
Schema di decreto legislativo

2026/2(9)NA
(segue) Le disposizioni sull'attività di polizia e le disposizioni penali sostanziali e processuali

Come illustrato nel contributo che precede in questa Rubrica ([2026/2(8)FZ]), con lo schema di decreto legislativo approvato il 9.6.2026, atto di governo n. 418 (lo **schema n. 418** o **lo schema**), in attuazione delle deleghe contenute nell' art. 24(2)(h) e nell'art. 24(3), quest'ultima come specificata dalle disposizioni dell'art. 24(5) della legge 23 settembre 2025, n. 132 (sulla legge 132/2025 v. in questa Rubrica il contributo n. 1 del numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016), il Governo ha affrontato lo spinoso problema della protezione dagli illeciti nella società assistita, e ormai pervasa, dall'intelligenza artificiale.
Nello schema n. 418, **l'IA viene regolata al contempo come strumento di ausilio e di minaccia:** di ausilio nella prevenzione e nel contrasto dei reati, e di minaccia dei diritti dei consociati da possibili eventi lesivi derivanti dal contatto con questa tecnologia.
L'analisi a prima lettura che segue si limiterà alle disposizioni aventi più diretto rilievo per la giustizia penale, ossia gli artt. 1-15 dello schema n. 418. Seguendo l'ordine dello schema, dopo l'individuazione dell'oggetto di disciplina, la puntualizzazione dei limiti normativi e assiologici all'interno dei quali ci si muove (in sintesi, il rispetto dei diritti fondamentali, dei principi di proporzionalità e non discriminazione, nonché di trasparenza e di sorveglianza umana) e la formulazione delle definizioni necessarie per la comprensione dell'articolato (**titolo I, capo I, artt. 1 e 2**), il legislatore delinea le direttive fondamentali a cui deve essere improntato l'impiego dell'IA nell'attività di polizia (**titolo I, capo II, art. 3**). In buona sintesi, si stabilisce che **l'utilizzo di sistemi di IA debba avvenire in funzione strumentale e di supporto alle forze dell'ordine, e che i risultati delle elaborazioni automatiche debbano essere sottoposti a «revisione umana qualificata», documentata in modo tracciabile, prima di essere impiegati in atti e provvedimenti incidenti sulla sfera giuridica degli interessati**. In tal modo, **si cerca di prevenire deleghe decisionali a favore dei sistemi automatizzati**, imponendo l'obbligo di adoperarli soltanto come strumenti di efficientamento delle attività, garantendo al contempo una supervisione effettiva dei processi produttivi degli output impiegati.
Gli **artt. 4, 5 e 6** dello schema n. 418 completano le misure del capo II. In particolare, si disciplinano le **collaborazioni scientifiche** con «partner» quali

ISSN 2239-8570

università, enti di ricerca e soggetti pubblici o privati (**art. 4**), e si legittimano **spazi di sperimentazione normativa** per il trattamento di dati personali funzionali allo sviluppo di questi sistemi (**art. 5**). Inoltre, si impone la predisposizione di **corsi di formazione specifici per il personale di polizia**, che siano in grado di preparare gli agenti sui principi di funzionamento dell'IA, sui possibili bias, sul riconoscimento biometrico, sull'analisi predittiva, nonché sui profili di responsabilità e cybersicurezza (**art. 6**). Una previsione davvero imprescindibile, soprattutto nell'ottica di fornire competenze adeguate a rendere effettiva la possibilità di sorveglianza umana.
Lo schema passa poi ad occuparsi dell'utilizzo dell'intelligenza artificiale per l'identificazione biometrica dei soggetti rilevanti nell'ambito delle attività di prevenzione e contrasto (**titolo I, capo III: artt. 7-10**).
Il primo degli articoli di questo capo, **l'art. 7, fornisce le basi per l'effettuazione di procedure di «etichettatura, filtraggio e categorizzazione di dati biometrici»**.
A proposito di queste attività o usi «tecnici» dei dati biometrici, in primo luogo, l'art. 7(1) dello schema prevede un coordinamento con la disciplina delle «pratiche di IA vietate» ai sensi del reg. (UE) 2024/1689 (**AI Act** o **AIA**), precisando che **si deve trattare di dati acquisiti lecitamente**, **ai sensi dell'articolo 5(1)(g) ultimo periodo dell'AI Act, per finalità di polizia.**
In secondo luogo, l'art. 7 dispone che tali operazioni non possano essere compiute per inferire caratteristiche sensibili vietate, o per fondare da sole decisioni produttive di effetti giuridici nei confronti delle persone fisiche, prevedendo inoltre a carico del titolare del trattamento l'obbligo di prevenire reimpieghi dei dati per finalità incompatibili con quelle per cui sono stati raccolti.
Più in particolare, l'art. 7(1) dello schema consente gli usi «tecnici» consistenti nell'etichettatura, filtraggio e categorizzazione di dati biometrici, solo quando tali usi:

1. non sono finalizzati a inferire o dedurre le caratteristiche vietate dall'articolo 5(1)(g) primo periodo, dell'AI Act (quali, ad esempio, opinioni politiche, convinzioni religiose o filosofiche, orientamento sessuale);
2. sono funzionali alla comparazione o alla ricerca, ovvero ad altre attività conformi alla normativa vigente, e sono effettuati unicamente per finalità di polizia;
3. non costituiscono l'unico fondamento di decisioni che producano effetti giuridici negativi sulle persone interessate;
4. il titolare del trattamento adotta misure idonee a prevenire il reimpiego dei dati e dei risultati per finalità incompatibili.

Il successivo **art. 8** dello schema contiene disposizioni molto importanti. Esso è inteso a stabilire **in che modo e a quali fini possa essere effettuata la c.d. «identificazione biometrica remota in tempo reale» in conformità con le disposizioni dell'AI Act:** art. 5(1)(h), 5(2), 5(3), 5(4), 5(5) e 5(6) AIA.
Nello specifico, **le disposizioni dell'art. 8 dello schema sono circoscritte a due delle tre categorie di ipotesi eccezionali consentite dall'AI Act**, **ossia alla ricerca mirata di specifiche vittime** di sequestro di persona, tratta o sfruttamento sessuale, nonché di persone scomparse (art. 5(1)(h)(i) AIA), **e**

ISSN 2239-8570

alla prevenzione di minacce specifiche, sostanziali e imminenti per la vita o l'incolumità delle persone ovvero di attacchi terroristici (art. 5(1)(h)(ii) AIA). La terza categoria di ipotesi contemplata dall'art. 5(1)(h)(iii) AIA, concernente la localizzazione o l'identificazione di una persona sospettata di aver commesso uno dei reati elencati nell'allegato II dell'AI Act, è considerata dall'art. 13 dello schema, a proposito dell'introduzione di un nuovo articolo nel codice di procedura penale, l'art. 359 ter c.p.p (v. *infra*).
Nell'ambito considerato dall'art. 8 dello schema, l'identificazione biometrica remota in tempo reale può essere utilizzata **esclusivamente per confermare l'identità di persone specificamente individuate o individuabili, ovvero per la loro ricerca e localizzazione, mediante il confronto con banche dati lecitamente costituite**. Resta **espressamente vietato**, invece, **il ricorso ad archivi alimentati**, foss'anche solo in parte, **con tecniche di scraping non mirato**.
A corredo di queste previsioni, il legislatore delegato ha previsto un articolato sistema di garanzie procedimentali. In effetti, **l'impiego di tale sistema richiede, di regola, una richiesta del questore o del comandante provinciale dell'Arma dei carabinieri e della Guardia di finanza, ovvero dei responsabili dei Servizi centrali** (di cui all'articolo 12 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203) **e l'autorizzazione del procuratore della Repubblica presso il tribunale del capoluogo del distretto competente**, il quale deve delimitare il provvedimento quanto alle finalità perseguite, alla durata, all'ambito territoriale e ai soggetti interessati. L'autorizzazione ha efficacia massima di quindici giorni, prorogabile con provvedimento motivato. **Nei casi di urgenza, è tuttavia consentita l'attivazione immediata del sistema da parte dell'autorità di polizia** (su disposizione del questore, dei comandanti o dei responsabili sopra indicati)**, previa comunicazione anche in forma orale al Procuratore della Repubblica e successiva richiesta di autorizzazione entro ventiquattro ore**; il Procuratore della Repubblica provvede sulla richiesta nelle ventiquattro ore successive. L'inosservanza delle condizioni previste dalla legge, così come il mancato rilascio dell'autorizzazione, determinano l'obbligo di immediata interruzione delle operazioni, l'obbligo di cancellazione dei dati, dei risultati e degli output e l'inutilizzabilità degli elementi acquisiti in violazione delle condizioni previste.
Al fine di rafforzare ulteriormente il quadro delle garanzie, il successivo **art. 9** dello schema **pone quale condizione per l'impiego dei sistemi di identificazione biometrica remota in tempo reale, una previa valutazione d'impatto sui diritti fondamentali ai sensi dell'art. 27 AIA**.
In aggiunta a ciò, **ogni utilizzo deve essere registrato mediante file di log non modificabili**, **conservati per cinque anni e accessibili alle autorità competenti ai fini dei controlli di legittimità e dell'eventuale procedimento penale**.
Lo schema prevede altresì un sistema di **notificazione al Garante per la protezione dei dati personali** (il **Garante**), pur con la possibilità di differirla quando ricorrano esigenze di segretezza investigativa, e demanda a un **successivo decreto ministeriale** (decreto del Ministro dell'interno di

ISSN 2239-8570

concerto con il Ministro della giustizia e sentiti il Garante e le Autorità nazionali per l'IA) **la definizione dei requisiti tecnici minimi** di affidabilità e accuratezza dei sistemi di IA per l'identificazione biometrica in tempo reale, delle soglie operative, delle modalità di monitoraggio dei *bias* e delle misure di sicurezza.

L'art. 10 dello schema n. 418 disciplina invece il **riconoscimento facciale a posteriori mediante sistemi di videosorveglianza integrati con l'intelligenza artificiale per il contrasto di reati**. La disposizione in commento permette l'integrazione di componenti di IA in sistemi di videosorveglianza soltanto nei casi in cui la loro installazione sia consentita da specifiche disposizioni di legge, ricorrano "esigenze di ordine e sicurezza pubblica" e in conformità alla normativa sul trattamento dei dati personali e nel rispetto dell'AI Act. L'art. 10 dello schema distingue l'uso "a posteriori" del riconoscimento facciale da quello in tempo reale, in modo da non configurare un'ipotesi prevista dall'art. 5(1)(h) AI Act, prevedendo limiti temporali, di finalità e di responsabilità. A differenza dei sistemi precedenti, quelli di videosorveglianza integrati con l'IA **possono essere attivati soltanto dopo la commissione di un fatto di reato, anche tentato, e al solo fine di identificare persone già indiziate sulla base di documentazione video-fotografica e di elementi oggettivi e verificabili**.

Il comma 3 dell'art. 10 dello schema n. 418, specifica e prevede tuttavia che, in contesti caratterizzati da particolari esigenze di ordine e sicurezza pubblica, l'installazione di tali sistemi possa comportare il trattamento automatizzato dei dati biometrici delle persone che accedono ai luoghi o agli eventi, con memorizzazione locale in una base dati di riferimento, unitamente, senza far ricorso ad applicazioni biometriche di IA, ai corrispondenti dati anagrafici e, ove previsto, ad esempio nel caso di eventi con posti numerati, dell'identificativo del posto assegnato. **In caso di reato, l'attivazione delle tecnologie di riconoscimento facciale comporta il confronto biometrico a posteriori tra i dati delle persone da identificare (già indiziate) e quelli biometrici e anagrafici (e, se disponibili, ubicativi) presenti nella base dati di riferimento**.

La disposizione prevede, inoltre, specifiche misure in materia di protezione dei dati personali, relative alla conservazione, alla valutazione d'impatto sul livello di protezione, alla registrazione delle operazioni, nonché alla consultazione del Garante, statuendo il divieto di fondare sui soli risultati dell'elaborazione automatizzata le decisioni produttive di effetti giuridici in capo alle persone fisiche.

L'ultimo comma dell'art. 10, in piena continuità con gli 'usi e costumi' ormai invalsi negli ultimi decenni in materia di sicurezza e politica criminale, riporta la consueta clausola d'invarianza finanziaria.

Segue il **titolo II**, il cui **capo I (artt. 11-15)** contiene le norme espressamente dedicate al **diritto penale sostanziale e processuale**

L'art. 11 prevede l'applicazione delle definizioni contenute nell'art. 3 dell'AI Act.

L'art. 12 rubricato «Modifiche al codice penale» introduce il **nuovo art. 437 bis c.p.**, rubricato **«Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi»**. La disposizione è

ISSN 2239-8570

inserita all'interno dei delitti di comune pericolo contro l'incolumità pubblica (libro II, titolo VI, capo I del codice penale), e incrimina, al suo primo comma, l'omessa adozione di misure tecniche idonee a prevenire malfunzionamenti o alterazioni del funzionamento dei sistemi di IA ad alto rischio, nonché l'omissione delle necessarie misure di sorveglianza umana, quando da tali condotte derivi un pericolo concreto per la vita o l'incolumità individuale, con un aggravamento di pena quando tale pericolo si estenda all'incolumità pubblica o alla sicurezza dello Stato. Al secondo comma, invece, è prevista una fattispecie sussidiaria di alterazione illecita dei sistemi di cui al co. 1, anch'essa costruita come reato di pericolo concreto e corredata da un più severo trattamento sanzionatorio. Infine, il terzo comma contempla la possibilità di punire i fatti descritti dal primo anche in caso di colpa grave.

Oltre all'introduzione di fattispecie *ad hoc*, si interviene pure sulla **responsabilità amministrativa da reato degli enti**. In sintesi, **l'art. 15 dello schema n. 418 inserisce nel d.lgs. n. 231 del 2001 il nuovo art. 25 vicies, che estende tale responsabilità sia al nuovo delitto di cui all'art. 437 bis c.p., sia al reato di illecita diffusione di contenuti generati o manipolati artificialmente di cui all'art. 612 quater c.p.**, già introdotto dalla legge 132/2025. Per entrambe le fattispecie sono previste sanzioni pecuniarie e l'applicazione delle principali sanzioni interdittive contemplate dall'art. 9 del d.lgs. 231/2001.

Sul piano processuale, infine, **l'art. 13**, rubricato «Modifiche al codice di procedura penale» inserisce nel codice di procedura penale il **nuovo art. 359 ter c.p.p., rubricato «Identificazione e localizzazione mediante sistemi di intelligenza artificiale per l'identificazione biometrica remota in tempo reale».** La disposizione corrisponde alla previsione della terza categoria delle ipotesi eccezionalmente ammesse ai sensi dell'art 5(1)(iii) dell'AI Act. In breve, **l'utilizzo è consentito solo per confermare l'identificazione o ricercare persone nei cui confronti sussistano sufficienti indizi della commissione di uno dei delitti indicati nell'allegato II dell'AI Act**, puniti con la pena della reclusione non inferiore nel massimo a quattro anni. Il comma 2 del nuovo art. 359 ter c.p.p. contiene previsioni analoghe per la ricerca di **latitanti**. L'impiego del sistema è subordinato, di regola, all'**autorizzazione del giudice per le indagini preliminari**, su richiesta del pubblico ministero, mediante decreto motivato che delimita l'ambito territoriale, le persone interessate e la durata dell'attività, comunque non superiore a quindici giorni, salvo proroga. Sono inoltre disciplinate le procedure d'urgenza, che consentono, in presenza dei relativi presupposti, l'attivazione del sistema da parte del pubblico ministero ovvero, ove strettamente necessario, della polizia giudiziaria, ferma restando la successiva convalida giurisdizionale. Anche in questo contesto, lo schema prevede l'inutilizzabilità dei risultati ottenuti mediante sistemi di IA quando essi siano impiegati fuori dei casi consentiti dalla legge o in assenza delle prescritte autorizzazioni. Completa il quadro l'**art. 14** dello schema, che interviene con una **modifica di coordinamento sull'art. 104, co. 1, disp. att. c.p.p.**, estendendone la previsione della **lettera e bis)** ai dati «generati anche con sistemi di intelligenza artificiale».

ISSN 2239-8570

Con questo articolato, il Governo dà corpo a un intervento molto atteso, che inizia a tracciare i profili della giustizia penale e della politica criminale che dovranno gestire i rischi illeciti determinati dalla diffusione sempre più capillare dei sistemi intelligenti. In proposito, le linee di fondo, i principi ispiratori e le finalità dell'intervento appaiono in linea con i regolamenti UE e senz'altro condivisibili. Anzitutto, concepire e adoperare l'IA quale **strumento puramente ausiliario** rispetto alle attività di polizia e dell'autorità giudiziaria è senz'altro opportuno, poiché mantiene la decisione e, con essa, la responsabilità, saldamente in capo all'agente di polizia, prevenendo tanto deleghe decisionali surrettizie quanto la dispersione dell'accountability nelle maglie dei processi socio-tecnici complessi. In secondo luogo, per quel che concerne il diritto penale sostanziale, era da tempo avvertita, e più volte segnalata dalla dottrina, la necessità di introdurre **fattispecie incriminatrici in grado di intervenire anticipatamente** e indipendentemente rispetto alla verificazione di un evento lesivo derivante dal contatto con l'IA. In effetti, è ormai acquisito come essa rappresenti una nuova e complessa infrastruttura, che necessita di essere gestita nel suo intero ciclo vita per essere resa sicura. Pertanto. l'obiettivo di rafforzare penalmente il rispetto degli standard di sviluppo, implementazione e impiego merita di essere avallata, specie in relazione ai dispositivi c.d. ad alto rischio. A tale proposito, l'inserimento di simili illeciti nel catalogo dei **delitti presupposto della responsabilità da reato degli enti** lo si può ritenere addirittura necessitato: la polverizzazione dei processi di produzione e gestione dell'IA, distribuiti lungo catene di fornitura che assommano fornitori, sviluppatori, integratori e utilizzatori professionali, rende spesso impraticabile l'individuazione di una persona fisica cui muovere un rimprovero pienamente colpevole, sicché l'ente si candida a rimanere l'unico centro di imputazione realmente raggiungibile, anche dalla risposta punitiva.

Al netto della condivisibilità delle direttrici che sembrano sostenere questo articolato, vi sono però serie perplessità sulle tecniche e modalità impiegate per concretizzarle. A ben vedere, infatti, il provvedimento è caratterizzato da una vaghezza a tratti eccessiva, oltreché da lacune che rischiano di comprometterne l'impianto complessivo.

Partendo dalle garanzie predisposte per l'implementazione dell'IA nell'attività di polizia, esse risultano generiche nella loro formulazione, e piuttosto limitate nella loro estensione. In primo luogo, le «forme di revisione umana qualificata» sono disciplinate in termini eccessivamente elastici, poiché la norma si limita a richiedere «adeguate forme» di controllo (cfr. art. 3(4) schema n. 418), senza fissare standard minimi di competenza del personale e demandando *tout court* la loro individuazione alle procedure interne di ciascuna Forza. Come noto, **per effettuare una sorveglianza effettiva sarebbe necessario il possesso di competenze adeguate, altrimenti non esiste alcuna reale possibilità di discostarsi motivatamente dall'output**, prevenendo il ben noto fenomeno dell'*automation bias*. Inoltre, la garanzia opera soltanto prima dell'impiego dell'output in atti o provvedimenti incidenti sulla sfera giuridica delle persone, si lascia dunque scoperta tutta la fase precedente, nella quale i sistemi di IA possono già orientare attività di polizia suscettibili di produrre comunque effetti selettivi

ISSN 2239-8570

o stigmatizzanti (si pensi alla possibilità di effettuare controlli mirati, attenzionamenti, o valutazioni preliminari di pericolosità). Sempre in relazione al problema della competenza, poi, appare davvero poco credibile che la **formazione necessaria ad assicurare le competenze necessarie per l'utilizzo di queste nuove tecnologie, possa essere somministrata «nell'ambito delle risorse disponibili a legislazione vigente» (art. 6(1)** schema n. 418). La formazione effettiva costa, e prevederla senza dotazioni *ad hoc* rischia di trasformarla in un mero adempimento cartolare.

Ancora, l'impiego della identificazione biometrica in tempo reale (**art. 8** dello schema) soffre di diverse criticità, la più significativa delle quali appare di tipo procedurale. Invero, trattandosi di una **tecnologia capace di convertire ogni spazio pubblico in un ambiente identificativo, la richiesta di autorizzazione preventiva al pubblico ministero appare problematica**: è evidente come tale organo, pur appartenendo all'ordine giudiziario, non sia terzo rispetto alle esigenze investigative. Invero, la riserva di giurisdizione in senso proprio – che lo stesso schema mostra di saper costruire quando, all'art. 359 ter c.p.p., affida l'autorizzazione al giudice per le indagini preliminari – avrebbe costituito la soluzione più coerente con l'intensità dell'ingerenza che l'identificazione biometrica produce.

Venendo alle disposizioni sui sistemi di videosorveglianza dotati della tecnologia di riconoscimento facciale a posteriori (**art. 10** dello schema), esse si candidano a essere le più problematiche dell'intero articolato. In primo luogo, quest'attività per essere espletata presuppone la raccolta e memorizzazione preventiva dei dati biometrici di tutte le persone che accedono a determinati luoghi o eventi. Si tratta, dunque, di un **arruolamento biometrico di una platea ampia e indifferenziata, anteriore alla commissione di qualsivoglia illecito**. In secondo luogo, il presupposto applicativo è piuttosto ampio: si parla della «commissione di un fatto di reato, anche nell'ipotesi tentata», senza alcuna distinzione sulla base della gravità dell'illecito commesso. Il rischio, dunque, è che una tecnologia altamente invasiva sia attivabile per fatti non necessariamente proporzionati rispetto alla compressione dei diritti che essa determina in capo a molti dei soggetti biometricamente acquisiti.

Parla da sola, poi, la scelta di concludere il titolo I con una clausola d'invarianza finanziaria (art. 10(13) dello schema n. 418). In effetti, si tratta di una previsione davvero poco credibile, sia per l'ambizione che questo articolato assume, sia per gli interventi che il suo adempimento presuppone.

Venendo, infine, alle disposizioni dedicate al diritto penale sostanziale e processuale, vi sono diversi profili critici in materia di legalità, proporzionalità e offensività dell'intervento repressivo, nonché in relazione al rispetto del giusto processo.

Partendo dal primo dei reati introdotti dall'art. 12 dello schema (comma 1 del nuovo art. 437 bis c.p), si tratta di un illecito solo apparentemente comune, che per di più è stato riformulato in modo poco tassativo e potenzialmente ineffettivo. Procedendo con ordine, le condotte descritte presuppongono il possesso di ruoli che, a cagione dell'ampiezza del precetto, risultano essere anche molto distanti: a solo titolo esemplificativo, vi sono il fornitore (cui fanno capo progettazione, addestramento e sviluppo del sistema),

ISSN 2239-8570

l'importatore, il distributore, il rappresentante autorizzato (art. 3, punti 3-7, dell'AI Act), il fabbricante del prodotto che integra il sistema, figura alla quale la disciplina della responsabilità da prodotto (dir. UE 2024/2853) affianca il fabbricante di componenti e chi apporta modifiche sostanziali, fino alla persona fisica incaricata della sorveglianza umana ai sensi dell'art. 14 dell'AI Act, e del deployer che lo impiega sotto la propria autorità (il riferimento all' «utilizzo professionale» sembra alludere proprio a tale figura, con il rischio di attrarre nell'area del penalmente rilevante qualsiasi professionista che impieghi sistemi ad alto rischio nell'esercizio della propria attività). Nondimeno, nella disposizione, la loro posizione risulta del tutto parificata sotto l'ampio ombrello del "chiunque", sulla base di soli due concetti organizzatori: la mancata adozione di misure tecniche idonee a prevenire malfunzionamenti o alterazioni dei sistemi, ovvero di misure di sorveglianza umana; il verificarsi di un pericolo concreto per la vita o l'incolumità individuale a causa di essi. Ebbene, si tratta di una soluzione che sembra dettata da un deficit di approfondimento, piuttosto che da una avveduta scelta politico-criminale. Lo dimostra la mancata tipizzazione delle condotte: sebbene esse siano suscettibili di essere meglio specificate dall'interprete attraverso la loro (non semplice, e tantomeno lineare) integrazione con l'AI Act e la normativa settoriale volta per volta rilevante, esse sono state descritte mediante clausole funzionali e rinvii tanto estesi da sollevare dubbi quanto al rispetto dei canoni di determinatezza e accessibilità del precetto penale. Inoltre, esse rischiano di produrre persino **problemi di *ne bis in idem***: l'AI Act, infatti, prevede un ampio *parterre* (tra l'altro) di sanzioni amministrative, con cui questa penalizzazione "a tappeto" delle non conformità rischia di coincidere (con quanto ne segue in punto di *matière pénale* e di garanzie europee e convenzionali). E che sia il *deficit* di approfondimento a sostenere le scelte di tipizzazione del precetto sembra confermarlo pure il riferimento al pericolo concreto, che pure il legislatore sembra aver previsto proprio per correggere almeno in chiave di idoneità lesiva tale genericità, cercando al contempo di conferire alla norma un maggior grado di offensività rispetto alle mere difformità (già sanzionate in via amministrativa). A ben vedere, infatti, tale referente viene qui caricato di un compito selettivo che, da solo, non sembra in grado di assolvere. Invero, **in assenza di condotte ben tipizzate**, il suo accertamento giudiziale (da condurre su sistemi opachi, probabilistici e in continuo aggiornamento) rischia di risolversi, nella prassi, in una presunzione ricavata a ritroso dalla violazione di una qualsivoglia regola cautelare. Si tratta della ben nota fallacia del senno di poi (*hindsight bias*), che potrà eventualmente essere innescata dal riscontro di un rapporto di rischio con l'evento che si è verificato (ciò a maggior ragione nei casi in cui l'accertamento venga occasionato dal verificarsi di un accadimento lesivo dopo il contatto con queste tecnologie, dato che nella prassi finirà per vanificare ulteriormente questo filtro selettivo). Sarebbe stato più opportuno, dunque, differenziare meglio le diverse posizioni soggettive, e specificare in modo più adeguato le differenti categorie d'inosservanze suscettibili di giustificare l'intervento repressivo. In particolare, si sarebbero potute selezionare le più significative negligenze nei processi di sviluppo, addestramento, validazione, integrazione e sorveglianza,

ISSN 2239-8570

limitando la rilevanza penale alle violazioni capaci di incidere in misura critica sulla sicurezza degli utenti finali. Pertanto, più che una macro-norma generale (*rectius*, generica), sarebbe stata preferibile una disciplina maggiormente differenziata, capace di valorizzare il tessuto regolatorio che circonda la produzione e l'impiego dei sistemi di IA nei singoli settori ad alto rischio (in ambito sanitario, per esempio, dovrebbero essere considerati non soltanto gli obblighi derivanti dall'AI Act, ma anche quelli previsti dal regolamento (UE) 2017/745 relativo ai dispositivi medici e dalle ulteriori discipline concernenti la sicurezza delle cure, la valutazione di conformità e la sorveglianza successiva all'immissione sul mercato).

Per quel che concerne, invece, la seconda disposizione incriminatrice (comma 2 del nuovo art. 437-bis c.p), la clausola di sussidiarietà che la introduce («salvo che il fatto costituisca più grave reato») cede il passo agli illeciti più gravi, ma nulla dispone per l'ipotesi in cui l'alterazione del sistema integri anche reati informatici di gravità pari o inferiore. Lo si vede bene prendendo in considerazione il raggruppamento delle fattispecie relative al danneggiamento informatico. Quando il sistema IA ad alto rischio è altrui, l'alterazione che ne ostacoli gravemente il funzionamento o lo renda inservibile ricade nell'art. 635-quater c.p., che è punito con la reclusione da uno a cinque anni. La pena è dunque inferiore, dunque la clausola è inoperante. Se poi il sistema è di pubblico interesse (si pensi, per esempio, proprio a quelli in dotazione all'autorità di pubblica sicurezza), viene in rilievo l'art. 635-quinquies c.p., che, dopo la riscrittura ad opera della l. 90/2024, commina la medesima pena della prima ipotesi del comma in esame, ossia la reclusione da due a sei anni. Analogo discorso vale per la frode informatica. Tra l'altro, si tratta di fattispecie poste per lo più in rapporto di interferenza, e in ogni caso non di specialità unilaterale, con conseguente esclusione del criterio di specialità (art. 15 c.p.). L'esito prevedibile, quindi, è la moltiplicazione delle ipotesi di concorso formale di reati (art. 81 c.p.), con ricadute sanzionatorie che il legislatore delegato avrebbe potuto, e forse dovuto, governare in modo più attento.

Infine, la previsione che punisce i fatti del primo comma commessi per colpa grave con pena "ridotta da un terzo a un sesto" aggiunge una nota d'insolito a un edificio già periclitante. L'intervallo della diminuzione, infatti, è enunciato in ordine decrescente, contro la prassi legislativa che lo esprime dal minimo al massimo. Inoltre, si adopera una modalità di descrizione in stile circostanziale, per un precetto che – delineando un'ipotesi colposa di un reato altrimenti doloso – non può che dar vita a una fattispecie autonoma. La tecnica di redazione che doveva essere adoperata, allora, era quella che il codice impiega per esempio nella coppia degli artt. 437 e 451 c.p.: due norme distinte, non un comma di rinvio con una pena determinata in modo bizzarro e *per relationem*. Merita invece approvazione la scelta della colpa grave quale soglia di rilevanza dell'illecito colposo. Si tratta di una soglia che restringe la punibilità rispetto alla delega, operando in *bonam partem*, ed è coerente con la linea di politica del diritto che riserva la sanzione penale alle violazioni macroscopiche nei contesti connotati da speciale complessità tecnica e da incertezza nomologica (ai quali i sistemi IA ad alto rischio indubbiamente appartengono).

ISSN 2239-8570

Venendo al piano processuale, è apprezzabile la scelta di affidare al giudice per le indagini preliminari l'autorizzazione all'impiego dei sistemi di cui all'art. 359-ter c.p.p., nondimeno le problematiche restano, e gravano sul piano epistemico. Difatti, non si stabilisce nulla in merito alla verificabilità scientifica e alla confutabilità degli esiti algoritmici. Esiste dunque il rischio di acquisire nel processo *output* che né le parti né il giudice sono in condizione di controllare, con evidente compressione del contraddittorio nella formazione della prova. D'altra parte, se si allarga lo sguardo alle disposizioni prevista in materia di responsabilità civile, il paradosso diventa piuttosto evidente: l'art. 19 infatti accorda al danneggiato l'esibizione dei registri, della documentazione tecnica e dei parametri di supervisione umana del sistema; nulla di simile, invece, è previsto per la giustizia penale. Né la sanzione dell'inutilizzabilità basta a risolvere le problematiche che s'intravedono, poiché essa colpisce i "risultati" forniti dal sistema, ma tace sulle prove derivate. In definitiva, le direttrici dell'intervento risultano condivisibili, ma la tecnica attuativa porta allo scoperto il *deficit* di approfondimento delle dinamiche di funzionamento e delle esigenze di tutela proprie del peculiare sistema socio-tecnico che si sta sviluppando. Sul fronte del diritto penale sostanziale e processuale, pare evidente l'esigenza di un importante intervento di modifica, che restituisca determinatezza al precetto penale, coordini le nuove incriminazioni con l'apparato sanzionatorio amministrativo europeo e incrementi le garanzie processuali, assicurando la trasparenza e l'effettiva sindacabilità degli strumenti IA impiegati. Del resto, per la giustizia penale di una repubblica democratica, non può che valere ancora, e qui più che mai, l'insegnamento di Franco Cordero, tutto proteso a creare la consapevolezza del primato del metodo, e delle sue garanzie, sul risultato.

NICOLÒ AMORE

Schema di decreto legislativo

2026/2(10)TDMCDV
(segue) Le disposizioni sulla responsabilità civile

Come illustrato *supra* nel contributo n. 8 in questa Rubrica ([2026/2(8)FZ]), con lo schema di decreto legislativo approvato il 9.6.2026, atto di governo n. 418 (lo **schema n. 418** o lo **schema**), in attuazione della delega contenuta nell'art. 24(3), come specificata dall'art. 24(5)(d) della legge 23 settembre 2025, n. 132 (sulla legge 132/2025 v. in questa Rubrica il contributo n. 1 del numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016), il Governo ha previsto nel **capo II del titolo II** dello schema n. 418, agli **artt. 16-20**, una serie di disposizioni sotto il titolo «**Strumenti processuali civili per il risarcimento dei danni cagionati dall'utilizzo di sistemi di IA**».
L'art. 16 dello schema disciplina l'ambito di applicazione e il foro del consumatore. Il comma 1 prevede l'applicabilità del particolare regime di accesso alle prove introdotto dal successivo art. 17 (cfr. *infra*) a tutte le «**azioni di risarcimento del danno, sia contrattuale sia extracontrattuale,**

ISSN 2239-8570

cagionato nell'utilizzo di un sistema di IA», mentre il comma 2 precisa che, qualora tali azioni riguardino un danno che derivi dalla **violazione di uno o più obblighi previsti dal reg. (UE) 2024/1689** (**AI Act** o **AIA**), si applicano anche gli artt. 18 e 19 dello schema (cfr. *infra*). Rimane salva l'applicazione, ai sensi del comma 3 dell'art. 16, delle regole di responsabilità civile poste dalla disciplina del reg. (UE) 2016/679 (**GDPR**) sull'illecito trattamento di dati personali (**art. 82 GDPR**) e dal recepimento della nuova direttiva sulla responsabilità da prodotto difettoso (direttiva UE 2024/2853 o **nuova PLD**). Per quanto riguarda il foro, il comma 4 dell'art. 16 dello schema dispone che, nelle azioni suddette, **quando il danneggiato è una persona fisica che agisce per scopi estranei all'attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta, è altresì competente il giudice del luogo in cui il danneggiato ha la residenza o il domicilio**.

L'art. 17 dello schema introduce un regime di accesso alle prove, simile a quanto previsto nella nuova PLD e che ricalca, in tema di divulgazione di elementi di prova, il contenuto della proposta di direttiva sulla responsabilità civile per l'IA (cd AI liability directive) del 28 settembre 2022 (su cui v. in questa Rubrica il contributo n. 1 del numero 2/2022, in PeM 2022, p. 500), successivamente ritirata dalla Commissione europea nel 2025. Una differenza fondamentale, però, rispetto alla precedente proposta europea è che **lo schema n. 418 non limita il regime di divulgazione alle cause risarcitorie fondate sulla colpa del convenuto, ma si estende potenzialmente a qualsiasi criterio di imputazione, soggettivo o oggettivo, extracontrattuale o contrattuale**. Il comma 1 dell'art. 17 dello schema prevede che, nelle azioni di risarcimento del danno menzionate, il giudice, su istanza della parte che allega di avere subito il danno, **ordina all'altra parte o al terzo** che ne dispone **l'esibizione** degli elementi di prova specificamente pertinenti relativi al funzionamento del sistema di IA, quando l'istante presenta fatti ed elementi idonei a rendere verosimile la fondatezza della domanda, anche con riferimento al collegamento tra il risultato prodotto dal sistema di IA e il danno lamentato. Viene, pertanto, mantenuta anche nella versione nazionale il **prerequisito della plausibilità della domanda per poter accedere a tale strumento processuale**. Ai sensi del comma 2 dell'art. 17, **tra gli elementi di prova di cui al comma 1 vengano elencati in via esemplificativa**:

a) i registri di cui all'art. 12 AIA (dove si conservano le registrazioni automatiche degli eventi, o «log»);

b) la documentazione relativa al sistema di gestione dei rischi di cui all'art. 9 AIA;

c) le informazioni pertinenti contenute nella documentazione tecnica di cui all'art. 11 AIA;

d) le informazioni relative ai parametri e alle modalità di supervisione umana di cui all'art. 14 AIA.

AI sensi dell'**art. 17(3)** dello schema, l'ordine di esibizione dovrà essere limitato a quanto necessario e proporzionato rispetto alla domanda, tenendo in considerazione tutti gli interessi delle parti con particolare riguardo alla tutela dei segreti commerciali e delle informazioni riservate per la cui tutela, ai sensi del successivo **comma 4**, il giudice adotta tutte le misure idonee. Il

ISSN 2239-8570

comma 5 dell'art. 17 dello schema fa discendere dall'ingiustificato inadempimento, totale o parziale, dell'ordine di esibizione rivolta alla parte conseguenze favorevoli per l'istante: infatti, in tali casi, il giudice può desumere argomenti di prova ai sensi dell'**articolo 116 c.p.c.**, mentre se l'inadempimento riguarda la documentazione di cui al comma 2 il giudice, valutato ogni altro elemento di prova, ritiene come ammessi i fatti allegati dall'istante, operando in maniera similare a una presunzione legale – senza, peraltro, esplicito riferimento alla possibilità di fornire una prova contraria – ovvero secondo un meccanismo di non contestazione.
Se invece l'ordine di esibizione viene rivolto a un **terzo** e questi senza giustificato motivo non adempie, anche parzialmente, il giudice lo condanna a una **pena pecuniaria** da euro 1.500 a euro 10.000 (**art. 17(6)**)
Gli artt. 18 e 19 dello schema attuano un ulteriore collegamento con la disciplina di cui all'AI Act. In particolare, l'**art. 18** prevede una (questa volta esplicita) **presunzione del nesso di causalità tra violazione di uno o più obblighi previsti dall'AI Act e danno**, quando (venga allegato che) il danno derivi dalla violazione di uno o più obblighi previsti dall'AI Act. In tal caso, è esplicitamente ammessa la prova contraria del convenuto. L'**art. 19** precisa, invece, che «**la conformità del sistema di IA agli obblighi previsti dal[l'AI Act], anche se certificata ai sensi del capo III, sezione 5, del medesimo regolamento, non esclude di per sé la responsabilità** del convenuto». Da tale disposizione si evince la volontà del Governo di sottolineare la differenza tra **regole di sicurezza e regole di responsabilità**, che non sempre si sovrappongono nel loro ambito applicativo, in modo da scongiurare il rischio che la sola conformità all'AI Act divenga per le imprese una sorta di *safe harbour* idoneo a schermarle da qualsiasi pretesa risarcitoria.
Infine, l'**art. 20** dello schema introduce alcune norme in tema di **azione diretta del danneggiato nei confronti dell'impresa di assicurazione** del convenuto. In particolare, chi intende promuovere un'azione risarcitoria può chiedere preventivamente al soggetto che ritiene responsabile se è assistito da un contratto di assicurazione della responsabilità civile relativo al danno medesimo. Tale richiesta non costituisce condizione di procedibilità della domanda ma, in caso di omessa o incompleta comunicazione entro trenta giorni dalla sua ricezione, il giudice può desumere argomenti di prova ai sensi dell'art. 116 c.p.c. Ciò premesso, il danneggiato ha azione diretta per il risarcimento del danno nei confronti dell'impresa di assicurazione del convenuto – il quale è litisconsorte necessario a norma del comma 5 – rimanendo opponibili al danneggiato le eccezioni derivanti dal contratto di assicurazione, purché anteriori al sinistro. L'impresa di assicurazione che effettua il pagamento ha poi diritto di rivalsa verso l'assicurato nella misura in cui avrebbe avuto titolo contrattuale per rifiutare o ridurre la propria prestazione. L'azione diretta è soggetta al medesimo termine di prescrizione dell'azione nei confronti del soggetto individuato quale responsabile del danno.

TOMMASO DE MARI CASARETO DAL VERME

Schema di decreto legislativo

ISSN 2239-8570

2026/2(11)FPa

La versione finale del 10.6.2026 del code of practice sulla trasparenza dei contenuti generati da sistemi di IA ai sensi dell'AI Act

Il 10 giugno 2026 è stata pubblicata la versione finale del *Codice di buone pratiche sulla trasparenza di contenuti generati dall'intelligenza artificiale* (il **Codice**). Il Codice, elaborato ai sensi dell'**art. 50(7)** del reg. (UE) 2024/1689 (**AI Act** o **AIA**), è stato il frutto di un lavoro che ha riguardato oltre centottanta tra stakeholders, esperti, accademici e membri della società civile divisi in due gruppi tematici: uno relativo alla trasparenza in capo al fornitore di strumenti di IA, l'altro relativo al distributore. Con il parere della Commissione europea (la **Commissione**) sulla adeguatezza del Codice (C(2026) 4839 final), adottato l'8.7.2026 ai sensi degli **articoli 50(7) e 56(6) AIA** (il **parere della Commissione**) unitamente alla parallela conclusione del Comitato europeo per l'intelligenza artificiale (**EAIB** o **AI Board**) (la **conclusione dell'AI Board**), si è davvero chiuso il procedimento avviato lo scorso anno e che aveva visto una **prima bozza del Codice pubblicata il 17 dicembre 2025**. Di tale prima bozza, e della sua impostazione di fondo, ci si è occupati in un precedente contributo su questa Rivista (v. in questa Rubrica il contributo n. 8 del numero 4/2025 , [2025/4(8)FPa] in PeM, 2025, p. 1041). In quella sede, si erano messi in luce la funzione trasversale dell'art. 50 nell'architettura dell'AI Act e il ruolo di cerniera tra *soft law* e *hard law* che il Codice era destinato ad assumere. Le presenti note intendono invece soffermarsi su ciò che la chiusura del procedimento consente ora di osservare con maggiore nitidezza: la **fisionomia degli obblighi gravanti sulla filiera dei fornitori**, il significato che la **volontarietà dello strumento** assume all'indomani della valutazione di adeguatezza e, in prospettiva interna, il raccordo, tutt'altro che lineare, con le scelte compiute dal legislatore italiano con la **legge 23 settembre 2025, n. 132** (sulla legge 132/2025 v. in questa Rubrica il contributo n. 1 del numero 3/2025 [2025/3(1)AA], in PeM 2025, p. 1016), che ha affidato al **diritto penale** la risposta ai medesimi fenomeni che l'AI Act affronta, invece, con la tecnica della trasparenza e della *soft law*.
Cominciando dalle **disposizioni sui fornitori e la filiera del *marking***, può osservarsi che la Sezione 1 del Codice dà attuazione agli obblighi di cui all'art. 50, parr. 2 e 5, dell'AI Act, che gravano sui fornitori di sistemi di IA generativa:

- **marcatura degli output in formato leggibile da macchina**,
- loro **rilevabilità** come artificialmente generati o manipolati,
- rispetto dei quattro **requisiti tecnici di efficacia, interoperabilità, robustezza e affidabilità**, e
- **comunicazione del risultato** della rilevazione alle persone fisiche in modo chiaro e distinguibile.

Come sottolineato dal parere della Commissione, si tratta di elementi distinti ma intrinsecamente collegati di un'unica obbligazione di trasparenza, che il Codice traduce in quattro doveri (**Commitments**) che si traducono in una pluralità di misure applicatove (**Measures**): ***(i)*** la marcatura secondo un

ISSN 2239-8570

approccio a doppio livello (metadati firmati digitalmente e *watermarking* impercettibile), giustificato dalla constatazione che nessuna tecnica è, allo stato dell'arte, da sola sufficiente; ***(ii)*** la predisposizione di una *detection solution*, in linea di principio gratuita, accessibile a *deployer*, utenti, autorità, ricercatori e società civile; ***(iii)*** le specificazioni tecniche dei requisiti di efficacia, interoperabilità, robustezza e affidabilità, con un'implementazione a fasi dell'interoperabilità che culmina nella scadenza del 2 febbraio 2027 per le soluzioni di interoperabilità tra meccanismi di rilevazione del *watermarking*; ***(iv)*** infine, i processi di *testing*, verifica e *compliance* lungo l'intero ciclo di vita del sistema.

Il punto che merita maggiore attenzione è, tuttavia, il perimetro soggettivo della Sezione. **Destinatari degli obblighi sono, e restano, i fornitori di sistemi di IA generativa**: la Sezione 1 non si applica, in linea di principio, ai *deployer*, i cui obblighi di etichettatura trovano collocazione nella distinta Sezione 2. E però il Codice apre espressamente all'**adesione volontaria di due ulteriori categorie di operatori** che l'art. 50(2) AIA non contempla: i fornitori di modelli di IA generativa immessi sul mercato indipendentemente da un sistema, e i fornitori terzi di soluzioni di *marking* e *detection*. Costoro possono aderire al Codice per dimostrare che il proprio modello o la propria soluzione tecnica soddisfa i requisiti dell'art. 50, parr. 2 e 5 AIA, «con l'obiettivo di facilitare la compliance dei fornitori a valle» di sistemi costruiti su quei modelli o che si avvalgono di quelle soluzioni. La Commissione valorizza espressamente questa apertura, riconducendola all'obiettivo, enunciato dal **cons. 135 dell'AI Act**, di facilitare la cooperazione lungo la catena del valore.

Si tratta di una scelta significativa sotto un duplice profilo. Per un verso, essa prende atto della realtà industriale della trasparenza tecnica: la marcatura, e in particolare il *watermarking* a livello di modello, è tanto più robusta quanto più a monte viene implementata, sicché il baricentro effettivo della compliance tende a spostarsi dal fornitore del sistema, formale destinatario dell'obbligo, al fornitore del modello o della soluzione tecnica, che destinatario non è.

Per altro verso, la costruzione conferma che **l'art. 50 AIA impone obblighi a livello di sistema e non di modello**: la prima bozza del Codice, che aveva prospettato impegni vincolanti per i fornitori di modelli di AI generativi firmatari, è stata su questo punto ridimensionata, e il testo finale si limita a incoraggiarne l'adesione e a chiarire che, in tal caso, Commitments e Measures si intendono riferiti al modello o alla soluzione di *marking* del firmatario. Ne risulta una filiera della trasparenza a "geometria variabile", nella quale la responsabilità ultima resta in capo al *provider* del sistema, che può fare affidamento su soluzioni e documentazione di terzi «senza pregiudizio» della propria responsabilità, mentre gli anelli a monte partecipano su base volontaria. È una soluzione coerente con il dato normativo, ma che consegna alle dinamiche contrattuali e di mercato la distribuzione effettiva degli oneri di trasparenza lungo la catena del valore.

Il secondo profilo su cui la chiusura del procedimento con la pubblicazione della versione finale del Codice consente una riflessione più matura è il **significato della volontarietà**. Formalmente, nulla è mutato: il Codice resta

ISSN 2239-8570

uno strumento ad adesione volontaria e la stessa Commissione ribadisce che l'adesione «non costituisce prova conclusiva di conformità» agli obblighi dell'art. 50 AIA. E tuttavia la valutazione di adeguatezza ne trasforma sensibilmente la portata pratica. La Commissione conclude che fornitori e deployer «possono fare affidamento sul Codice quale strumento riconosciuto a livello di Unione considerato adeguato ad assicurare la conformità» ai rispettivi obblighi, indipendentemente dal luogo di stabilimento e dall'autorità di vigilanza competente; l'AI Board si spinge oltre, indicando alle autorità di vigilanza del mercato che il Codice deve essere considerato, a partire dal luglio 2026, «l'unico strumento pratico a livello UE» valutato come adeguato per l'attuazione degli obblighi di trasparenza.

Ne discende una situazione che è ormai familiare nell'esperienza dei codici previsti dall'AI Act, il precedente immediato è il Codice per i modelli di IA per finalità generali adottato nel corso del 2025 (su cui v. in questa Rubrica il contributo n. 7 nel numero 4/2025 [2025/4(7)SO], in PeM 2025, p. 1039), ma che qui si presenta con tratti peculiari. L'adesione non esonera dal controllo: le autorità conservano intatti i poteri di richiedere informazioni e di verificare che gli impegni siano stati effettivamente attuati. Chi sceglie percorsi di *compliance* alternativi, però, non si trova nella stessa posizione di chi aderisce, perché dovrà dimostrare autonomamente l'adeguatezza dei percorsi alternativi, con un onere probatorio e un margine di incertezza che rendono l'adesione, più che una scelta reputazionale, una strategia di riduzione del rischio regolatorio. **La volontarietà, in altri termini, si riduce alla scelta del percorso, non del risultato: l'obbligo di trasparenza è vincolante per legge, e il Codice ne rappresenta la via di adempimento «presuntivamente» sicura**.

Vi è di più. Sia il parere della Commissione che la Conclusione dell'AI Board configurano l'adeguatezza come condizionata e reversibile. L'AI Board individua espressamente nella "Measure 3.4" sull'interoperabilità, e nella scadenza del 2 febbraio 2027, il banco di prova del Codice, riservandosi, in caso di progressi insufficienti, di raccomandare alla Commissione una revisione mirata o l'adozione di *common rules* ai sensi dell'art. 50(7) AIA. L'AI Board segnala inoltre che la determinazione di ciò che costituisce una soluzione sufficientemente robusta «non può essere lasciata alla sola valutazione dei firmatari», invita a revisioni mirate ove emergano soluzioni di interoperabilità più robuste non adottate dai firmatari. Sul versante dei *deployer*, l'EIAB annuncia un monitoraggio sulla misura in cui, nella prassi, le etichette siano effettivamente conservate nella successiva elaborazione e distribuzione su piattaforma: questione cruciale, e volutamente lasciata aperta dal Codice, che sul punto si affida a impegni di cooperazione *best effort* nel concreto e ogni operatore per quanto di propria competenza.

L'adeguatezza si configura, dunque, non come un giudizio statico, ma come un patto di implementazione sotto osservazione, il cui inadempimento riattiva l'opzione regolatoria unilaterale. È la conferma più nitida della funzione di cerniera tra *soft law* e *hard law* che si era prospettata commentando la prima bozza: cerniera che, ora, ha anche una data di verifica.

La chiusura del procedimento consente infine di precisare **quale nozione di trasparenza** il sistema dell'art. 50 AIA effettivamente accolga. Non si tratta

ISSN 2239-8570

di una trasparenza sul funzionamento del sistema (quella, interna alla filiera, dell'art. 13 AIA), né di un giudizio di attendibilità del contenuto: come chiarisce la Sezione 2 del Codice, la disclosure non mira a informare gli individui sulla affidabilità di ciò che vedono, ma sulla sua origine artificiale o sul ruolo dell'IA nella sua manipolazione. Si tratta, piuttosto, di una **trasparenza a doppio strato: *machine-facing*,** nella misura in cui la marcatura leggibile da macchina e i meccanismi di *detection* costruiscono un'infrastruttura di verificabilità destinata a piattaforme, autorità, ricercatori e *fact-checker*; ***human-facing*,** nella misura in cui etichette, icone e *disclaimer* traducono quella verificabilità in informazione immediatamente percepibile dalla persona esposta al contenuto.

Il primo strato grava sui fornitori, il secondo sui deployer; la valutazione di adeguatezza li salda in un unico ecosistema, il cui funzionamento dipende però, ed è il punto su cui entrambi i pareri concentrano le proprie riserve, dalla tenuta degli anelli intermedi: ossia, interoperabilità delle soluzioni di individuazione del contenuto artificiale e persistenza delle marcature e delle etichette lungo la catena di disseminazione.

Appare, infine, interessante, indagare il **raccordo con l'ordinamento italiano** e in particolare con **la legge n. 132/2025**.

Ed infatti, proprio la natura infrastrutturale e preventiva della trasparenza europea rende utile un confronto con la strategia seguita dal legislatore italiano. La legge 132/2025 ha infatti affidato la risposta ai fenomeni di *deception* generativa, in primis i *deepfake*, allo strumento penale, secondo tre direttrici. In primo luogo, l'introduzione all'**art. 61 c.p.** della **circostanza aggravante comune di cui al n. 11-undecies**, per l'aver commesso il fatto mediante l'impiego di sistemi di IA quando questi, per natura o modalità di utilizzo, abbiano costituito mezzo insidioso, ostacolato la difesa pubblica o privata ovvero aggravato le conseguenze del reato. In secondo luogo, l'aggravamento sanzionatorio dell'**art. 294 c.p.** quando l'inganno ai danni dell'elettore sia realizzato mediante sistemi di IA. In terzo luogo, ed è la novità di maggior rilievo sistematico, l'introduzione dell'**art. 612-quater c.p.**, che punisce con la reclusione da uno a cinque anni chiunque cagioni un danno ingiusto a una persona cedendo, pubblicando o comunque diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante sistemi di IA e «idonei a indurre in inganno sulla loro genuinità».

Il confronto tra i due modelli è istruttivo anzitutto sul piano dei destinatari. L'art. 50 dell'AI Act e il Codice si rivolgono a operatori qualificati della filiera, *provider* e *deployer*, e operano *ex ante*, imponendo marcatura, rilevabilità ed etichettatura prima e a prescindere da qualsiasi danno. L'**art. 612-quater c.p.**, invece, si rivolge a chiunque diffonda il contenuto e opera *ex post*, sanzionando la lesione effettivamente cagionata. I due regimi intercettano dunque segmenti diversi, e in parte complementari, della medesima catena: il diritto europeo presidia la produzione e la prima immissione in circolazione del contenuto sintetico; il diritto penale interno ne presidia la circolazione dannosa, tipicamente ad opera di soggetti (il singolo utente che diffonde il *deepfake* non consensuale) che restano estranei tanto alla nozione di *provider* quanto, nella generalità dei casi, a quella di *deployer* rilevante ai sensi dell'**art. 50(4) AIA**.

ISSN 2239-8570

Più delicato è il punto di contatto rappresentato dal requisito dell'idoneità ingannatoria. Ci si può chiedere, in particolare, se un contenuto regolarmente marcato ed etichettato in conformità al Codice conservi l'idoneità «a indurre in inganno sulla genuinità» richiesta dalla fattispecie. La risposta non può essere univoca. La marcatura *machine-readable* di cui alla Sezione 1, per definizione impercettibile alla persona, non incide di per sé sulla capacità decettiva del contenuto agli occhi di chi vi è esposto; l'etichetta percepibile di cui alla Sezione 2, viceversa, è astrattamente idonea a neutralizzarla, ma la sua rimozione, che il Codice affronta con obblighi di robustezza e con impegni di preservazione lungo la filiera la cui tenuta, come visto, lo stesso Board si riserva di monitorare, riporta il contenuto nella piena operatività della fattispecie penale.

Né, in senso inverso, l'etichettatura vale come salvacondotto: lo stesso Codice precisa che l'apposizione dell'etichetta non esonera dal rispetto delle altre norme dell'Unione e degli Stati membri poste a tutela dei diritti dei terzi, ivi compresi i requisiti di consenso delle persone ritratte: previsione che dialoga direttamente con l'**art. 612-quater c.p.**, imperniato appunto sull'assenza di consenso e sul danno ingiusto. Se ne può concludere che la *compliance* trasparenziale e la responsabilità penale corrono su piani distinti, ma non incomunicanti: l'adempimento degli obblighi di marcatura ed etichettatura potrà semmai rilevare, in concreto, nella valutazione dell'idoneità decettiva del contenuto o del carattere insidioso del mezzo ai fini dell'aggravante di cui all'**art. 61, n. 11-undecies, c.p.**, senza tuttavia elidere l'illiceità della diffusione non consensuale e dannosa.

In conclusione, la trasparenza europea e la repressione penale di matrice interna appaiono meno alternative di quanto la diversità di tecnica normativa lascerebbe supporre: la prima costruisce l'infrastruttura, di marcatura, rilevabilità ed etichettatura, che rende riconoscibile il contenuto sintetico; la seconda sanziona chi di quella riconoscibilità si disfa, o comunque impiega il contenuto per ledere. Il buon funzionamento del raccordo dipenderà, ancora una volta, dall'effettività della capacità di *enforcement* dell'una e dell'altra misura e, in particolare, dalla persistenza delle marcature e delle etichette lungo la catena di disseminazione, che la valutazione di adeguatezza ha eletto, non a caso, a oggetto privilegiato del monitoraggio che si apre ora.

FEDERICA PAOLUCCI

Code of practice
Timeline of Code of practice
Parere della Commissione
Conclusione dell'AI Board

2026/2(12)SO
Il quadro legislativo nazionale sull'intelligenza artificiale dell'amministrazione Trump, annunciato il 20 marzo 2026

ISSN 2239-8570

In continuità con le linee di politica legislativa espressi negli *executive orders* emanati nel corso del 2025, il National Policy Framework for Artificial Intelligence della Casa Bianca, pubblicato il 20.3.2026 (il **Documento**), è un documento di indirizzo non vincolante che esorta il Congresso a stabilire un regime federale unificato, lungo tre direttrici:

- preclusione delle leggi statali sull'IA,
- supremazia tecnologica statunitense, e
- approccio favorevole all'innovazione.

Il Documento sviluppa queste tre direttrici nelle seguenti sette aree di intervento, o pilastri tematici:

I. Protecting Children and Empowering Parents
II. Safeguarding and Strengthening American Communities
III. Respecting Intellectual Property Rights and Supporting Creators
IV. Preventing Censorship and Protecting Free Speech
V. Enabling Innovation and Ensuring American AI Dominance
VI. Educating Americans and Developing an A I-Ready Workforce
VII. Establishing a Federal Policy Framework, Preempting Cumbersome State AI Laws

Si tratta, come detto, essenzialmente di una *summa* degli *executive orders* già emanati dal Presidente Trump a partire dal gennaio 2025, con qualche novità.

Il **primo** pilastro tematico (*Protecting Children and Empowering Parents)* esprime l'unica istanza di tutela delle persone fisiche esposte agli output di sistemi di IA, ravvisata dall'amministrazione Trump.

Il **secondo** pilastro tematico dal titolo piuttosto oscuro (*Safeguarding and Strengthening American Communities*) riguarda in realtà le *policies* ampiamente anticipate nei precedenti *executive orders* e altri atti di indirizzo marcatamente favorevoli allo ***sviluppo di data centers*.** Il *favor* è confermato anche nel Documento, unitamente al richiamo dell'esigenza di gestire l'impatto infrastrutturale e la fornitura energetica dei centri di calcolo per rafforzare (*sic*) e tutelare le comunità americane.

Relativamente al **terzo** pilastro tematico (*Respecting Intellectual Property Rights and Supporting Creators*), **l'amministrazione Trump dichiara sostanzialmente di non aver ancora individuato la direzione da adottare per risolvere i conflitti tra diritti degli sviluppatori e degli autori, e al momento richiede al Congresso di non legiferare in materia e di attendere gli sviluppi della giurisprudenza**: «*Although the Administration believes that training of AI models on copyrighted material does not violate copyright laws, it acknowledges arguments to the contrary exist and therefore supports allowing the Courts to resolve this issue. Similarly, Congress should not take any actions that would impact the judiciary's resolution of whether training on copyrighted material constitutes fair use*».

Il **quarto** pilastro tematico (*Preventing Censorship and Protecting Free Speech*) è un capolavoro letterario di rovesciamento di significato: cela le politiche di censura governativa e di soppressione della libera manifestazione del pensiero già espresse e formalmente dichiarate dall'amministrazione Trump, intestandole alla prevenzione della censura e alla protezione del *free speech*. Ci riferiamo in particolare al "Piano di azione americano sulla IA"

ISSN 2239-8570

del 23.7.205 e al coevo *executive order* dal titolo "*Preventing Woke AI in the Federal Government*". Con il primo intervento, l'Amministrazione Trump ha richiesto *inter alia*, al Dipartimento del Commercio di modificare il *National Institute of Standards and Technology AI Risk Management Framework* al fine di «**eliminare riferimenti al cambiamento climatico e ad iniziative DEI** [Diversità Equità Inclusione]», e ha istruito le agenzie federali affinché esse si approvvigionino soltanto di large language models (LLMs) che siano «*objective and free from topdown ideological bias*» (v. *amplius* il contributo n. 2 nel numero 3/2025 [2025/3(2)SO] in *PeM* 2025, p. 1020). Similmente, l'*executive order* dall'eloquente titolo "*Preventing Woke AI in the Federal Government*" si diffonde sui **requisiti ideologici** dei sistemi di IA di cui al coevo Piano, sopra richiamato, richiedendo alle agenzie federali di attenersi a due c.d. «*Unbiased AI Principles*» (la «ricerca della verità» e la «neutralità ideologica») in particolare **vietando applicazioni IA che possano «manipolare le risposte favorendo dogmi ideologici come DEI»** (v. *amplius* il contributo n. 2 nel numero 3/2025 [2025/3(2)SO] in *PeM* 2025, p. 1020).

I rimanenti tre pilatri tematici del Documento - il **quinto**, il **sesto** e il **settimo** - sono assolutamente in linea con gli *executive orders* e gli altri atti di indirizzo già emanati nel corso degli ultimi mesi dal Presidente Trump (**POTUS**), che riassumiamo qui di seguito:

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

ISSN 2239-8570

amplius il contributo n. 2 nel numero 3/2025 [2025/3(2)SO] in *PeM* 2025, p. 1020);

- il già citato executive order emesso dal POTUS il 23.7.2025 dal titolo "*Preventing Woke AI in the Federal Government*" (il **Bias EO**) coevo al Piano di azione americano sulla IA, che si diffonde sui requisiti ideologici dei sistemi di IA di cui al medesimo Piano, come già sopra ricordato, e che inoltre prevede una serie dettagliata di policy recommendations per **snellire i procedimenti autorizzativi e facilitare lo sviluppo di data centers** e altre infrastrutture e per **«esportare la IA americana» a «partner e alleati degli Stati Uniti»** (v. *amplius* il contributo n. 2 nel numero 3/2025 [2025/3(2)SO] in *PeM* 2025, p. 1020);
- l'executive order del 24.11.2025 intitolato "Launching the Genesis Mission" (**Genesis Mission EO**) e
- l'executive order dell' 11.12.2025 intitolato "Ensuring a National Policy Framework for Artificial Intelligence" (**Policy Framework EO**).

Questi ultimi due ordini esecutivi (sui quali v. *amplius* in questa rubrica il contributo n. 1 del numero 4/2025 [2025/4(1)SO] in *PeM* 2025, p. 1019) sono coerenti con i contenuti del Documento di cui hanno anticipato in particolare i pilastri tematici quinto, sesto e settimo.

SALVATORE ORLANDO

National Policy Framework

2026/2(13)FC
Il controllo governativo preventivo dei *frontier models* negli USA: l'Executive Order n. 14409 (*Promoting Advanced Artificial Intelligence Innovation and Security*) del 2.6.2026 e le altre misure adottate dall'amministrazione Trump nel mese di giugno 2026 a proposito dei modelli Fable 5 e Mythos 5 di Anthropic e del modello GPT.5-6 di Open AI

Nel mese di giugno 2026 l'Amministrazione Trump ha adottato una serie di misure, intestate ad **esigenze di sicurezza nazionale**, che segnano **un primo mutamento dell'approccio statunitense alla regolazione dei modelli di intelligenza artificiale avanzata,** e che prevedono l'intervento delle autorità pubbliche alla fase antecedente alla loro distribuzione.
I principali interventi adottati dall'Amministrazione statunitense nel corso del mese di giugno 2026, più sotto commentati, possono essere sinteticamente ricostruiti nei termini che seguono:

- il **2 giugno 2026,** con l'**Executive Order n. 14409** (*Promoting Advanced Artificial Intelligence Innovation and Security*) il Presidente degli Stati Uniti d'America (**POTUS**) ha disposto l'istituzione di un quadro di cooperazione volontaria tra le autorità federali competenti e gli sviluppatori dei c.d. *covered frontier models*. In particolare, la Section 3 introduce un

ISSN 2239-8570

meccanismo di valutazione preventiva dei modelli di intelligenza artificiale avanzata. A tal fine, la **Section 3(a)** demanda alle competenti autorità federali l'elaborazione di un *classified benchmarking process* volto a individuare i modelli suscettibili di presentare rischi per la sicurezza nazionale e a verificarne l'eventuale riconducibilità alla categoria dei *covered frontier models*. Sulla base di tale processo, **la Section 3(b)** prevede l'istituzione di un *voluntary framework* nell'ambito del quale gli sviluppatori possono consentire alle autorità federali l'accesso ai modelli fino a trenta giorni prima della loro diffusione a soggetti terzi, al fine di permettere lo svolgimento di attività di valutazione preventiva dei rischi individuati dal *classified benchmarking process*. Il sistema così delineato conserva, tuttavia, carattere esclusivamente volontario, poiché la **Section 3(c)** precisa espressamente che esso non introduce alcun regime obbligatorio di autorizzazione preventiva (*preclearance*), di licenza o di altra forma di approvazione preventiva quale condizione per lo sviluppo, il rilascio o la distribuzione dei modelli di intelligenza artificiale.

- Il **12 giugno 2026,** il Governo degli Stati Uniti d'America (il **Governo**), per il tramite del proprio *Department of Commerce* (il **Dipartimento**), ha adottato una direttiva con la quale ha disposto **la sospensione dell'accesso** ai modelli di intelligenza artificiale avanzata *Fable 5* e *Mythos 5*, sviluppati dalla società **Anthropic**, nei confronti di tutti i soggetti privi della cittadinanza statunitense, anche se presenti sul territorio degli Stati Uniti, inclusi i dipendenti della stessa società di nazionalità straniera (la **Direttiva Anthropic**). Secondo quanto emerge dalle comunicazioni ufficiali diffuse da Anthropic - atteso che il testo della direttiva non risulta, allo stato, pubblicamente disponibile - la misura sarebbe stata adottata nell'esercizio dei poteri attribuiti al Dipartimento in materia di *export controls,* invocando esigenze riconducibili alla tutela della sicurezza nazionale, con particolare riguardo ai rischi derivanti dalle capacità avanzate dei modelli e dalla possibile elusione dei meccanismi di sicurezza predisposti per limitarne utilizzi impropri (c.d. ***jailbreaking***). L'attuazione della Direttiva Anthropic ha evidenziato la criticità, rappresentata dalla stessa Anthropic, dell'impossibilità di verificare in modo tempestivo e sufficientemente affidabile la cittadinanza degli utenti autorizzati ad accedere ai modelli, circostanza che ha indotto la società a **sospenderne temporaneamente l'accesso per tutti gli utenti**.
- Il **26 giugno 2026**, OpenAI ha annunciato, attraverso i propri canali ufficiali, di aver limitato il rilascio iniziale del modello **GPT-5.6** ad un ristretto numero di *trusted partners*, su richiesta dell'Amministrazione statunitense. Secondo quanto dichiarato dalla società, la misura, di carattere temporaneo, era finalizzata a consentire alle autorità federali di completare la valutazione del modello sotto il profilo della sicurezza nazionale e della cybersicurezza, nell'ambito del quadro delineato dall'Executive Order del 2 giugno 2026. Allo stato, tuttavia, non risulta pubblicato alcun provvedimento amministrativo che formalizzi tale richiesta, né sono noti il relativo fondamento giuridico, i criteri di individuazione dei *trusted partners* o le modalità attraverso le quali l'Amministrazione abbia esercitato tale

ISSN 2239-8570

interlocuzione. Successivamente, la stessa OpenAI ha annunciato il progressivo ampliamento dell'accesso al modello.

- Il **30 giugno 2026** il Dipartimento ha revocato i controlli all'esportazione applicati ai modelli *Fable 5* e *Mythos 5* sulla base della Direttiva Anthropic. Secondo quanto riportato da fonti di stampa sulla base di una lettera del Segretario al Commercio degli Stati Uniti Howard Lutnick - successivamente confermata da Anthropic mediante un comunicato ufficiale - il Dipartimento ha disposto la revoca dei controlli all'esportazione applicati ai modelli *Fable 5* e *Mythos 5*, in considerazione dell'adozione, da parte della società, di misure di mitigazione del rischio. Tale decisione ha determinato dunque **la cessazione degli effetti** della Direttiva Anthropic del 12 giugno 2026 e ha consentito il progressivo ripristino dell'accesso ai modelli.

Come detto, l'Executive Order del 2 giugno 2026 segna un primo mutamento dell'approccio statunitense alla regolazione dei modelli di intelligenza artificiale avanzata, anticipando l'intervento delle autorità pubbliche alla fase antecedente alla loro distribuzione. Il fulcro del nuovo modello non risiede nell'introduzione di limiti all'impiego dei sistemi di intelligenza artificiale già immessi sul mercato, bensì **nell'istituzionalizzazione di un meccanismo di valutazione preventiva dei rischi**, attraverso il quale la sicurezza nazionale diviene un parametro rilevante già nella fase di sviluppo e di pre-rilascio dei *frontier models*. Nel quadro delineato dall'Executive Order del 2 giugno 2026 si colloca la vicenda concernente il rilascio del modello **GPT-5.6** sviluppato da OpenAI. L'episodio concernente il rilascio del modello *GPT-5.6* appare di particolare interesse non tanto per il temporaneo differimento della sua diffusione, quanto per le modalità attraverso le quali l'Amministrazione statunitense sembra aver perseguito gli obiettivi di sicurezza nazionale delineati dall'Executive Order del 2 giugno 2026. Pur in assenza di un provvedimento formalmente adottato e pubblicamente conoscibile, l'interlocuzione tra autorità pubbliche e sviluppatore ha infatti inciso in maniera significativa sulle modalità e sui tempi di distribuzione del modello. A differenza della successiva vicenda Anthropic, infatti, **non emerge l'adozione di un provvedimento amministrativo formalmente vincolante,** bensì una richiesta rivolta allo sviluppatore, alla quale OpenAI ha spontaneamente aderito, limitando il rilascio iniziale del modello. Tale circostanza assume rilievo sotto un duplice profilo. Da un lato, essa conferma come il modello delineato dall'Executive Order trovi una prima applicazione concreta attraverso forme di interlocuzione diretta tra autorità pubbliche e sviluppatori dei modelli avanzati. Dall'altro, evidenzia come il perseguimento di esigenze di sicurezza nazionale possa realizzarsi anche **in assenza dell'esercizio di poteri autoritativi, mediante strumenti di cooperazione** che, pur privi di una veste provvedimentale di carattere formale, **risultano idonei ad orientare le modalità di rilascio dei modelli**. In conclusione, pur in assenza di un provvedimento formalmente vincolante, l'interlocuzione con l'Amministrazione ha determinato **un concreto differimento delle modalità di rilascio del modello**, incidendo sull'attività dell'operatore economico senza ricorrere all'esercizio di poteri coercitivi. Sotto tale profilo, il caso OpenAI si inscrive in un modello di ***soft regulation*.** Infatti, più che un esempio di esercizio del potere amministrativo, la fattispecie sembra

ISSN 2239-8570

rappresentare una forma di **regolazione cooperativa,** nella quale il perseguimento di obiettivi pubblici viene affidato, almeno sul piano formale, non all'imposizione di obblighi giuridici, bensì alla collaborazione tra amministrazione e operatori economici.

Resta tuttavia aperto l'interrogativo se tale cooperazione sia effettivamente espressione di una libera adesione del destinatario ovvero se il significativo squilibrio istituzionale tra autorità pubblica e operatore economico finisca, di fatto, per attribuire alla richiesta governativa un'efficacia conformativa non dissimile da quella di un atto autoritativo. La fondatezza di tale interrogativo emerge con ancora maggiore evidenza dal raffronto tra il caso OpenAI e quello concernente Anthropic. Se, nel caso OpenAI, l'intervento governativo sembra essersi sviluppato nell'ambito di un modello di regolazione cooperativa, coerente con l'impostazione delineata dall'Executive Order del 2 giugno 2026, **la misura adottata nei confronti di Anthropic costituisce, invece, un intervento autoritativo, riconducibile alla disciplina statunitense dei controlli all'esportazione.**

Particolarmente significativo appare, infatti, l'oggetto stesso della misura. La direttiva:

- non riguardava il trasferimento di componenti *hardware*, infrastrutture di calcolo, *model weights* o altre tecnologie tradizionalmente assoggettate alla disciplina dei controlli all'esportazione, bensì l'accesso remoto ai modelli di intelligenza artificiale *Fable 5* e *Mythos 5*, distribuiti da Anthropic secondo il modello *AI-as-a-Service*;
- individuava i destinatari secondo un criterio personale, anziché territoriale, trovando applicazione anche nei confronti dei soggetti non aventi cittadinanza statunitense indipendentemente dal luogo in cui essi si trovassero;
- era motivata, secondo quanto comunicato da Anthropic, dalle preoccupazioni dell'Amministrazione circa l'impossibilità, per la società, di verificare in modo tempestivo e sufficientemente affidabile la cittadinanza degli utenti autorizzati ad accedere ai modelli.

Proprio tale circostanza ha indotto Anthropic a sospendere temporaneamente l'accesso ai modelli per tutti gli utenti, procedendo al progressivo ripristino del servizio soltanto dopo il ritiro dei controlli all'esportazione disposto dal Department of Commerce il 30 giugno 2026. Al fine di assicurare l'immediata osservanza della direttiva, la società ha quindi disabilitato integralmente Fable 5 e Mythos 5 per **tutti gli utenti**.

La vicenda evidenzia come un provvedimento formalmente circoscritto ai soggetti non aventi cittadinanza statunitense possa produrre, nella pratica, effetti generalizzati sull'accessibilità dei modelli, quale conseguenza delle caratteristiche tecniche della piattaforma di distribuzione. Rimangono, tuttavia, non conoscibili, in assenza della pubblicazione della direttiva, il percorso decisionale seguito dall'Amministrazione, i presupposti tecnico-fattuali posti a fondamento della misura e gli elementi istruttori che hanno condotto a qualificare i modelli *Fable 5* e *Mythos 5* come suscettibili di compromettere la sicurezza nazionale. **Anthropic ha contestato la ricostruzione dell'Amministrazione,** sostenendo che le vulnerabilità richiamate riguardavano esclusivamente tecniche già note, di limitata

ISSN 2239-8570

rilevanza e comunque individuabili anche in altri modelli concorrenti di intelligenza artificiale già liberamente disponibili sul mercato. La società ha inoltre evidenziato come il Governo non aveva fornito elementi tecnici dettagliati né dimostrato l'esistenza di una effettiva *universal jailbreak*, ossia di una tecnica idonea ad eludere le misure di sicurezza del modello. **Solo a seguito dell'adozione**, da parte della società, **di ulteriori misure di mitigazione del rischio,** il Dipartimento ha disposto il ritiro dei controlli all'esportazione applicati ai modelli *Fable 5* e *Mythos.*

Di particolare interesse è il profilo concernente il fondamento giuridico della direttiva. In assenza della pubblicazione del provvedimento, non è possibile individuare con certezza la base normativa sulla quale il Dipartimento ha fondato il proprio intervento. Tuttavia, sia la qualificazione dell'atto come *export control directive*, sia il successivo ritiro dei controlli all'esportazione disposto il 30 giugno 2026, inducono ragionevolmente a ritenere che la misura sia stata adottata nell'esercizio dei poteri attribuiti al Dipartimento dalla disciplina statunitense in materia di controlli all'esportazione, e in particolare dall'***Export Control Reform Act*** **(ECRA)** e dalle relative ***Export Administration Regulations*** **(EAR)**. Se tale ricostruzione fosse corretta, la direttiva costituirebbe la prima applicazione pubblicamente nota di tali strumenti ad un modello di intelligenza artificiale avanzata distribuito come servizio, anziché al trasferimento di beni o tecnologie tradizionalmente soggetti ai regimi di esportazione. Nel caso di specie, invece, l'oggetto della restrizione non sembra essere il trasferimento della tecnologia in senso tradizionale, bensì l'accesso remoto alle capacità offerte da un modello di intelligenza artificiale distribuito mediante infrastrutture cloud. **L'"esportazione" tende così a coincidere non più con la circolazione materiale della tecnologia, ma con la possibilità stessa di fruirne da remoto.**

Nel complesso, la successione degli interventi adottati nel corso del mese di giugno 2026 evidenzia una significativa tensione interna al nuovo modello statunitense di regolazione dei *frontier models*. A soli dieci giorni dall'adozione dell'Executive Order del 2 giugno 2026, che fonda la gestione dei rischi sull'adesione volontaria degli sviluppatori ad un sistema di cooperazione preventiva con le autorità pubbliche, **il Department of Commerce è ricorso ad una export control directive** formalmente vincolante, limitando direttamente l'accesso a specifici modelli di intelligenza artificiale avanzata. La fattispecie sembra così dimostrare come, nell'ordinamento statunitense, gli strumenti di cooperazione e quelli autoritativi non costituiscano modelli alternativi, **bensì strumenti tra loro complementari, suscettibili di essere impiegati in funzione dell'intensità del rischio percepito per la sicurezza nazionale.**

Gli interventi dell'Amministrazione sollevano, altresì, rilevanti questioni sotto il profilo delle garanzie procedimentali. Allo stato, infatti, non è possibile verificare i criteri utilizzati per qualificare i modelli *Fable 5* e *Mythos 5* quali tecnologie suscettibili di compromettere la sicurezza nazionale, né valutare la proporzionalità e la ragionevolezza dell'intervento, non essendo stati pubblicati né il testo della direttiva né i presupposti tecnico-giuridici che ne hanno giustificato l'adozione. Secondo quanto emerge dalle

ISSN 2239-8570

informazioni disponibili, la misura è stata infatti comunicata ad Anthropic mediante una lettera riservata (*private directive letter*), mai resa pubblica. Tale circostanza pone, più in generale, interrogativi circa la trasparenza, la sindacabilità e il controllo giurisdizionale di misure adottate nell'esercizio dei poteri statali in materia di sicurezza nazionale.
Sotto entrambi i profili trattati, gli atti dell'Amministrazione statunitense confermano una progressiva qualificazione dei *frontier models* quali tecnologie strategiche, suscettibili di essere assoggettate a limitazioni analoghe a quelle previste per altre tecnologie rilevanti ai fini della sicurezza nazionale. Il controllo pubblico non riguarda, infatti, la conformità del modello o le modalità del suo utilizzo, bensì l'accesso stesso alle sue capacità computazionali. Da ultimo, la decisione di Anthropic di sospendere temporaneamente l'accesso ai modelli per tutti gli utenti, motivata dall'impossibilità tecnica di verificare con immediatezza la nazionalità dei destinatari, dimostra come provvedimenti nazionali possano determinare effetti sostanzialmente globali quando applicati a servizi digitali distribuiti attraverso infrastrutture cloud, ponendo nuove questioni in ordine ai rapporti tra sicurezza nazionale, sovranità statale e circolazione transfrontaliera dei servizi di intelligenza artificiale.

FIAMMA CONCARELLA

Executive order 14409
Statement on the US government directive to suspend access to Fable 5 and Mythos 5
Anteprima di GPT-5.6

2026/2(14)MT
Il progetto argentino di riforma del diritto societario del 29.5.2026: la nuova *Ley General de Sociedades* tra «società automatizzate» e DAO

Il 29 maggio 2026, il *Poder Ejecutivo Nacional* ha trasmesso al Congresso argentino un progetto di legge che propone l'abrogazione integrale della *Ley de Sociedades Comerciales* (*Ley* n. 19.550, vigente dal 1972) e la sua sostituzione con una nuova *Ley General de Sociedades*.
Il progetto si connota per il tentativo, esplicitamente dichiarato, di facilitare l'attività delle imprese, semplificare le norme e adattare il sistema societario alle innovazioni tecnologiche.
Quanto all'impostazione della *Ley General de Sociedades*, in estrema sintesi, possono individuarsi alcune principali direttrici di intervento. In primo luogo, può osservarsi l'ampliamento della sfera di autonomia riservata ai soci nello stabilire l'organizzazione interna, le funzioni e le modalità di funzionamento delle società. Tale ampliamento supera la tradizionale impostazione della vigente *Ley de Sociedades Comerciales*, tradizionalmente interpretata come disciplina a carattere imperativo, attribuendo alla legge, nel progetto di riforma, una funzione prevalentemente suppletiva (ad eccezione di specifiche norme imperative).

ISSN 2239-8570

In secondo luogo, il progetto modifica l'impostazione precedente anche con riferimento alla disciplina della responsabilità degli amministratori e dell'oggetto sociale. Si presume, infatti, la buona fede delle decisioni gestorie, purché assunte in modo informato e in assenza di conflitto di interessi, con possibile attenuazione della responsabilità civile degli amministratori. Al contempo, si rileva una maggiore flessibilità dell'oggetto sociale, che può essere ampio, plurimo e persino indeterminato, ove lo statuto non lo definisca.
In terzo luogo, **la *Ley General de Sociedades* accentua la digitalizzazione della vita societaria, attraverso firme digitali, domicili elettronici, libri digitali e procedimenti interamente da remoto**.
Ancora, in materia di tipi di società, il progetto semplifica il sistema, riducendolo a cinque tipi societari: la società semplice, la società a responsabilità limitata, la società anonima, la società per azioni semplificata, nonché l'innovativa *Sociedad Descentralizada Autónoma Operativa* (DAO).
Tra i profili più qualificanti della riforma, meritevoli di approfondimento, vi è l'esplicito riconoscimento che **la società possa operare mediante sistemi algoritmici autonomi o agenti di intelligenza artificiale**.
In particolare, il progetto argentino introduce, all'art. 14 delle *Disposiciones Generales*, la figura della ***Sociedad Automatizada* (società automatizzata), configurata non come autonomo tipo societario, ma come qualificazione riferibile a una società appartenente a uno qualsiasi dei tipi previsti dalla legge, allorché essa persegua il proprio oggetto sociale mediante sistemi algoritmici autonomi o agenti di intelligenza artificiale, senza richiedere, per la propria operatività ordinaria, l'impiego di lavoratori subordinati né, più in generale, di risorse umane**. In tale prospettiva, la qualificazione di "automatizzazione" deve risultare espressamente dallo statuto e la denominazione sociale deve contenere l'espressione "*automatizada*".
La disposizione assume rilievo in quanto prende in considerazione l'ipotesi, ormai non più soltanto teorica, di un'impresa nella quale l'organizzazione produttiva non si fondi stabilmente su una struttura "umana", bensì su un'infrastruttura computazionale. In tale prospettiva, l'algoritmo non assurge al rango di soggetto di diritto, né diviene titolare di un'autonoma sfera patrimoniale, dovendosi unicamente intendere quale strumento attraverso cui la società svolge la propria attività.
Coerentemente, lo stesso art. 14 stabilisce che **la società automatizzata risponde con il proprio patrimonio nei confronti dei terzi per i danni causati dai sistemi algoritmici autonomi o dagli agenti di intelligenza artificiale**. L'attività materialmente svolta dal sistema o dall'agente, dunque, resta attività della società, con la conseguenza che i danni derivanti dalla stessa vengono riferiti al patrimonio sociale. La disposizione sembra così voler esplicitamente escludere l'argomento, talvolta evocato in termini suggestivi, secondo cui l'autonomia tecnica del sistema potrebbe determinare una zona di irresponsabilità.
Su un piano diverso, ma complementare, si colloca l'art. 102, dedicato ai **sistemi di intelligenza artificiale nella gestione. La norma consente all'organo amministrativo di utilizzare sistemi di IA o algoritmi per l'esecuzione di funzioni operative o per l'adozione di decisioni. Tuttavia, il loro impiego non esclude o limita la responsabilità degli**

ISSN 2239-8570

amministratori, né costituisce esimente rispetto al dovere di configurazione e supervisione del sistema e dei relativi risultati.

Ulteriore aspetto che rende il progetto di riforma del diritto societario argentino di particolare interesse riguarda la decisione di **affrontare normativamente il fenomeno delle organizzazioni autonome decentralizzate, o secondo la prevalente denominazione anglosassone *Decentralized Autonomous Organizations* (DAO)**. Si tratta di forme organizzative la cui crescente diffusione pone rilevanti problemi in termini di qualificazione giuridica, imputazione degli atti, responsabilità dei partecipanti e disciplina applicabile. Solo alcuni ordinamenti hanno scelto di regolare espressamente tali organizzazioni. In ordinamenti come quello italiano, allo stato, manca una disciplina organica delle DAO, mentre altri Stati hanno iniziato a sperimentare forme di riconoscimento normativo, come avvenuto, tra gli altri, a Malta, Abu Dhabi, nelle Isole Cayman e, negli Stati Uniti, in Vermont, Wyoming, Colorado, Tennessee, Utah e New Hampshire (sulla legge dello Stato del Wyoming del 21 aprile 2021 v. in questa Rubrica il contributo n. 12 nel numero 4/2021 [2021/4(12)BC] in *Atlante*, p. 138, in *PeM* 2021, p. 905). Il progetto di *Ley General de Sociedades* affronta tale tematica prevedendo – agli artt. da 258 a 265 – **l'introduzione di un nuovo tipo sociale, la *Sociedad Descentralizada Autónoma Operativa***, mutuando, sotto diversi profili (*inter alia*, rappresentanza legale, personalità giuridica e specifiche cause di scioglimento), la disciplina dettata dalla *DAO Model Law* della *Coalition of Automated Legal Applications* (COALA, 2021).

In particolare, **l'art. 258 qualifica la DAO come tipo societario, prevedendo che essa possa essere strutturata in modo totalmente o parzialmente autonomo e decentralizzato**, in conformità alle regole di organizzazione interna, alle funzioni e alle modalità di funzionamento stabilite nell'atto costitutivo o nel **protocollo**. Quest'ultimo è definito – con terminologia volutamente ampia, idonea a comprendere le varie esperienze che si riscontrano nella realtà "*on-chain*" – come l'**insieme delle regole tecniche e di *governance* che determinano il funzionamento della DAO, indipendentemente dalla tecnologia o dal supporto (tecnico e tecnologico) utilizzato**.

La disposizione, peraltro, chiarisce esplicitamente che **non possono qualificarsi in termini di DAO le società che si limitino a utilizzare la tecnologia per finalità meramente strumentali o amministrative, senza che essa incida in modo essenziale sulla struttura organizzativa o sui meccanismi di *governance***. In sostanza, oltre a individuarne il perimetro definitorio, la *Ley General de Sociedades* detta una norma di principio a garanzia della conformità della *Sociedad Descentralizada Autónoma Operativa* ai caratteri strutturali – in termini di decentramento e applicazioni tecnologiche – del fenomeno DAO. Merita rilievo, peraltro, l'esplicito rinvio, per eventuali applicazioni analogiche e suppletive, alla disciplina della *Sociedad por Acciones Simplificada*, oltre che a quella contenuta nelle *Disposiciones Generales*.

L'art. 259, in materia di partecipazioni, chiarisce che queste possono essere rappresentate da titoli, *token* o gettoni crittografici emessi su *distributed ledger technology* (DLT) o altre applicazioni tecnologiche, e

ISSN 2239-8570

possono anche essere prive di valore nominale. L'acquisto e il trasferimento avvengono mediante registrazione nella DLT o nel sistema tecnologico dichiarato dalla società, senza necessità di ulteriori formalità, purché il sistema ne garantisca la tracciabilità.

Risolvendo l'annoso dilemma della rappresentanza delle DAO nel mondo "*off-chain*", **l'art. 260 impone che la rappresentanza legale sia attribuita a una o più persone fisiche chiamate a rappresentare la DAO nei suoi rapporti con i terzi e a compiere gli atti che richiedono l'intervento umano**. In sostanza, la norma supera quelle difficoltà che più volte sono state evidenziate in dottrina e che hanno spinto molti, tra studiosi e sviluppatori di DAO, a immaginare il collegamento tra DAO e mondo esterno mediante un *legal wrapper*.

Con riferimento all'atto costitutivo, l'art. 261 statuisce che esso sia formato e iscritto secondo le regole previste in termini generali per tutte le società (artt. 6, 7 e 8 del progetto di riforma), indicando, tra l'altro, il promotore, il rappresentante legale, la denominazione, il domicilio, la sede, l'identificazione del protocollo o dello *smart contract*, e la determinazione dell'oggetto sociale.

Particolarmente significativa è la previsione di cui all'**art. 261, n. 7), secondo cui l'acquisto o il trasferimento delle partecipazioni sociali deve avvenire solo con modalità idonee ad assicurare la conoscibilità dell'identità del relativo titolare**. La norma, nelle sue implicazioni pratiche, merita di essere posta in adeguato rilievo, **risolvendo *ex lege* il problema dell'identità dei detentori dei *token* di partecipazione delle DAO**. Infatti, come si è avuto modo di vedere in esperienze giurisprudenziali straniere (tra tutte, la ben nota pronuncia della *Southern District Court* della California, *Sarcuni v. bZx DAO*, del 27 marzo 2023), la natura stessa della tecnologia *blockchain* assicura l'anonimato ai detentori dei *token* di partecipazione, con tutte le implicazioni, *ex multis* in materia di responsabilità, che ne derivano.

Proprio al tema della responsabilità è dedicato l'art. 262 del progetto di legge in commento. Tale disposizione delinea un sistema di imputazione degli effetti giuridici in forza del quale la DAO risponde con il proprio patrimonio per le obbligazioni assunte e per i danni cagionati nello svolgimento della sua attività, ivi compresi quelli derivanti da operazioni eseguite automaticamente dal protocollo. Lo stesso art. 262 individua, inoltre, il regime di responsabilità cui sono soggetti il rappresentante legale e il promotore della DAO. Il primo, in particolare, è responsabile secondo il regime previsto dall'art. 257, che, relativamente alla *Sociedad por Acciones Simplificada*, dispone che i rappresentanti rispondono esclusivamente per i danni derivanti da dolo, abuso dei propri poteri, ovvero da violazione della legge, dello statuto o delle istruzioni impartite dall'organo competente. Il promotore – tipicamente, per le DAO, si tratta di uno o più sviluppatori che creano la piattaforma, composta da *smart contract* implementati su reti *blockchain*, e che, coerentemente, l'art. 261, n. 1), definisce come la persona che sottoscrive l'atto costitutivo, promuove e cura la costituzione della *Sociedad Descentralizada Autónoma Operativa* –, invece, risponde illimitatamente e solidalmente per le obbligazioni contratte ai fini della costituzione e dell'iscrizione della DAO,

ISSN 2239-8570

salvo liberazione a seguito dell'iscrizione e dell'assunzione delle obbligazioni stesse da parte della società.
Quanto agli aspetti pubblicitari e documentali, gli artt. 263-264 prevedono che **i registri digitali possano sostituire tutti i supporti fisici, a condizione che siano pubblicamente verificabili, riproducibili in formato leggibile e idonei a consentire la ricostruzione della situazione patrimoniale della DAO**.
Un ulteriore indice di come il fatto tecnico divenga fatto rilevante per il diritto societario, si evince, infine, dall'art. 265, il quale **prevede specifiche cause di scioglimento della DAO connesse all'irreversibile impossibilità tecnica di eseguire il protocollo, alla perdita definitiva di accesso al protocollo o allo *smart contract*, nonché alla modifica del protocollo idonea a eliminare i meccanismi di identificazione dei membri**.
In conclusione, appare evidente come il progetto di legge argentino si candidi a divenire uno dei tentativi più innovativi di modernizzazione del diritto societario. Con particolare riferimento alle DAO, tuttavia, resta da verificare se un modello così costruito sarà in grado di attrarre effettivamente le DAO più radicalmente decentralizzate, le quali potrebbero percepire l'identificazione dei titolari e la presenza di rappresentanti umani come un arretramento rispetto alla logica originaria del fenomeno.

MATTEO TARASCHI

Testo ufficiale

2026/2(15)IG
L'annuncio del governo del Regno Unito del progetto di vietare l'accesso ai social media ai minori di anni 16

Con un comunicato stampa del 15 giugno 2026, il Primo Ministro britannico Keir Starmer ha annunciato di voler introdurre un divieto generalizzato di accesso alle piattaforme di social media per i minori di sedici anni, sul rilievo che tali servizi «rendono i bambini infelici», li espongono a contenuti dannosi o pericolosi e sono «progettati per creare dipendenza». La misura è destinata a riguardare le piattaforme di interazione sociale, quali **Snapchat, TikTok, YouTube, Instagram, Facebook e X**, con esclusione dei servizi di messaggistica quali WhatsApp, ma sono state prospettate ulteriori misure, quali il blocco delle funzioni di *livestreaming* e della comunicazione tra minori ed estranei, destinate ad essere applicate ad una più ampia gamma di servizi on line, compresi i siti di gioco.
L'iniziativa del governo si ispira all'esperienza australiana. Con l'*Online Safety Amendment* (*Social Media Minimum Age*) *Act* 2024, che ha modificato l'*Online Safety Act* 2021, l'Australia è stata infatti il primo Paese a vietare l'accesso ai social ai minori di sedici anni (v. in questa Rubrica, il contributo n. 53 del numero 4/2024 [2024/4(53)RRa], in PeM 2024, p. 1570), ma si inserisce in un trend che sta interessando diversi ordinamenti. Così l'Indonesia, che dal marzo 2026 applica un analogo divieto per i minori di 16

ISSN 2239-8570

anni e il Canada, il cui progetto di legge sulla sicurezza digitale, presentato recentemente, mira a precludere ai minori di 16 anni la titolarità di account social, imponendo altresì ai chatbot fondati sull'intelligenza artificiale limiti alla produzione di contenuti dannosi. Altri Stati, come la Francia, la Spagna (v. in questa Rubrica, il contributo n. 18 del numero 4/2025 [2025/4(18)RR], in PeM 2025, p. 1088), la Danimarca e la Corea del Sud hanno annunciato l'intenzione di adottare misure analoghe.
Si tratta di un modello regolatorio radicale, la cui introduzione solleva alcune questioni. Viene in rilievo la difficoltà applicativa di tale divieto, considerando anche l'esigenza di approntare sistemi di verifica dell'età proporzionati e non lesivi della privacy degli utenti. Si pone inoltre il tema del bilanciamento tra l'esigenza di protezione del minore e quella della sua autodeterminazione, che include la libertà, per il minore capace di discernimento, di accedere a uno spazio ormai divenuto sede di esercizio di diritti e di sviluppo della personalità. Si è inoltre osservato che un divieto d'accesso incentrato sull'età potrebbe distogliere l'attenzione dagli interventi sulla progettazione delle piattaforme, che mirano ad escludere o comunque mitigare all'origine rischi suscettibili di incidere non solo sui soli minori, ma sulla generalità degli utenti e, in particolare, sulla categoria di soggetti vulnerabili a prescindere dall'età.

ILARIA GARACI

Press release

2026/2(16)IG
L'iniziativa del governo norvegese di vietare l'IA generativa nelle scuole per gli alunni da 6 a 13 anni e di consentirla agli alunni da 14 a 16 anni solo con supervisione degli insegnanti: la protezione del minore si sposta sul livello cognitivo

Il Primo Ministro norvegese Jonas Gahr Støre ha annunciato, in una conferenza stampa del 19 giugno 2026, che, a partire dal nuovo anno scolastico, il Governo limiterà significativamente l'impiego degli strumenti di intelligenza artificiale generativa nelle scuole. In particolare, per gli studenti di età inferiore ai tredici anni è previsto un divieto generalizzato di utilizzo; per le fasce successive l'uso è subordinato alla supervisione degli insegnanti (studenti dai quattordici ai sedici anni) ovvero ricondotto a percorsi progressivi di educazione critica (studenti dai diciassette ai diciannove anni). La ratio dell'intervento, come dichiarato dallo stesso Primo Ministro, risiede nella necessità di garantire lo **sviluppo delle competenze cognitive fondamentali** dei più giovani, che si teme possa essere compromesso da un impiego precoce e non guidato di tali sistemi. La misura, che, differenziando l'intervento per fasce d'età, gradua la restrizione sulla capacità evolutiva del minore, muove dalla consapevolezza dell'emersione di una nuova categoria di rischio: quella della cosiddetta **«delega cognitiva precoce»**, suscettibile di tradursi in un mancato sviluppo o comunque indebolimento delle capacità

ISSN 2239-8570

cognitive. Affidare alla macchina attività complesse, ordinariamente rimesse alla mente umana, come **la scrittura, la sintesi, la risoluzione di problemi**, comporta il rischio che lo studente non sviluppi tali capacità, con pregiudizio per il **pensiero critico e autonomo** e pertanto per la sua **capacità di autodeterminazione**.
L'iniziativa si inserisce nel solco di una strategia nazionale più ampia, volta a governare in modo più sostenibile l'ambiente digitale e, in particolare, quello scolastico. Si consideri, da un lato, il divieto degli smartphone nelle aule introdotto nel 2024 e l'annunciato ritorno al libro cartaceo e alla scrittura manuale, in controtendenza rispetto alla massiccia digitalizzazione degli ultimi decenni; dall'altro, il disegno di legge, atteso in Parlamento entro la fine del 2026, volto a fissare a sedici anni la soglia d'accesso ai social media. Quest'ultima previsione segue, peraltro, l'esempio dell'Australia, che con l'*Online Safety Amendment* (*Social Media Minimum Age*) *Act* 2024 è stata il primo Paese a vietare l'accesso ai social ai minori di sedici anni, e si allinea a un orientamento che sta interessando diversi altri paesi (v. *supra* in questa Rubrica, il contributo che precede).
La misura di limitare l'impiego dei sistemi di IA generativa nelle scuole lascia, nondimeno, intendere la necessità di introdurre nuovi parametri di conformità dei prodotti digitali e, in particolare, dei sistemi di intelligenza artificiale generativa, **non più soltanto circoscritti alla sicurezza o alla liceità dei contenuti, ma estesi anche alla loro compatibilità con le finalità educative e con lo sviluppo progressivo delle capacità del minore**.

ILARIA GARACI

Press release

2026/2(17)RA
L'annullamento della designazione di Meta come *gatekeeper* per Marketplace ai sensi del Digital Services Act (Tribunale UE, causa T-1078/23)

Con sentenza del 3 giugno 2026, resa nella causa T-1078/23, il Tribunale dell'Unione europea ha parzialmente accolto il ricorso proposto da Meta Platforms Inc. (**Meta**) avverso la decisione del 5 settembre 2023 con cui la Commissione europea (la **Commissione**) l'aveva designata come *gatekeeper* ai sensi dell'art. 3 del *Digital Markets Act* (**DMA**), tra l'altro, in relazione ai servizi Facebook, Messenger e Marketplace (v. in questa Rubrica il contributo n. 3 del numero 3/ 2023 [(3)RA] in *PeM* 2023, p. 587).
Nella decisione impugnata, in particolare, la Commissione aveva qualificato Messenger e Marketplace come "*servizi di piattaforma di base*" ai fini del DMA, reputandoli, rispettivamente, un servizio di comunicazione interpersonale indipendente dal numero e un servizio di intermediazione *online*. Avendo accertato il superamento delle soglie quantitative previste dall'art. 3(2) DMA per ciascuno di tali servizi, la Commissione aveva

ISSN 2239-8570

reputato operanti le presunzioni relative alla sussistenza dei requisiti necessari per la designazione di Meta come *gatekeeper* con riferimento a entrambi.
Meta ha tuttavia proposto ricorso ai sensi dell'art. 263 del Trattato sul funzionamento dell'Unione europea (**TFUE**), chiedendo al Tribunale dell'Unione europea l'annullamento della decisione della Commissione nella parte relativa ai servizi Marketplace e Messenger. In parziale accoglimento del ricorso, il Tribunale ha annullato la decisione con riferimento a Marketplace, confermandola, invece, nella parte relativa a Messenger.
Quanto a Messenger, infatti, il Tribunale ha ritenuto che la Commissione avesse correttamente qualificato tale servizio come autonomo servizio di piattaforma di base, distinto dal *social network* Facebook. A tale conclusione conducono, secondo il Tribunale, l'esistenza di applicazioni autonome dedicate ai due servizi, la possibilità di utilizzare Messenger indipendentemente da Facebook e la presenza di strumenti specificamente destinati all'interazione con gli utenti di ciascun servizio. Non possono, invece, essere considerate sufficienti a deporre in senso contrario né la stretta integrazione tra i due servizi, né la sostanziale coincidenza delle rispettive basi di utenti. Il Tribunale, per un verso, ha poi precisato che l'esigenza, prevista dall'art. 3(9) DMA, secondo cui ciascun servizio deve costituire "*individualmente*" un punto di accesso importante non impone alla Commissione di computare soltanto gli utenti di Messenger che non siano anche utenti di Facebook. Per altro verso, ha escluso che la Commissione fosse tenuta ad avviare un'indagine di mercato ai sensi dell'art. 17(3) DMA prima di concludere che Messenger costituisse un punto di accesso importante, non avendo Meta fornito argomenti sufficienti a mettere manifestamente in dubbio le presunzioni previste dal DMA.
A diversa conclusione il Tribunale è giunto, invece, con riferimento a Marketplace. A tale proposito, occorre rammentare come la Commissione avesse reputato di potersi basare, ai fini della qualificazione del servizio, sui dati relativi ai tre esercizi precedenti la designazione. Secondo il Tribunale, tale impostazione confonde il periodo rilevante per verificare il superamento delle soglie quantitative, che può richiedere una valutazione retrospettiva, con quello pertinente alla qualificazione, di natura qualitativa, del servizio di piattaforma di base. In assenza di una diversa previsione normativa, quest'ultima valutazione deve essere compiuta sulla base degli elementi di fatto e di diritto esistenti al momento dell'adozione della decisione.
A tale ultimo fine assumono, pertanto, rilievo le modifiche apportate da Meta a Marketplace il 31 luglio 2023 (e, dunque, prima della decisione), mediante le quali è stato limitato il numero di annunci pubblicabili da ciascun utente. Tali modifiche, secondo il Tribunale, hanno inciso direttamente sul criterio da utilizzare per individuare gli utenti commerciali, fondato sulla categoria dei c.d. *power seller*, sicché la Commissione ne avrebbe dovuto tenere conto al fine di qualificare (o meno) Marketplace come servizio di intermediazione *online*. La decisione impugnata, invece, si è limitata a considerare tali limitazioni come ancora in fase di attuazione e ad affermare, in termini ipotetici, che gli utenti avrebbero comunque potuto essere considerati commerciali in funzione delle circostanze del caso concreto, senza tuttavia spiegare quali circostanze dovrebbero reputarsi rilevanti né in che modo le

ISSN 2239-8570

modifiche già attuate incidono (o meno) sulla qualificazione di Marketplace come servizio di intermediazione *online*.
Il Tribunale ha quindi ravvisato, sul punto, sia un errore di diritto che un difetto di motivazione della decisione impugnata, poiché essa non consente a Meta di comprendere adeguatamente le ragioni poste a fondamento della qualificazione del servizio, né al giudice dell'Unione di esercitare il proprio sindacato sulla legittimità della decisione stessa.
Ne è conseguito, come accennato, l'annullamento della decisione della Commissione, nella parte in cui ha designato Meta come *gatekeeper* per Marketplace.

RICCARDO ALFONSI

Testo ufficiale

2026/2(18)FF
Il rapporto sull'IA dell'AGCOM del 17.6.2026

L'Autorità per le garanzie nelle comunicazioni (**AGCOM**) ha pubblicato il 17 giugno 2026 il proprio **Rapporto sull'intelligenza artificiale** (il **Rapporto**), un documento volto ad offrire una ricostruzione organica e interdisciplinare delle principali evoluzioni tecnologiche, economiche, sociali e giuridiche connesse allo sviluppo e alla diffusione dei sistemi di IA, con particolare attenzione ai settori di competenza dell'Autorità e al ruolo che essa è chiamata a svolgere nell'ecosistema digitale italo-europeo.
Il Rapporto si articola in **due parti**, definite dagli stessi autori come «autonome e complementari».
La **prima parte**, predisposta dall'**Ufficio intelligenza artificiale dell'AGCOM,** ha una funzione introduttiva e ricostruttiva, volta a fornire le basi tecniche, economiche e concettuali necessarie per comprendere il fenomeno dell'IA. Essa si compone di sei capitoli: dopo il capitolo 1, contenente un'**introduzione generale**, il capitolo 2 ripercorre l'**evoluzione storica** dell'IA, dalla sua affermazione come disciplina scientifica nel 1956 fino agli sviluppi più recenti, quali l'IA generativa e l'IA agentica; il capitolo 3 è dedicato alle **caratteristiche tecniche** dell'IA, evidenziando come la comprensione del suo funzionamento costituisca un presupposto indispensabile, poiché «senza una reale comprensione del motore sottostante […] ogni discussione normativa o economica rischia di essere astratta, sbilanciata o poco efficace»; il capitolo 4 analizza le **peculiarità economiche** del "bene" IA e dei mercati e delle industrie che ne sostengono lo sviluppo e l'impiego; il capitolo 5 affronta le principali **questioni aperte**, esaminando, accanto ai profili tecnologici ed economici, gli impatti di carattere generale, ambientale e sui diritti fondamentali, fungendo da raccordo con la seconda parte del Rapporto; il capitolo 6 contiene, infine, le **considerazioni conclusive**.
La **seconda parte** del Rapporto è elaborata dal **Comitato sull'intelligenza Artificiale**, istituito presso l'AGCOM con delibera 11/24/CONS del 24

ISSN 2239-8570

gennaio 2024 per fornire all'Autorità supporto scientifico e consultivo in relazione all'impatto dell'IA sulle materie di propria competenza. Essa rappresenta il naturale sviluppo della prima parte, poiché sposta l'attenzione dall'inquadramento tecnico ed economico del fenomeno all'analisi delle sue **implicazioni giuridiche, regolatorie e sociali nei settori affidati all'AGCOM**.

Il Rapporto del Comitato si articola in nove capitoli.

Dopo il capitolo 1, contenente l'Introduzione di **Andrea Renda**, dedicata all'evoluzione dell'*AI Act* nel **quadro regolatorio europeo**, anche alla luce dei più recenti sviluppi tecnologici, **Giovanna de Minico**, nel capitolo 2 ricostruisce le **competenze dell'AGCOM** nell'assetto delineato dall'AI Act e dal Digital Services Act; il capitolo 3, curato da **Andrea Imperiali di Francavilla**, offre una ricognizione dell'impatto dell'IA sui **settori di competenza dell'Autorità**, dalle comunicazioni elettroniche ai servizi digitali, dai media audiovisivi ai servizi postali e alla tutela dei consumatori.

I capitoli successivi affrontano alcune delle principali questioni aperte poste dall'IA: **Andrea Simoncini**, nel capitolo 4, analizza le **implicazioni costituzionali** per la democrazia e la libertà di informazione, alla luce del ruolo assunto dalle piattaforme digitali quali formazioni sociali titolari di un potere normativo privato su scala globale. **Giovanni Boccia Artieri**, nel capitolo 5, esamina i **rischi sistemici derivanti dall'impiego dell'IA generativa quale infrastruttura cognitiva del discorso pubblico**. **Giuseppe Cassano**, nel capitolo 6, si sofferma sui problemi dell'autorialità e della tutela del **diritto d'autore**. **Mauro Giusto**, al capitolo 7, affronta il tema dell'**educazione** e dell'alfabetizzazione digitale delle giovani generazioni. **Giovanna De Minico,** nel capitolo 8, dedica infine un ulteriore contributo al rapporto tra tecnica e diritto, interrogandosi sul rischio di una progressiva transizione dalla *rule of law* alla ***rule of tech***. Il Rapporto si conclude con le **raccomandazioni** elaborate dal Comitato, contenute nel capitolo 9, che sottolineano l'esigenza di un ruolo proattivo dell'AGCOM nell'attuazione del nuovo quadro europeo.

Si offre di seguito una sintetica ricostruzione dei contenuti essenziali del Rapporto. La numerazione adottata richiama quella del documento: il numero romano ne identifica la parte (**Parte I** e **Parte II**), mentre il numero arabo individua il relativo capitolo. Restano esclusi da un esame autonomo i capitoli introduttivi e conclusivi.

Parte I: Il Rapporto tecnico dell'Ufficio IA

I.2. Evoluzione storica

Il **capitolo 2** ripercorre l'evoluzione storica dell'IA a partire dal ***Dartmouth Summer Research Project on Artificial Intelligence*** del 1956, occasione nella quale **John McCarthy** coniò l'espressione «*Artificial Intelligence*», definendola come «*the science and engineering of making intelligent machines*». Il Rapporto richiama, tuttavia, anche il precedente contributo di **Alan Turing**, il cui celebre test del 1950 rappresenta uno dei primi tentativi di verificare la capacità delle macchine di riprodurre un comportamento intelligente.

L'analisi ricostruisce quindi l'alternarsi di fasi di forte sviluppo (*AI springs*) e di periodi di rallentamento della ricerca (*AI winters)*, evidenziando la

ISSN 2239-8570

contrapposizione tra l'approccio **simbolico**, e quello **sub-simbolico** o connessionista. Il Rapporto individua nell'attuale fase, definita «**terza primavera dell'IA**», avviata a partire dal 2012, il momento di definitiva affermazione dell'approccio sub-simbolico, resa possibile dalla combinazione tra la disponibilità di enormi quantità di dati (*big data*) e l'incremento della capacità computazionale. Da tale evoluzione deriva anche lo **sviluppo di interfacce conversazionali in linguaggio naturale che favoriscono l'antropomorfizzazione dei sistemi di IA**. Va altresì segnalato il progressivo spostamento degli investimenti dalla ricerca pubblica a quella privata, con conseguente concentrazione dello sviluppo tecnologico nelle mani di **pochi grandi operatori**. La ricostruzione storica costituisce la premessa per l'analisi delle caratteristiche tecniche dell'IA sviluppata nel capitolo successivo.

I.3. Caratteristiche tecniche

Nel **capitolo 3**, il Rapporto distingue tra **modelli simbolici**, fondati su regole logiche ed esplicite e caratterizzati da un funzionamento deterministico, e **modelli sub-simbolici**, basati sull'apprendimento automatico (***machine learning***) nei quali le inferenze derivano dall'individuazione di relazioni statistiche tra i dati e assumono natura probabilistica. All'interno di questi ultimi, particolare attenzione è dedicata al ***deep learning***, fondato su reti neurali profonde, ispirate al funzionamento del cervello umano. Se i modelli simbolici risultano più trasparenti e interpretabili, quelli sub-simbolici presentano prestazioni sensibilmente superiori, ma pongono il noto problema della ***black-box***, ossia della difficoltà di ricostruire il percorso logico seguito dal sistema nell'elaborazione dell'*output*.

Il Rapporto richiama inoltre le principali modalità di apprendimento automatico – supervisionato, non supervisionato, per trasferimento e per rinforzo – per poi soffermarsi sull'**IA generativa** (GenAI), una particolare applicazione del deep learning capace di produrre contenuti originali sulla base dei dati di addestramento. Tale evoluzione è stata resa possibile dall'architettura ***Transformer***, introdotta nel 2017 da Ashish Vaswani e alcuni suoi colleghi, fondata su nuove modalità di rappresentazione ed elaborazione del linguaggio naturale (NLP). Il capitolo si conclude distinguendo gli attuali sistemi di **IA debole** (*weak AI*), progettati per svolgere compiti specifici, dalle prospettive dell'**IA generale** (*Artificial General Intelligence* – AGI), ancora oggetto di ricerca, richiamando, quale esempio delle più recenti evoluzioni, la ***Darwin Gödel Machine***, modello sperimentale capace di modificare autonomamente il proprio codice al fine di migliorare le proprie prestazioni.

I.4. Caratteristiche economiche

Il **capitolo 4** esamina le caratteristiche economiche dell'IA, descritta tanto come un bene privato, a seguito del processo di *commodification*, quanto come bene dinamico a vocazione globale, distribuito secondo logiche flessibili di accesso, segmentazione e aggiornamento. L'IA costituisce il nucleo emergente di una **infrastruttura economica** riconducibile ad un **mercato multilaterale** (*multi-sided market*), fondato su due principali relazioni economiche: quella tra piattaforme e produttori dei contenuti utilizzati per l'addestramento dei modelli, nella quale il ricorso a materiali

ISSN 2239-8570

protetti da *copyright* ha favorito il passaggio dalle controversie sul *fair use* e sull'uso trasformativo alla conclusione di accordi di *licensing ex ante*; e quella tra piattaforme e utenti finali, nella quale prevalgono modelli di offerta di tipo *freemium*.

La **struttura produttiva** dell'IA è fortemente *capital intensive*, in ragione degli ingenti costi fissi necessari allo sviluppo dei modelli, alla produzione di semiconduttori avanzati e alla realizzazione di infrastrutture computazionali (*data center* iperscalabili), che costituiscono rilevanti barriere all'ingresso. Ai modelli inizialmente chiusi, fondati sul segreto industriale e su meccanismi di *lock-in*, si affiancano oggi forme differenziate di apertura (*data transparency*, *open weights*, *code transparency* e *open source*), che non hanno tuttavia eliminato l'elevato livello di integrazione del settore. Le imprese leader, infatti, operano contemporaneamente quali sviluppatori di modelli di IA, fornitori delle infrastrutture computazionali, gestori delle piattaforme di accesso al mercato e fornitori dei servizi digitali finali, realizzando strategie di integrazione verticale e di filiera lungo l'intera catena del valore. Ne deriva una **struttura di mercato oligopolistica**, fondata su vantaggi cumulativi e su un potere economico e cognitivo di dimensione sovranazionale.

I.5. Questioni aperte sull'IA

A conclusione della parte tecnico-economica, emergono alcune «questioni aperte» raccolte nel **capitolo 5**. L'attuale fase di sviluppo dell'IA è caratterizzata da una netta asimmetria tra l'innovazione tecnologica e la capacità delle istituzioni di governarne gli effetti. Tale criticità si accentua con la diffusione di sistemi di **IA agentica**, che segnano un momento-soglia dell'evoluzione tecnologica, essendo in grado di pianificare ed eseguire autonomamente sequenze di azioni, e rendendo imprescindibile il mantenimento di un controllo umano effettivo (***human in the loop***). Assumono altresì rilievo anche gli **aspetti ambientali**, legati all'elevato consumo di energia, acqua e risorse computazionali richiesto dall'addestramento e dall'impiego su larga scala dei modelli di IA. Da qui l'esigenza di promuovere una ***Sustainable AI***, orientata allo sviluppo di sistemi più efficienti e a minore impatto ambientale, attraverso una chiara definizione delle priorità strategiche.

Merita, infine, un cenno la **posizione dell'Europa** nello scenario globale. Se, da un lato, essa si conferma leader nella definizione di un modello di *governance* etica e regolatoria, dall'altro continua a scontare un ritardo sul piano tecnologico e industriale rispetto ai principali *competitor* internazionali. Ne deriva l'esigenza di rafforzare un ecosistema europeo dell'IA, valorizzando modelli autonomi, coordinando gli investimenti pubblici e privati e superando la tradizionale polarizzazione tra Stati Uniti e Cina. In questa direzione si colloca il **Piano d'Azione per l'Intelligenza Artificiale** (*AI Continent Action Plan*) presentato dalla Commissione europea il 9 aprile 2025. Nello stesso quadro possono essere lette anche iniziative operative quali **LLMs4EU**, volte a promuovere lo sviluppo di modelli linguistici europei e a tradurre in pratica l'obiettivo di una maggiore autonomia tecnologica dell'Unione. Strategia industriale, innovazione tecnologica e

ISSN 2239-8570

tutela dei diritti fondamentali sono così concepite come dimensioni complementari di un'unica politica europea dell'IA.

Parte II: il rapporto giuridico del Comitato IA di AGCOM

Su queste premesse si innesta la seconda parte del Rapporto, dedicata all'analisi del quadro regolatorio e del ruolo che l'AGCOM è chiamata a svolgere nell'ecosistema digitale.

II.2. La *regulation* dell'AGCOM nell'ecosistema digitale

Il **capitolo 2** ricostruisce le **competenze** dell'AGCOM attraverso una lettura coordinata del reg. (UE) 2022/2065 (**Digital Services Act** o **DSA**) e del reg. (UE) 2024/1689 (**AI Act** o **AIA**) (sui quali, v. in questa Rubrica, rispettivamente il contributo n. 1 del numero 4/2022 [2022/4(1)ST] e il contributo n. 2 del numero 2/2024 [2024/2(2)SO]). Il fondamento della sua competenza è individuato nell'art. 49 DSA che introduce la figura del *Digital Services Coordinator* (DSC), funzione attribuita in Italia all'AGCOM mediante modifica additiva della legge istitutiva (l. n. 249/1997) ad opera del decreto Caivano (d.l. 123/2023). L'Autorità è chiamata a vigilare sulla diffusione di «contenuti illegali», cioè contrari al diritto dell'Unione o nazionale *ex* art. 3(1)(h), DSA, la cui mera circolazione integra *ex se* un illecito di pericolo.

Diversamente, né l'*AI Act* né la legge italiana sull'IA (l. n. 132/2025, sulla quale, v., in questa Rubrica, il contributo n. 1 del numero 3/2025 [2025/3(1)AA]) attribuiscono specifiche competenze all'AGCOM, individuando quali autorità di riferimento l'Agenzia per l'Italia Digitale (**AgID**) e l'Agenzia per la cybersicurezza nazionale (**ACN**), salvo il richiamo alla disciplina sul diritto d'autore (art. 25(1) legge 633/1941: **l.d.a.**), che estende la tutela anche alle opere realizzate con l'ausilio dell'IA, purché espressione del lavoro intellettuale dell'autore. L'AGCOM, pertanto, non esercita poteri sull'IA in quanto tale, ma interviene sugli effetti che essa produce nei settori di propria competenza, in particolare quando costituisce lo strumento di diffusione di contenuti «illegali». A tali competenze si aggiunge quella in materia di pubblicità politica online: il Reg. (UE) 2024/900 rinvia infatti, per gli obblighi gravanti sui prestatori di servizi intermediari (artt. 7-17 e 21), al sistema di vigilanza delineato dal DSA (art. 22, par. 3), attribuendo all'AGCOM le relative funzioni, ferme restando la competenza del Garante *privacy* (europeo o nazionale) in materia di *targeting* (artt. 18 e 19) e quella della Commissione europea nei confronti di piattaforme e dei motori di ricerca di dimensioni molto grandi (VLOPs e VLOSEs).

II.3. L'impatto IA nei settori regolati dall'AGCOM

Il **capitolo 3** offre una mappatura sistematica degli impatti dell'IA nei settori di competenza dell'AGCOM, quali: comunicazioni elettroniche; servizi digitali e *media* audiovisivi, servizi postali e tutela dei consumatori. Per ciascun ambito sono distinti gli impatti effettivi da quelli potenziali, ne è valutata la priorità in rapporto alla gravità del rischio e al grado di preparazione normativa e sono individuati gli strumenti di intervento disponibili, secondo una scansione *ex ante*, *in itinere* ed *ex post*, corrispondente a una regolazione continua fondata sulla prevenzione, sulla vigilanza e sulla correzione.

ISSN 2239-8570

Tra i rischi più rilevanti figurano, nelle **comunicazioni elettroniche**: la discriminazione algoritmica del traffico, la collusione automatizzata dei prezzi e la perdita di controllo umano nella gestione delle reti; nei **servizi digitali**: la diffusione dei *deepfake*, l'incidenza degli algoritmi di raccomandazione sul pluralismo e le manipolazioni del processo elettorale; nei **servizi postali**: la sorveglianza commerciale, il monitoraggio delle merci e il *greenwashing* algoritmico; infine, nella **tutela dei consumatori**: l'opacità delle decisioni automatizzate, la sorveglianza biometrica e le tecniche di manipolazione cognitiva dei soggetti vulnerabili, secondo logiche di *addiction by design*.

La ricognizione è completata dal confronto con le esperienze di altri regolatori europei, tra cui Ofcom (Regno Unito), Arcom (Francia) e BNetzA (Germania), e dall'analisi del quadro normativo applicabile. In tale contesto assume rilievo l'art. 70 *AI A*ct, che consente agli Stati membri di designare come autorità nazionali competenti anche autorità di settore: una scelta che potrebbe riconoscere all'AGCOM, nei mercati già sottoposti alla sua vigilanza, competenze parallele e coordinate rispetto a quelle già attribuite ad AgID e ACN.

II.4. Democrazia costituzionale e libertà dell'informazione al tempo dell'IA

Il **capitolo 4** esamina la libertà in una prospettiva costituzionale tridimensionale: libertà di conoscere, tutelata dagli artt. 21 e 33 cost.; libertà di informare, riconducibile all'art. 21 cost.; libertà di comunicare, garantita dall'art. 15 cost. Il riferimento dell'art. 21 cost. a «ogni altro mezzo di diffusione» conferma la capacità della Costituzione di adattarsi ai mutamenti tecnologici (cd. *future proof*). In questo quadro, le piattaforme digitali assumono la natura di «formazioni sociali» *ex* art. 2 cost., nelle quali si sviluppano relazioni decisive per la costruzione dell'identità personale. Esse rappresentano, tuttavia, al tempo stesso spazi di libertà e possibili fonti di compressione dei diritti: divenute ormai essenziali per l'ordinaria partecipazione alla vita sociale, espongono gli utenti ai rischi della profilazione, del filtraggio algoritmico delle informazioni e del passaggio dai «motori di ricerca» ai «motori di risposta», che restituiscono contenuti diretti relegando in secondo piano le fonti originarie. La libertà non può quindi essere intesa soltanto come assenza di interferenze del potere pubblico, ma richiede protezione anche rispetto alla selezione e alla manipolazione privata dei flussi informativi. Trasparenza, *accountability*, educazione digitale e consapevolezza degli utenti costituiscono pertanto condizioni essenziali per l'effettivo esercizio delle libertà costituzionali nell'ecosistema digitale.

II.5. (*Segue*). IA generativa, disinformazione e *hate speech*

Strettamente collegato al precedente, il **capitolo 5** esamina l'IA generativa non come semplice strumento, ma come «infrastruttura cognitiva» capace di ridefinire le condizioni di produzione e circolazione del discorso pubblico. I principali rischi riguardano la manipolazione informativa, attraverso *deepfake*, *voice cloning* e contenuti sintetici prodotti su larga scala; la degradazione discorsiva, mediante l'amplificazione automatizzata dell'*hate speech*; i meccanismi dell'economia dell'attenzione, fondati su *micro-targeting*, sistemi di raccomandazione e circuiti di retroazione algoritmica.

ISSN 2239-8570

Per ciascun rischio sono individuati specifici strumenti regolatori, dai sistemi di *provenance* e *labeling* dei contenuti ai protocolli di risposta rapida, delineando per l'AGCOM un ruolo di coordinamento e garanzia quale «infrastruttura della fiducia» dell'ecosistema digitale.

II.6. Diritto d'autore e IA generativa

Il **capitolo 6** affronta il tema del diritto d'autore nell'era dell'IA, muovendo dalla premessa che la creatività giuridicamente rilevante resta quella umana. Ne consegue che la tutela può estendersi anche alle opere realizzate con l'ausilio dell'IA, purché espressione del lavoro intellettuale dell'autore, mentre resta esclusa per gli *output* interamente generati dalla macchina. In tale prospettiva si inserisce la modifica dell'art. 1 della l.d.a. ad opera della legge italiana sull'IA.

Il capitolo affronta inoltre l'utilizzo di opere protette per l'addestramento dei modelli. Mentre l'esperienza statunitense ricorre al principio del *fair use*, quella europea si fonda sulle eccezioni per il *text and data mining* previste dagli artt. 3 e 4 della direttiva (UE) 2019/790, recepite nell'ordinamento italiano dagli artt. 70-*ter* e 70-*quater* l. n. 633/1941. La loro applicazione resta tuttavia controversa: il *Landgericht München* I, con sentenza dell'11 novembre 2025 (42 O 14139/24), nel caso GEMA c. OpenAI, ha escluso l'applicazione dell'eccezione, distinguendo la mera estrazione dalla stabile memorizzazione delle opere nel modello e dalla loro successiva riproduzione negli *output*; di segno opposto è invece la decisione del *Landgericht Hamburg* del 27 settembre 2024, relativa al progetto LAION, che ha ritenuto applicabile l'eccezione per il *text and data mining* in favore di un'organizzazione senza scopo di lucro operante nella ricerca scientifica. In questo quadro, il Codice di buone pratiche per l'IA, il cui capitolo 2 è specificamente dedicato al *copyright*, è considerato uno strumento utile a bilanciare le esigenze di sviluppo dei modelli con la tutela dei titolari dei diritti.

II.7. L'IA e l'educazione dei giovani

Il **capitolo 7** affronta la dimensione educativa della sfida posta dall'IA, evidenziando il paradosso di una generazione «più connessa, ma meno consapevole». Tra i principali rischi per i minori sono richiamati l'abbandono educativo, la dipendenza tecnologica e la sostituzione delle relazioni umane con l'interazione costante con sistemi di IA, che, offrendo risposte sempre accondiscendenti e forme di accettazione incondizionata, ostacolano lo sviluppo dell'identità personale e della capacità critica. A ciò si aggiunge il rischio di una persuasione occulta, alimentata da *filter bubble*, *deepfake* e contenuti sintetici, che rende sempre più difficile distinguere il vero dal falso.

Il capitolo individua nella **scuola** il principale presidio educativo, qualificato anche dall'*AI Act* come ambito ad alto rischio, e propone un percorso di alfabetizzazione fondato sull'**algoretica**, articolato nei livelli della conoscenza, del discernimento critico e della responsabilità partecipativa. In tale prospettiva, l'AGCOM è chiamato a contribuire alla definizione di standard di tutela dei minori e di educazione digitale nell'ecosistema informativo.

II.8. Il mosaico di regole nell'Ecosistema digitale

Il **capitolo 8** esamina il mutamento del rapporto tra **Diritto** e **Tecnica**. Muovendo dal mito prometeico narrato da Eschilo e dalla riflessione

ISSN 2239-8570

aristotelica, la tecnica è ricostruita come un fattore di emancipazione per l'uomo solo finché resta subordinata ai fini definiti dalla politica e dal diritto. Nel lungo percorso che si snoda dalla Grecia antica fino agli odierni mercati digitali, questo equilibrio tende progressivamente a invertirsi: la tecnica erode la primazia della regola giuridica e, da strumento servente, si trasforma in una fonte normativa autonoma, dotata di forza effettiva ma priva di una corrispondente legittimazione democratica.

L'evoluzione è articolata in tre passaggi.

(i) Il completamento discrezionale delle norme antitrust aperte.

La disciplina della concorrenza ricorre a clausole elastiche e concetti indeterminati, destinati ad adattarsi al mutamento dei mercati; spetta quindi all'Antitrust precisarne il contenuto nel caso concreto, attraverso parametri economici e tecnici. L'Autorità non si limita così ad applicare una regola già definita, ma contribuisce a costruire il criterio del giudizio, esercitando una funzione ibrida tra *iuris dictio* e *iuris latio*, con una componente di indirizzo politico. Nei mercati digitali, tale attività impone inoltre di superare la rigida separazione tra concorrenza e protezione dei dati, poiché la lesione della *privacy* può costituire anche un indice di abuso del potere di mercato.

(ii) L'autoregolazione privata come fonte normativa

Codici di condotta, standard tecnici e regole predisposte dagli operatori digitali non restano confinati alla sfera privata, ma incidono in modo generale sui comportamenti e sui diritti degli utenti. La loro trasformazione in veri e propri «codici-fonti» è ammissibile soltanto in presenza di adeguate garanzie di rappresentatività, trasparenza, partecipazione, imparzialità, controllo pubblico e tutela dei diritti fondamentali. In assenza di tali condizioni, la co-regolazione rischia di legittimare un potere normativo privato sottratto a effettivi contrappesi.

Da questa prospettiva emergono le criticità dei codici volontari previsti dal DSA, il cui contenuto resta in larga misura affidato agli stessi operatori regolati. Analoga cautela riguarda l'*AI Act*, che, pur orientato alla protezione della persona, fa ampio ricorso ad autodichiarazioni, valutazioni interne e procedure di conformità predisposte dai fornitori, non sempre compensate da controlli pubblici indipendenti.

(iii) Il rischio che i sistemi di IA divengano direttamente *source of law*.

Il rischio più radicale si manifesta quando il sistema di IA produce direttamente decisioni particolari e concrete. La statuizione algoritmica tende allora a sostituirsi alla norma generale e astratta, indebolendo la certezza del diritto, rendendo opachi i criteri decisionali e riproducendo discriminazioni incorporate nei dati e nei modelli. È in questo passaggio che *la rule of law* rischia di cedere alla *rule of tech*.

La soluzione proposta consiste nel ridefinire il **rapporto tra Diritto e Tecnica**, assegnando a ciascuno un ruolo distinto. Alla norma spetta ricondurre la pluralità degli interessi entro un quadro unitario di valori; alla tecnica, svilupparsi nel rispetto di tali coordinate. In questa prospettiva, il legislatore europeo dovrebbe «fare meno», ma «in modo diverso»: da un lato, eliminando regole superate, inutilmente invasive o discriminatorie nei confronti dei piccoli operatori; dall'altro, correggendo gli squilibri prodotti dal potere tecnologico attraverso rimedi effettivi nei confronti delle grandi

ISSN 2239-8570

piattaforme e sostituendo i meccanismi di autodichiarazione con controlli pubblici realmente indipendenti. Solo a queste condizioni l'intreccio tra politica e tecnica può diventare un fattore di rafforzamento, anziché di erosione, dell'ordinamento democratico.

Osservazioni conclusive

Numerose sono le suggestioni che emergono dal Rapporto. Volendo trarne sinteticamente le fila, possono formularsi alcune considerazioni finali.

In primo luogo, emerge l'esigenza di un intervento tempestivo dell'AGCOM, senza attendere la piena stabilizzazione del quadro normativo europeo, destinato a rimanere in continua evoluzione anche alla luce del *Digital Omnibus Package*. Se, da un lato, il primo tassello di tale pacchetto – il cd. *Digital Omnibus on AI*, originariamente presentato con la proposta COM(2025)836 (sulla quale v., in questa Rubrica, la notizia n. 6 del numero 4/2025 [2025/4(6)Est] e la n. 1 del numero 1/2026 [2026/1(1)Est]), è stato adottato con il Reg. (UE) 2026/1744 dell'8 luglio 2026 (v. *supra* contributo n. 2 in questo numero di questa Rubrica [2026/2(2)ES]) dall'altro, l'iniziativa COM(2025)837 relativa al cd. *Data Acquis* europeo (sulla quale v. il contributo n. 5 del numero 4/2025 [2025/4(5)Est]) è tuttora all'esame del legislatore europeo. La persistente evoluzione del quadro regolatorio non può, tuttavia, tradursi in inerzia istituzionale, soprattutto in un settore caratterizzato da una rapidissima innovazione tecnologica.

In secondo luogo, il Rapporto evidenzia come l'IA non possa essere affrontata secondo una logica settoriale, ma richieda un paradigma regolatorio trasversale. I principi comuni – trasparenza, supervisione umana, non discriminazione e tutela dei soggetti vulnerabili – devono essere declinati attraverso strumenti differenziati in relazione ai diversi contesti applicativi, secondo un approccio inevitabilmente interdisciplinare, capace di integrare competenze giuridiche, economiche, tecnologiche e sociali.

In questa prospettiva si colloca anche il richiamo alla costruzione di un'infrastruttura tecnologica europea (**EuroStack**), quale presupposto della sovranità digitale dell'Unione. La competitività tecnologica non è presentata come un obiettivo alternativo alla tutela dei diritti fondamentali, ma come una condizione per preservare l'autonomia regolatoria europea rispetto ai grandi operatori globali. In tale contesto, l'AGCOM è chiamata a svolgere un ruolo di raccordo istituzionale, contribuendo a una *governance* della tecnologia fondata sulla legittimazione democratica e sull'*accountability* pubblica, attraverso l'imprescindibile coordinamento con le altre autorità nazionali ed europee.

FRANCESCA FERRETTI

Rapporto IA 2026

2026/2(19)CDS
Il (video)gioco è una cosa seria! Il documento di raccomandazioni e buone pratiche per la protezione dei dati personali nei videogiochi

ISSN 2239-8570

emanato dalle autorità per la protezione dei dati personali spagnola e belga nel giugno 2026

Nel mese di giugno 2026, realizzando una mirabile espressione di cooperazione tra le autorità di controllo in vista di una coerente applicazione del reg. (UE) 2016/679 (il **Regolamento** o **GDPR**) in tutta l'Unione europea (cons. 10, 123 art. 50 GDPR) le autorità di controllo per la protezione dei dati spagnola e belga hanno licenziato le ***Recommendations and best practices for data protection in video games***" (le **Raccomandazioni** o il **Documento**). Si tratta di un corposo documento, degno di nota nella forma e nel contenuto, rivolto a professionisti e organizzazioni coinvolti nell'ecosistema dei videogiochi, teso a fornire indicazioni legali e a individuare misure organizzative e tecniche per la progettazione, lo sviluppo e la fornitura di videogiochi coerenti con i principi e i requisiti del GDPR.
Il Documento, esemplare anche nella sua struttura per i titolari del trattamento che devono attuare il principio di *accountability* e i correlati obblighi di *privacy by design* e *by default* (cfr. artt. 5(2), 24 e 25 GDPR, e Linee guida 4/2019 del Comitato europeo per la protezione dei dati (**EDPB**) sull'art. 25 GDPR, intitolate "Protezione dei dati fin dalla progettazione e per impostazione predefinita") procede individuando e approfondendo i seguenti sette ambiti:

- **cosa sono e come possono classificarsi i videogame**;
- **i principali attori coinvolti nel processo industriale di creazione del prodotto**;
- **le fasi di tale processo**;
- **i dati personali raccolti e ulteriormente trattati in ciascuna fase**,
- **le finalità dei trattamenti e le categorie degli interessati**;
- **le principali minacce e i rischi ai quali i dati sono esposti nelle diverse fasi del ciclo di vita di un videogame**;
- **le raccomandazioni da rispettare e le buone prassi da applicare in ciascuna di queste fasi**.

Il Documento si conclude con cinque allegati contenenti una ***checklist*** indicativa e non esaustiva per la verifica dell'adozione delle principali misure tecniche e organizzative suggerite ai soggetti a vario titolo coinvolti nel ciclo di vita di un videogame.
Il Documento presenta quindi uno **schema logico estremamente utile** per un'efficace attuazione degli obblighi di protezione dei dati personali che i titolari potranno e dovrebbero mutuare non solo in tale settore ma, con le dovute modifiche, anche nei più disparati cotesti.
Con specifico riferimento al settore esaminato, un osservatore superficiale potrebbe individuare in alcune delle buone prassi indicate nel Documento (quali la creazione di "*GDPR role gate*"; la compilazione di inventari, *checklist*, mappe scritte del ciclo di vita dei dati o *data dictionary*, l'introduzione di etichette sulla *privacy*, la costituzione di centri o *hub* dedicati alla *privacy* etc.) l'imposizione di ulteriori adempimenti formali. Al contrario, quanto suggerito fornisce una dimostrazione plastica dell'attuazione del principio di *accountability*.

ISSN 2239-8570

Salvo rare eccezioni, infatti, il GDPR non indica le misure in concreto richieste al titolare per attuare e dimostrare i principi di protezione dei dati personali, rimettendone la scelta al titolare.
Ebbene il Documento, che riconosce un'opportunità nella libertà di forme concessa dal GDPR, esemplifica, in maniera estremamente efficace, cosa si intende per atteggiamento proattivo, attraverso l'esemplificazione di una serie di misure specifiche che, presupponendo una profonda e imprescindibile conoscenza delle tecnologie impiegate, risultano non solo altamente adattate al contesto di riferimento ma che producono altresì l'effetto di semplificare lo svolgimento degli ulteriori adempimenti specificamente richiesti dal Regolamento.
Venendo al **PRIMO AMBITO DI APPROFONDIMENTO** (**cosa sono e come possono classificarsi i videogame**) il Documento sia apre riportando alcune informazioni sul mercato dei videogiochi. Si ricorda che **il *gaming* è un settore di mercato in continua espansione**, che, grazie anche all'interazione con l'intelligenza artificiale, produce ricavi annuali globali stimati intorno ai 200 miliardi di dollari. La maggior parte dei giochi è venduta in formato digitale, producendo un significativo slancio per lo sviluppo di piattaforme e servizi *online* e nuovi modelli di *business*.
Tutto ciò contribuisce ad accrescerne l'interesse e la centralità rispetto ai temi di protezione dei dati personali, tenuto conto anche degli specifici rischi correlati ai videogame, amplificati dal riguardare un **momento ricreativo** della vita degli individui, naturalmente meno propensi all'**attenzione**, dal coinvolgere per lo più soggetti vulnerabili, in quanto **minori**, e dal prevedere spesso **trattamenti opachi** che superano di gran lunga la legittima aspettativa degli interessati.
Il **videogioco** è definito, considerando sia i giochi tradizionali che quelli più evoluti, come **un'esperienza digitale** in cui uno o più giocatori interagiscono tra loro e con ambienti virtuali attraverso un sistema di regole, obiettivi e *feedback*, solitamente utilizzando dispositivi elettronici come *computer*, *console*, *smartphone* o piattaforme *cloud*, ma anche realtà virtuali o aumentate e sistemi di intelligenza artificiale.
In sintesi, gli elementi caratterizzanti un videogame sono: **l'interattività; la presenza di un'interfaccia digitale; regole e obiettivi; un sistema di *feedback*; l'intrattenimento**.
Il Documento crea una tassonomia dei videogame sulla base di diversi criteri:

- in base all'obiettivo: il gioco può essere **di intrattenimento puro, educativo/formativo o "serio"**;
- in base al livello di connettività: vi sono giochi ***on line* e *off line***; ù
- in base alla piattaforma tecnologica impiegata: vi sono giochi **su *hardware* dedicati**, giochi che si svolgono **in *cloud*/*streaming*, in realtà virtuali o nel metaverso**;
- in base al modello economico o alla strategia di monetizzazione impiegata: il gioco può richiedere un **acquisto *una tantum***, il pagamento di un **canone ricorrente**, può essere **"*Free-to-Play*" (F2P)** - ossia consentire ai giocatori di accedervi gratuitamente - generando ricavi attraverso microtransazioni, pubblicità *in-game* o altri metodi di monetizzazione o infine **"*Freemium*"** - ossia basato su

ISSN 2239-8570

una combinazione di contenuti gratuiti e *premium*, offrendo l'accesso gratuito al gioco ma prevedendo un costo per le funzionalità avanzate.

Per ciascuna categoria di gioco l'interessato è esposto a **diverse tipologie di rischi**, anche in relazione alla probabilità che essi si verifichino e alla gravità delle conseguenze che ne possono conseguire.

Venendo al **SECONDO AMBITO DI APPROFONDIMENTO (i principali attori coinvolti nel processo industriale di creazione del prodotto)** Il Documento individua**:**

- **i fornitori di *hardware;***
- **i creatori, *designer* e sviluppatori;**
- **i fornitori di tecnologie per lo sviluppo dei giochi;**
- **gli editori;**
- **i distributori.**

Vieppiù viene messo in evidenza come sovente sia **la stessa comunità di giocatori** ad arricchire i videogiochi creando dei contenuti (***User-generated content:* UGC**), rendendo così i videogame dei veri e propri **ecosistemi collaborativi** in cui i giocatori contribuiscono a plasmare l'esperienza.

Quanto al **TERZO AMBITO DI APPROFONDIMENTO (le fasi del processo industriale di creazione del prodotto)**, aderendo a una delle più comuni concettualizzazioni del ciclo di vita dei videogiochi, il Documento individua tre principali macro fasi:

- **pre-produzione e produzione** (a sua volta divisa in ideazione, pre-produzione, produzione, collaudo e pre-lancio);
- ***release*** (rilascio al pubblico, in modo che i giocatori possano giocare);
- **post-produzione** che include attività di correzione dei *bug*, il rilascio di aggiornamenti graduali e di contenuti scaricabili, il *marketing*.

Il Documento si rivolge quindi al **QUARTO E AL QUINTO AMBITO DI APPROFONDIMENTO** ossia all'**individuazione delle categorie dei dati raccolti e ulteriormente trattati**, e alle **finalità dei relativi trattamenti**.

Il Documento sottolinea innanzitutto l'enorme quantità di dati personali che possono essere trattati nelle diverse attività che si sviluppano durante tutto il ciclo di vita dei videogame.

Vengono in evidenza: **dati identificativi diretti** (es. username, indirizzo di posta elettronica, identificativo dell'*account*); **dati pseudonimi,** comunque idonei ad identificare in maniera univoca l'interessato (es. ID dei dispositivi, *token* di sessione o lo UUID - *Universally Unique Identifier* - che identifica un singolo giocatore attraverso varie sessioni di gioco senza rivelarne dati identificativi diretti); **metadati**, ossia dati che forniscono informazioni su altri dati o eventi all'interno dell'ambiente di gioco (es *timestamp*, *ping* di geolocalizzazione) riferibili ad un determinato soggetto. Perfino i profili di gioco resi (apparentemente) "anonimi" possono consentire l'identificazione di singoli individui se analizzati tramite "*fingerprinting*" comportamentali.

I dati personali degli utenti vengono generalmente raccolti, in primo luogo, per **la creazione e gestione degli *account*** degli utenti e per i connessi processi di autenticazione. Più nello specifico, questa fase include la: creazione dell'*account*; fase cd di IAAA *(Identification, Authentication, Authorisation, and Accountability*); personalizzazione e customizzazione dei

ISSN 2239-8570

contenuti; gestione delle interazioni con altri giocatori; assistenza clienti e risoluzione delle controversie; prevenzione delle frodi e sicurezza.
l dati personali dei giocatori vengono poi trattati per una particolare forma di monitoraggio, definita "**telemetria**", che determina la registrazione nel tempo del comportamento dei giocatori e le metriche relative alle loro prestazioni (es. la durata e la frequenza delle interazioni nel gioco; il livello raggiunto, statistiche, tempo di assenza dal gioco, dati biometrici come movimenti oculari, dilatazioni delle pupille, informazioni tecniche come indirizzo ip etc.), generalmente trasferendo via *internet* i dati a *server* remoti e poi trattati per successive analisi.
La telemetria può essere realizzata, in particolare, utilizzando servizi di analisi integrati per il monitoraggio degli eventi, registrando *log* sia sul *browser* che sul *server*; attraverso API *Application Programming Interface* di telemetria remota e flussi UDP *User Datagram Protocol*.
I videogiochi sono quindi ambienti unici, veri e propri **"laboratori naturali", in cui il comportamento dei giocatori può essere innescato intenzionalmente e poi monitorato a sua insaputa**.
Impiegando avanzate metodologie di analisi dei dati, basate anche sull'apprendimento automatico o sull'Intelligenza artificiale, i dati forniti direttamente e consapevolmente dagli interessati sono elaborati con i dati grezzi da essi prodotti inconsapevolmente nell'interazione con il gioco (telemetria) e raccolti a loro insaputa per **inferirne informazioni comportamentali**. Informazioni quindi che non sono in nessun modo, né implicito né esplicito, fornite dagli interessati ma desunte dal titolare sulla base di specifiche analisi.
Queste invasive (specie per la loro opacità) operazioni di trattamento, sono generalmente volte: al miglioramento del gioco, alla monetizzazione e al *marketing*, alla personalizzazione e customizzazione del prodotto, alla prevenzione di frodi e sicurezza.
Su questa base, e avvicinandosi così ai suoi obiettivi di indirizzo, il Documento passa al **SESTO AMBITO DI APPROFONDIMENTO (le principali minacce e i più probabili rischi ai quali i dati sono esposti nelle diverse fasi del ciclo di vita di un videogame**).
A tal proposito, nel Documento si procede osservando che gli editori e le piattaforme di videogame possono collegare diverse informazioni riferite al medesimo interessato, anche generate e fornite in contesti differenti, per crearne un **profilo estremamente raffinato** (***linkability***).
Attraverso l'uso (ad esempio) di *cookies* o *web beacons* i giocatori possono essere tracciati nelle diverse sessioni di gioco **anche se non sono loggati**. Può contribuire al tracciamento il *nickname* del giocatore impiegato in differenti giochi e piattaforme così come alcune sue caratteristiche univoche.
Non sono solo i dati raccolti e generati nel contesto del gioco che contribuiscono alla profilazione dell'utente ma **anche dati esterni a tale ecosistema; si pensi, quindi, ai profili *social* con i quali sempre più spesso le piattaforme di gioco invitano gli utenti a collegarsi**.
Ebbene, tutto ciò offre alla piattaforma di gioco la possibilità unica di creare, ad insaputa dell'utente e attraverso sofisticati strumenti di analisi dei dati, dei **profili molto specifici e dettagliati dei giocatori, esponendoli a rischi di**

ISSN 2239-8570

sfruttamento, manipolazione e discriminazioni tanto all'interno quanto all'esterno del contesto ludico dove questi profili sono generati.
Nell'ambito dell'ecosistema del gioco risulta quindi quasi impossibile per l'utente evitare il rischio di identificazione. Non solo l'utente fornisce spesso personalmente dati identificativi diretti per la creazione di un *account* ma la sua identità (se non il suo profilo) è, come visto, spesso rapidamente **desumibile dall'incrocio con altre informazioni** anche esterne alla piattaforma o dall'elaborazione di informazioni inferite.
Il rischio di identificazione evolve e si concretizza in un episodio di cd "***doxing"*** quando vengono pubblicamente divulgate informazioni private relative a una persona che intendeva mantenerle riservate.
In un contesto nel quale hanno (inaspettatamente) luogo operazioni di trattamento anche molto invasive per i diritti e le libertà fondamentali degli interessati, il rischio, più che concreto, di inesattezza dei dati può accrescere la pericolosità dei trattamenti (***inaccuracy***).
L'interazione di un giocatore con un videogame può essere discontinua o "frettolosa" per cui è verosimile che le informazioni ad esso riferite siano inesatte o diventino presto obsolete; così come è verosimile che ne vengano inferite di sbagliate. Tutto ciò si riverbera sull'utente oltre che sulla qualità della sua esperienza di gioco.
Si pensi, a titolo esemplificativo, ai rischi collegati alla verifica dell'età che se condotta in maniera inaccurata può, non solo, escludere soggetti adulti dal prendere parte a giochi a loro rivolti ma soprattutto consentire indebitamente l'accesso di minori a contenuti vietati; o ancora ai dati di telemetria volti a personalizzare i contenuti da presentare agli utenti che in caso di inesattezze possono vedersi offerte esperienze di gioco del tutto incoerenti con le loro preferenze.
L'ecosistema del videogame diventa un'enorme banca dati composta dalla registrazione e conservazione costante e progressiva di dati e comportamenti dell'utente e quindi una solida catena di prove delle azioni compiute che questi non può contestare (***non-repudiation***).
I meccanismi di non ripudio determinano l'impossibilità di negare in modo plausibile qualsiasi azione o comportamento anche involontario. Ciò, specie nel caso di correlata violazione del principio di esattezza dei dati, può comportare gravi conseguenze sociali, legali e di stigmatizzazione sia all'interno che all'esterno dell'ambiente di gioco.
Come tutti i *data base* anche quelli dei videogame sono inoltre esposti a concreti rischi di ***data breach,*** verosimilmente destinati a produrre un impatto elevato sui diritti e le libertà fondamentali degli interessati.
Le piattaforme di gioco espongono gli interessati al rischio di trattamenti ingannevoli (***deception***) principalmente per fini economici.
Strumenti come **"*dark patterns*", modelli di *design* ingannevoli e tecniche manipolative** vengono impiegati per influenzare il comportamento dei giocatori fino a indurli ad adottare decisioni che diversamente non avrebbero preso, ivi incluse quelle di condividere informazioni particolarmente delicate.
L'efficacia di queste tecniche fa spesso leva sulla vulnerabilità psicologica o sui *bias* cognitivi degli utenti che, in vario modo sedotti (attraverso, ad

ISSN 2239-8570

esempio, l'offerta di ricompense), possono variare le proprie emozioni, sottoscrivere abbonamenti o a "cliccare" su annunci pubblicitari.
Attraverso le pratiche manipolative, generalmente, l'utente è inconsapevolmente spinto a compiere attività che possono produrre effetti negativi. Ne costituiscono un sottoinsieme i modelli volti a creare dipendenza (**come il gioco su appuntamento o il "*grinding*") che inducono l'utente a trascorrere molto più tempo sulle piattaforme digitali di quanto sia salutare o fisiologico** che facciano, aumentando conseguentemente le occasioni per la piattaforma di raccogliere dati personali, in una spirale del tutto viziosa e negativa per l'inconsapevole giocatore.
È evidente quindi come i giocatori possano essere facilmente indotti a condividere e fornire a loro insaputa molte più informazioni di quelle effettivamente necessarie allo scopo (***data disclosure***).
È invero fondamentale **distinguere tra i dati forniti consapevolmente dagli utenti e quelli inferiti o raccolti implicitamente (tramite telemetria o analisi comportamentale)**. Mentre infatti sui primi gli interessati possono esercitare un controllo attivo, sui secondi (che per altro sono spesso idonei a rivelare informazioni altamente sensibili) sono naturalmente privi di poteri di intervento, a totale detrimento della loro autodeterminazione informativa.
Al riguardo, **è segnalato il crescente uso delle neurotecnologie nel contesto del *gaming*** (cd ***neurogaming***) ed in particolare delle BCI (*Brain-Computer Interfaces*) tanto "attive" - che consentono ai giocatori di addestrare il sistema ad associare una specifica azione immaginata o strategia mentale a un comando di gioco ben definito - quanto "passive" (sistemi neuroadattivi) -che monitorano continuamente gli stati cognitivi o emotivi (come il coinvolgimento, lo *stress* o la fatica) del giocatore per adattare la difficoltà, il ritmo o il contenuto del gioco alle sue (dedotte) esigenze.
Si tratta quindi di forme di gioco che per loro stessa natura comportano la raccolta e il trattamento di (neuro)dati degli utenti.
Ma sono ancora molte altre le informazioni che un giocatore si trova più o meno consapevolmente a condividere nel *gaming* (dati desunti da altre *app* presenti sul dispositivo, dati di geolocalizzazione, persino dati di terzi) che i titolari sovente trasferiscono a soggetti terzi stabiliti in ogni parte del mondo.
Alla limitazione, se non assenza, di ogni forma di consapevolezza e possibilità di controllo e intervento da parte degli interessati sui loro dati trattati dalle piattaforme di gioco e all'opacità dei sistemi di raccolta, si somma generalmente l'inadeguatezza delle informative sul trattamento dei dati personali (***unawareness and unintervenability***).
A dispetto di quanto richiesto dalla normativa vigente tali documenti sono spesso prolissi, redatti con un linguaggio complesso o impiegano formule vaghe che non consentono agli interessati di comprendere gli aspetti essenziali del trattamento, come la relativa base giuridica o le modalità di esercizio dei diritti.
La natura di soggetti vulnerabili, l'elevato livello di coinvolgimento, l'alfabetizzazione digitale limitata e l'attenzione del settore alla raccolta e alla monetizzazione dei loro dati rende i soggetti minori di età la categoria di interessati maggiormente esposta ai rischi sopra richiamati e per questo

ISSN 2239-8570

meritevoli di maggior tutela (***threats to children and other vulnerable players***).
In carenza di adeguate cautele, i rischi di *privacy* che si possono verificare nel contesto del *gaming* possono determinare conseguenze molto gravi per i giovani interessati, come furto d'identità, perdita di reputazione e discriminazione, sia attuale che futura, bullismo e persino stigmatizzazione e abusi.
L'ascesa dei modelli *free-to-play* (F2P) e delle microtransazioni espone i minori a pressioni di *marketing* che potrebbero non essere in grado di gestire. Un *design* ingannevole può sfruttare tali vulnerabilità, ad esempio creando l'impressione che i giocatori che non effettuano determinati acquisti all'interno del gioco rimangano esclusi da contenuti esclusivi o vantaggi o incoraggiando acquisti impulsivi, fino a contribuire alla dipendenza dal gioco d'azzardo.
Sulla base dei risultati di questo imponente lavoro di ricognizione, il Documento assolve dunque alla sua funzione, dedicandosi al **SETTIMO E ULTIMO AMBITO DI APPROFONDIMENTO** per fornire **specifiche raccomandazioni e indicando talune buone prassi** impiegabili da titolari e responsabili del trattamento dei dati personali nell'ecosistema dei videogame in ciascuna delle fasi rilevanti e per ciascuna tipologia di videogiochi, di dati personali e di trattamenti come delineati nel medesimo Documento.
Le Raccomandazioni fanno salvo, naturalmente il principio di *accountability* e gli obblighi di *privacy by design* e *by default* statuiti dal GDPR, ai sensi dei quali, il titolare è chiamato ad individuare le misure tecniche e organizzative più adeguate al contesto di riferimento.
Le Raccomandazioni partono **dalla fase di pre-produzione e produzione**, in quanto è solo affrontando sin dalla progettazione tutte le implicazioni di protezione dei dati personali che una determinata attività, nel caso di specie la creazione di un videogame, può determinare che si assicura l'effettivo rispetto della normativa applicabile.
I soggetti coinvolti nella fase in esame sono, in primo luogo, chiamati a definire i propri ruoli di protezione dei dati quali titolari o responsabili, avendo a mente le responsabilità che ne conseguono.
Per ogni specifica attività di trattamento (*rectius* finalità perseguita) le Raccomandazioni chiedono che venga (pre)definito il ruolo assunto, considerando che la realtà fattuale ben può cumulare in capo allo stesso soggetto pluralità di ruoli, funzioni e responsabilità.
Il Documento assume quindi le sembianze di **un vero e proprio manuale** nella misura in cui suggerisce che, **prima della creazione** di un nuovo gioco, ogni soggetto coinvolto (fornitori di *hardware;* creatori, *designer* e sviluppatori; fornitori di tecnologie per lo sviluppo dei giochi; editori; distributori) passi per un "***GDPR role gate***". Nello specifico, per tutti i trattamenti di dati personali necessari allo scopo, preventivamente censiti, ciascun soggetto è chiamato a rispondere ad una serie di domande che lo aiuteranno a meglio comprendere il proprio ruolo. Infine, è richiamata l'attenzione sull'importanza che gli (eventuali) accordi di contitolarità (ex art. 26 GDPR) e gli atti di nomina dei responsabili del trattamento (ex art. 28 del Regolamento) siano, se del caso, correttamente adottati e sottoscritti.

ISSN 2239-8570

Prima del rilascio del videogame, il titolare dovrebbe **predisporre un inventario** che ricomprenda **tutte le categorie di dati trattati** durante l'intero ciclo di vita del gioco, distinguendo i dati comuni da quelli inerenti alle particolari categorie, il cui trattamento non dovrebbe di regola essere ammesso.

Il successivo passaggio richiede la puntuale e circoscritta **definizione degli scopi** che si intende perseguire con i predetti dati e una verifica, non solo della relativa liceità, ma anche dell'effettiva necessità e della proporzionalità del tempo di conservazione.

L'effettiva applicazione dei principi di limitazione delle finalità e della conservazione e di minimizzazione dei dati è invocata, in particolare, in relazione ai trattamenti di telemetria o inferenza, ammissibili, ad esempio, solo in relazione a finalità specifiche, quali la "necessità tecnica".

Il titolare del trattamento dovrebbe assicurare che l'*hardware*, i sistemi operativi, le tecnologie di sviluppo e le relative funzionalità siano progettati così da garantire per impostazione predefinita i principi di minimizzazione e di limitazione della conservazione dei dati.

In omaggio al principio di *accountability*, le decisioni assunte andrebbero **registrate in apposite *checklist* o *data dictionary***, anche al fine di facilitare il compimento degli ulteriori adempimenti richiesti dal GDPR (es. informativa agli interessati, registro dei trattamenti, valutazione di impatto).

Da ultimo, quindi, va individuata la **base giuridica** idonea a supportare la raccolta e i successivi trattamenti necessari agli scopi che si intendono perseguire.

Tenendo a mente che tra le condizioni di liceità del trattamento di cui all'art. 6 del GDRP non esiste alcuna relazione gerarchica, il titolare dovrà farsi guidare dal principio di necessità per la scelta di quella in concreto più idonea, fermo restando che i dati personali raccolti per una finalità non possono essere ulteriormente utilizzati in modo incompatibile, se non in presenza di una distinta base giuridica.

Il documento suggerisce come ulteriore misura per assicurare effettiva applicazione al principio di *accountability* una **"*mappa scritta del ciclo di vita dei dati*"**, che illustri come ciascuna categoria di dati entri nell'ecosistema del videogame, venga trattata, conservata, trasferita, archiviata e cancellata, offrendo altresì l'indicazione di ulteriori e specifiche misure tecniche e organizzative che andrebbero, in determinati casi, implementate per impostazione predefinita.

La mappatura del dato all'interno dell'ecosistema del videogioco si dimostra particolarmente utile in quanto è più che verosimile che i dati dei giocatori vangano anche trasferiti a soggetti terzi stabiliti fuori dal territorio dell'Unione, nonché per evitare che, anche per l'effetto dell'impiego di *Software Development Kit* (per arginare i rischi dei quali il documento indica specifiche misure), si crei un fenomeno di scatole cinesi (o "effetto matrioska"), che porti alla perdita del controllo delle informazioni trattate.

Se è vero che la normativa in materia di protezione dei dati personali prevede specifici obblighi di *privacy by design* e *by default*, sono quindi onerati al loro rispetto anche i creatori, designer e sviluppatori dei videogame, per i quali essi rappresentano un vero e proprio "**vincolo creativo**", un parametro

ISSN 2239-8570

fondamentale della progettazione, che definisce quali meccaniche siano ammissibili senza un trattamento sproporzionato dei dati personali dei giocatori. Anche in questo caso il documento fornisce numerose indicazioni esemplificative.

Creatori, *designer* e sviluppatori per migliorare l'esperienza immersiva del videogame, vi integrano sempre più spesso NPC *Non-Player Character (Personaggio Non Giocante),* basati sull'intelligenza artificiale. Attraverso gli NPC è possibile elaborare i dati dei giocatori (es. messaggi di *chat*, comandi vocali, scelte di gioco e modelli comportamentali) per generare, ad esempio, risposte o adattare le narrazioni. A tal fine, non solo, sono richieste una specifica base giuridica, un'informativa agli interessati e il rispetto di tutti gli altri principi sanciti dal GDPR, ma per un principio di equità, devono altresì essere evitati esiti discriminatori da parte dei modelli di IA.

Inoltre, fermo restando che l'eventuale addestramento degli NPC basati sull'IA con dati relativi alle interazioni dei giocatori (*log* delle *chat*, scelte, modelli vocali, ecc.) comporta un nuovo e distinto scopo di trattamento (con tutte le conseguenze in termini di verifica della relativa liceità e degli ulteriori adempimenti connessi), il documento suggerisce come tale finalità ben potrebbe essere perseguita attraverso l'uso di **dati sintetici** o comunque impiegando svariati accorgimenti per minimizzare l'uso di quelli identificativi dei giocatori.

Attengono alla fase *design* anche le misure volte ad evitare che le interfacce di gioco e gli accordi contrattuali consentano o nascondano modelli ingannevoli o che creino dipendenza.

Così, ad esempio, i titolari del trattamento devono progettare le interfacce assicurando che l'accettazione e revoca di determinate scelte possano essere espresse con lo stesso livello di facilità, **evitando caselle preselezionate, tecniche di "*confirmshaming*" o opzioni di rinuncia mascherate**.

Deve essere limitata la conservazione dei dati (di gioco) dell'utente (ad esempio, le ultime 3 sessioni) per impedire la creazione di *dossier* che possano consentire deduzioni relative a punti deboli o vulnerabilità (ad esempio, segnali di dipendenza, *stress* finanziario) idonei a rivelare aspetti molti intimi degli interessati.

Particolare attenzione è rivolta ai cd **"*loot box*", "pacchetti misteriosi"**, spesso collocati all'interno dei videogiochi di cui l'interessato non conosce il contenuto ma solo la tipologia (comuni, rari, epici, etc.) e che possono essere ottenuti giocando o tramite acquisto diretto. Essi **si fondano sul principio del rinforzo a frequenza variabile, lo stesso che sta alla base delle *slot machine***: i premi sono imprevedibili, il che stimola fortemente il sistema di ricompensa del cervello e spinge i giocatori a continuare a provare **"*ancora una volta*" sviluppando tratti di impulsività, bisogno di novità o tendenze al gioco d'azzardo**.

Secondo il Documento (p. 51), nei casi in cui non sia addirittura equiparabile al gioco d'azzardo, **i titolari dovrebbero quanto meno vietare tale prassi ai minori e renderla facoltativa per il resto dei giocatori**.

Anche gli **"elementi cosmetici"**, pur non influenzando direttamente il *gameplay*, come la creazione e personalizzazione dell'immagine e dei profili degli *avatar,* può incidere sulla dipendenza dal gioco. La scelta di elementi

ISSN 2239-8570

come la *skin* e gli abiti di tali personaggi può, infatti, contribuire all'identificazione del giocatore con il personaggio stesso, che ne riconosce un'espressione (virtuale) di sé.

Sono diverse le pulsioni e le motivazioni che spingono ogni singolo giocatore a "investire" sul proprio *avatar* (sperimentazione, espressione di sé, prestigio sociale) ma facendo leva su ciascuna di queste le piattaforme possono indurre il giocatore ad azioni o transazioni, ripetute e compulsive.

Il documento raccomanda, quindi, il preventivo svolgimento di un *UX test* (***usability test***) per individuare e quindi evitare modelli ingannevoli, atti a creare dipendenze.

Per tutto quanto sopra, i trattamenti di dati personali svolti nell'ecosistema dei videogame sono considerati come "ad alto rischio" e quindi meritevoli di una preventiva **valutazione di impatto** ai sensi dell'art. 35 del Regolamento.

I **minori** sono i principali utenti delle piattaforme di gioco, questo onera i titolari del trattamento ad un atteggiamento particolarmente corretto che tenga concretamente conto della vulnerabilità e dell'assenza di strumenti di difesa solidi rispetto alle minacce sopra descritte nonché delle loro specifiche abilità cognitive nella comprensione dei documenti informativi che devono quindi essere appositamente adattati. Alcune delle funzionalità tipiche dei videogiochi (tra cui i canali di comunicazione pubblici, gli algoritmi di suggerimento degli amici, le interazioni basate sulla posizione, le realtà aumentate (AR) basate sulla fotocamera, gli *avatar* e le microtransazioni non trasparenti come i *loot box*) risultano particolarmente rischiose per i minori.

Tutto ciò implica, ad esempio, che anche i videogame espressamente pensati per un'utenza adulta siano rispettosi dei diritti dei minori, attraverso strumenti di *parental control* o verifica dell'età, e che, quando spetta agli esercenti la potestà genitoriale esprimere il consenso per i minori ex artt. 8 GDPR e 2-*quinquies* d.lgs. 30 giugno 2003, n. 196 (**Codice in materia di protezione dei dati personali** o **Codice**), siano implementate misure atte a garantire l'effettiva applicazione di tale previsione nel rispetto altresì del principio di minimizzazione.

I creatori, i progettisti e gli sviluppatori devono quindi preventivamente valutare la compatibilità di un gioco con il cd *best interest of the child* e se del caso prevedere delle misure che, per impostazione predefinita, ne riducano l'impatto sui diritti dei minori, rafforzando al contempo la sicurezza, la *privacy* e la conformità al GDPR.

Uno dei trattamenti maggiormente rischiosi per i minori è rappresentato dalla profilazione comportamentale (e dalla pubblicità) finalizzata alla monetizzazione. In questo senso, tutti gli attori del settore dovrebbero adottare un approccio "***safe-by-default***" (sicuro per impostazione predefinita), ad esempio disabilitandola esplicitamente per gli utenti generici che non dimostrino di aver superato una soglia di età richiesta.

La **fase di lancio** del gioco segna il momento in cui esso da mero progetto diventa realtà operativa e quindi i principi di protezione dai dati devono materialmente ora concretizzarsi nelle interfacce, nelle impostazioni, negli *user journeys*, nei flussi di monetizzazione e nei sistemi di *backend*.

ISSN 2239-8570

Il documento ribadisce l'importanza di determinare i ruoli di protezione dei dati già definiti nella fase di pre-produzione e produzione, suggerendo nuovamente delle "domande guida" per i soggetti coinvolti.
All'avvio di un nuovo videogame, gli interessati devono essere chiaramente informati dei trattamenti di dati personali che questo comporta (***embedding transparency in the player experience***).
Il GDPR richiede ai titolari che le informative siano concise, trasparenti, intelligibili, facilmente accessibili e rese con un linguaggio semplice e chiaro ma non ne impone una forma precisa. In questa libertà il documento riconosce una grande opportunità per i titolari che possono adattare le modalità di adempimento più adeguate al peculiare contesto di riferimento. I giochi offrono un enorme margine creativo per integrare la trasparenza, anziché relegarla a un testo legale statico e nascosto in una sezione remota del sito.
In particolare, è fortemente raccomandato l'inserimento graduale dei concetti relativi alla *privacy* nel processo di *onboarding*; così facendo l'interessato, piuttosto che venire sopraffatto da informazioni che sarebbe portato a tralasciare per loro lungaggine, viene progressivamente edotto delle implicazioni di *privacy* del gioco nel pieno rispetto del principio di trasparenza.
In concreto ciò potrebbe essere realizzato attraversò la presentazione progressiva e continua di "etichette sulla privacy", ferma restando la possibilità per i giocatori interessati di richiedere o accedere alle informazioni più dettagliate che potrebbero essere rese auspicabilmente reperibili presso "Centri o *Hub* dedicati alla privacy" appositamente creati.
Massima trasparenza è raccomandata infine sia rispetto alla telemetria, attraverso la creazione di appositi cataloghi, che alle *loot box*, ggetto di sempre maggiore attenzione da parte delle autorità di regolamentazione europee.
Al momento del lancio, e per l'instaurazione di un clima di fiducia, i titolari del trattamento devono attuare meccanismi di consenso solidi, che soddisfino i requisiti per un consenso valido ai sensi degli articoli 4, paragrafo 11, e 7 del GDPR (***obtaining valid consent***).
È raccomandata quindi la visualizzazione di ***banner*** dettagliati e separati prima dell'inizio del gioco, con chiare indicazioni in ordine alla raccolta di dati telemetrici, alla profilazione, alla condivisione con terze parti e alle diverse finalità perseguite (es. funzionalità *social*, monetizzazione). I titolari del trattamento dovrebbero utilizzare il "***meccanismo clickwrap***" per la raccolta del consenso e le opzioni di scelta fornite all'interessato devono essere chiare ed equilibrate, con pulsanti di attivazione/disattivazione separati per ciascuna categoria.
Tutti gli attori che partecipano all'ecosistema dovrebbero creare uno schema o un dizionario degli *account* ed eseguire *script* di verifica per garantirne l'aggiornamento e verificare periodicamente che non vengano raccolti o conservati dati eccedenti, disponendo la cancellazione automatica degli *account* inattivi dopo un periodo prestabilito.
Come detto non è solo nella fase di creazione dell'*account* che vengono raccolti i dati personali dei giocatori, durante l'esperienza di gioco infatti i dati sono continuamente generati dall'utente, raccolti e ulteriormente trattati

ISSN 2239-8570

dalla piattaforma. Ciò è ammesso a condizione che ogni flusso sia funzionale al perseguimento di una specifica e predefinita finalità e supportato da un'idonea condizione di liceità. A tal fine, i titolari del trattamento dovrebbero fissare uno schema di telemetria e inferenza di produzione ammesse, una *whitelist*, rifiutando quindi aggiornamenti o *hotfix* che aggiungano eventi o attributi non documentati o arbitrari (***ensuring purpose limitation and data minimisation during gameplay***).

È indispensabile che i titolari del trattamento facciano una chiara distinzione tra i trattamenti di dati personali necessari per consentire l'esperienza di gioco e quelli necessari solo alla monetizzazione, che generalmente richiedono il preventivo consenso degli interessati.

Eventuali offerte mirate o prezzi personalizzati basati sul comportamento degli utenti o su dati di telemetria (il cui impiego deve comunque essere ridotto al minimo) devono essere rappresentati chiaramente, evitando meccanismi che sfruttino *bias* cognitivi o altre vulnerabilità, integrando trattamenti opachi di profilazione manipolativa o, in generale altre, pratiche sleali.

Al contrario, le piattaforme di gioco dovrebbero promuovere il benessere dei giocatori, inserendo punti di controllo, salvataggi automatici e pause naturali (*timer* di sessione, messaggi che suggeriscono di fare una pausa) per limitare un coinvolgimento eccessivo (***aligning monetisation mechanics with GDPR principles).***

La peculiarità dell'ecosistema dei videogame si apprezza anche rispetto alle modalità con le quali gli interessati dovrebbero poter esercitare facilmente i propri diritti di protezione dei dati. L'esercizio dei diritti in generale avviene tramite moduli *web* o richieste via e-mail, queste modalità potrebbero risultare inefficaci nel (video)gaming dove essi dovrebbero, più efficacemente, essere considerati come elemento dell'esperienza di gioco, a prescindere dalla piattaforma o dal dispositivo utilizzato (***facilitating the exercise of data subject rights through player-centric interfaces).***

La quantità ed eterogenia di dati raccolti e generati nel contesto dei videogame potrebbe complicare la corretta gestione delle istanze di accesso ai dati. A fronte di una richiesta di accesso, i titolari non dovrebbero inondare gli interessati di enormi e incomprensibili quantità di dati grezzi, fornendo invece (o anche consentendo il *download* dagli *account*) dati strutturati accompagnati se del caso da note esplicative e/o riassuntive. Ciò al fine di consentire ai giocatori di comprendere cosa stia realmente accadendo ai propri dati personali e in che modo ciò possa influenzare la loro esperienza di gioco (***the right of access*****,** art. 15 GDPR).

Ai rischi, sopra richiamati, che possono derivare dall'inaccuratezza dei dati, segue l'importanza di garantire ai giocatori effettiva applicazione al diritto di rettifica degli stessi. I titolari del trattamento devono progettare sistemi in grado di rispondere alle richieste di rettifica che non compromettano l'integrità del *gameplay* né aprano la strada ad abusi. È quindi necessario fornire ai giocatori indicazioni chiare su quali dati possano o non possano essere rettificati e perché (***the right to rectification***, art. 16 GDPR).

Nei giochi, l'effettiva applicazione del diritto di cancellazione spesso si complica per i complessi insiemi di dati relativi alla progressione, ai grafici

ISSN 2239-8570

sociali, agli acquisti e agli inventari raccolti durante l'esperienza di gioco; i titolari del trattamento devono, in ogni caso, implementare misure adeguate a soddisfare le richieste degli interessati, nonché notificarle a eventuali terzi destinatari dei dati. I giocatori dovrebbero essere informati, in un linguaggio semplice, su ciò che accade all'esito della cancellazione dei dati: se i loro progressi andranno persi definitivamente, se le loro comunicazioni saranno rimosse o rese anonime, se la cronologia degli acquisti dovrà essere conservata temporaneamente per motivi legali e se alcuni elementi (ad esempio, transazioni irreversibili all'interno del gioco) non potranno essere annullati.

La **cancellazione** dovrebbe, in linea di principio, essere semplice quanto la creazione dell'*account* stesso. Per i minori e, ove necessario, i tutori, deve essere disponibile la possibilità di avviare la cancellazione tramite una *dashboard* genitoriale, in linea con il requisito dell'articolo 8 del GDPR, secondo cui il consenso e di conseguenza anche la sua revoca, ove il minore abbia un'età inferiore ai sedici anni (quattordici per il contesto italiano secondo quando disposto dall'articolo 2-*quinquies* del Codice), deve essere prestato o autorizzato dal titolare della responsabilità genitoriale (***the right to erasure,*** art. 17 GDPR)**.**

Anche il **diritto alla limitazione del trattamento** (art. 18 GDPR)può svolgere un ruolo cruciale nei sistemi interattivi come i videogiochi a tutela della posizione dei giocatori allorché, ad esempio, venga contestata l'accuratezza dei dati o la liceità dei trattamenti. Attraverso il diritto di limitazione l'interessato può ottenere la sospensione di processi di analisi dei dati non essenziali o di profilazione comportamentale per la durata di un eventuale contenzioso, scaturito ad esempio in ragione della classificazione operata da modelli *anti-cheat* o di rilevamento della tossicità.

Per l'effettiva applicazione di tale diritto, i titolari del trattamento devono progettare meccanismi interni per contrassegnare e isolare i dati soggetti a limitazione, al fine di impedirne un utilizzo involontario nelle operazioni in corso (***the right to restrict access***, art. 18 GDPR).

Nella pratica la richiesta di **"migrazione" – portabilità - di dati tra ecosistemi di gioco** è piuttosto rara, ciononostante anche tale diritto deve essere garantito agli interessati anche perché può comunque svolgere funzioni importanti favorendo l'apertura e la trasparenza dei videogiochi, fermi restando i diritti di proprietà intellettuale o i termini di licenza. Ad esempio, i giocatori potrebbero voler esportare i propri registri di progressione, i dati storici delle partite, gli inventari degli oggetti cosmetici o i grafici per utilizzarli altrove (es. applicazioni complementari).

I gestori dovrebbero quindi fornire formati di esportazione di dati ben strutturati, con metadati descrittivi e documentazione che spieghino come i *file* possano essere interpretati, e semplici strumenti di portabilità quali pulsanti «esporta i miei dati» con anteprime nei formati più comuni (***the right to data portability,*** art. 20 GDPR).

È fondamentale garantire effettiva applicazione al diritto di opposizione nell'ecosistema dei videogame, in particolare in relazione alle funzionalità facoltative quali offerte personalizzate, iniziative mirate di fidelizzazione, sistemi di raccomandazione e profilazione.

ISSN 2239-8570

Tramite interfacce chiare ed intuitive, integrate fin dalla progettazione nelle meccaniche di gioco l'interessato dovrebbe poter rinunciare a tali trattamenti a meno che la relativa prosecuzione non sia giustificata da una chiara eccezione. Gli editori e le piattaforme di distribuzione dovrebbero implementare un "registro centrale delle opposizioni" che blocchi la telemetria o le inferenze comportamentali su tutti i giochi offerti, in caso di reinstallazione.

Si raccomanda, inoltre, ai gestori di non considerare le richieste di opposizione come mere preferenze, sottolineandone il valore giuridicamente vincolante e di progettare le interfacce evitando di dissuadere i giocatori dall'opposizione (***the right to object,*** art. 21 GDPR).

Nell'ecosistema dei videogame vengono assunte molte "decisioni automatizzate" che incidono sui giocatori, si pensi al blocco delle frodi, alle sanzioni *anti-cheat*, ai livelli di *matchmaking*, rispetto alle quali non solo deve essere garantita la massima trasparenza - con riferimento, in particolare, alle logiche applicate e ai criteri decisionali -, ma devono anche essere resi disponibili canali di revisione umana entro un ragionevole lasso di tempo, es. 24/48 ore (***automated individual decision-making, including profiling, in live environments,*** art. 22 GDPR).

Il Documento individua, infine, raccomandazioni e buone prassi nella **fase di post- produzione** dei videogame, quando le implicazioni di protezione dei dati personali non sono più da progettare ma da gestire in modo concreto.

Una volta che il gioco è *online* infatti ogni aggiornamento, revisione del sistema, tentativo di monetizzazione etc. comporta specifiche implicazioni in materia di protezione dei dati, richiedendo, in particolare, una costante rivalutazione dei rischi del trattamento anche in base all'evoluzione della tecnologia impiegata.

La natura dinamica dei videogiochi implica in questa fase una particolare responsabilità dei soggetti coinvolti che si articola su tre direttrici: i. aggiornamenti continui ed evoluzione delle funzionalità; ii. *governance* e sicurezza dei dati costanti; iii. rispetto di standard legali ed etici nella fase conclusiva del ciclo di vita del gioco.

Nuovamente il Documento riporta quindi le domande operative alle quali ciascun soggetto coinvolto in questa fase nel ciclo di vita del videogame dovrebbe rispondere per individuare il proprio ruolo di protezione dei dati.

La natura dinamica del gioco può aumentare il rischio di "***purpose creep***", ossia di trattamenti dei dati per scopi differenti e incompatibili con quello della raccolta. Anche piccoli cambiamenti nel modo in cui viene interpretata la telemetria o nelle persone legittimate all'accesso ai dati, possono alterare nel tempo la natura e la portata del trattamento, in violazione del principio di limitazione della finalità di cui all'articolo 5, paragrafo 1, lettera b) del GDPR.

Questo fenomeno è particolarmente comune nel videogame per la grande quantità di dati prodotti in questo ecosistema e per gli interessi commerciali ivi perseguiti; i titolari del trattamento dovrebbero, pertanto, condurre revisioni strutturate e periodiche di ciascuna attività di trattamento svolta per verificarne la pertinenza rispetto alla finalità originaria, interrompendo il

ISSN 2239-8570

trattamento ovvero individuando specifiche condizioni di liceità per trattamenti volti al perseguimento di scopi nuovi e differenti.
In tale quadro, sono suggerite, come buona prassi, **campagne di rinnovo del consenso,** attesi anche i frequenti cambiamenti delle condizioni del consenso stesso o l'evoluzione delle legittime aspettative degli interessati in un ambiente mutevole.
La copiosa produzione di dati che ha luogo nell'ecosistema dei videogame richiede altresì una scrupolosa e periodica verifica della corretta applicazione dei principi di minimizzaione e limitazione della conservazione.
L'individuazione di dati adeguati, pertinenti e limitati allo scopo della raccolta così come del periodo di conservazione necessario e sufficiente al suo perseguimento deve essere considerata come un processo dinamico e progressivo piuttosto che un adempimento *una tantum.* Ciò anche al fine di intervenire attraverso la cancellazione o anonimizzazione delle informazioni che dovessero risultare obsolete e non più necessarie.
Una corretta gestione del ciclo di vita del dato all'interno dei videogame passa, da un punto di vista culturale, nel rifiuto della tendenza del cd "***keep data just in case***" e da, un punto di vista tecnico, per l'implementazione per impostazione predefinita di misure per la cancellazione.
In base al principio di *accountability* i titolari devono inoltre procedere alla mappatura del flusso dei dati previsto nel sistema del videogame e a una costante rivalutazione dei rischi. I giochi *online* subiscono spesso modifiche strutturali che alterano in modo ora impercettibile ora significativo i percorsi dei dati; in entrambi i casi le misure tecniche ed organizzative implementate per l'effettiva applicazione dei principi di protezione dei dati vanno verificate in punto di adeguatezza, auspicabilmente nell'ambito di una specifica valutazione di impatto, soprattutto se tali cambiamenti, ancorché minimi, coinvolgano soggetti minori di età.
Una particolare attenzione deve essere rivolta all'integrità e riservatezza dei dati, atteso che il contesto dei videogame è per sua natura altamente rischioso (appropriazione indebita di *account*, reti di *bot*, frodi con carte di credito, attacchi di *credential stuffing*)
Le misure di sicurezza dovrebbero includere: i. monitoraggio continuo di comportamenti anomali; ii. revisioni periodiche dei livelli di accesso; iii. analisi delle vulnerabilità, esercitazioni interne di *penetration testing* o *red teaming*; iv. revisioni periodiche dei *software*.
La complessità delle sfide per una corretta protezione dei dati personali nell'ecosistema dei videogame richiede un approccio strutturato che includa comitati interni per la protezione dei dati, *audit* e revisioni interdisciplinari nonché una documentazione standardizzata per ogni nuova attività di trattamento.
I titolari devono poter mantenere un vigile e serio controllo sulla catena di soggetti coinvolti nelle operazioni di trattamento: i responsabili dovrebbero essere sottoposti a specifici *audit* prima dell'incarico e ulteriori garanzie dovrebbero essere previste in apposite clausole contrattuali che prevedano l'imposizione di *audit*, l'obbligo di notifica delle violazioni e l'approvazione o il divieto di nominare sub-responsabili.

ISSN 2239-8570

Risulta inoltre fondamentale una seria diffusione della cultura della *privacy* nel mondo del videogame che preveda una formazione mirata per ciascuno dei soggetti coinvolti nel ciclo di vita del gioco in base alle diverse funzioni svolte.
Il dinamismo dell'ecosistema del gioco dovrebbe riflettersi sul registro dei trattamenti che i titolari (o se del caso i responsabili) dovrebbero curare come documento interattivo, utile quale punto di partenza per un coretto svolgimento e adattamento di tutto gli altri obblighi derivanti dal GDPR.
Anche ai responsabili della protezione dei dati deve quindi essere assicurata una partecipazione sostanziale e integrata nei processi di *governance* e decisionali, sicché ogni eventuale loro osservazione, specie se negativa, non dovrebbe essere considerata come mera consulenza formale ma tenuta in debita considerazione.
Anche la fase finale di un gioco presenta sfide significative rispetto all'applicazione del GDPR. Se un gioco viene "chiuso", infatti, gli interessati devono essere preventivamente e puntualmente informati in ordine alla sorte dei loro dati che dovrebbero di regola essere cancellati o anonimizzati: disabilitando l'accesso al gioco; pulendo i *database* sottostanti; rendendo anonimi o cancellando gli archivi di dati; inviando istruzioni di cancellazione a tutti i responsabili del trattamento terzi e richiedendo una conferma al riguardo.

CHIARA DI SOMMMA
Funzionario presso il Garante della protezione dei dati personali.
Quanto riportato e le opinioni espresse nel contributo impegnano solo l'autore

Recommendations and best practices for data protection in video games

2026/2(20)AG
Le Linee guida del Garante privacy italiano del 17.4.2026 sull'utilizzo di tracking pixel nelle comunicazioni di posta elettronica

Con provvedimento del 17.4.2026, il Garante per la protezione dei dati personali ha emanato Linee guida sull'utilizzo diffuso di *tracking pixel* da parte dei fornitori dei servizi della società dell'informazione, dei provider di servizi di posta elettronica e dei gestori di piattaforme per l'inoltro massivo di messaggi e-mail.
Si tratta di strumenti occulti, **non identificabili dagli interessati**, consistenti in minuscoli **frammenti di codice, nascosti soprattutto sotto forma di immagini trasparenti di un solo pixel** e **incorporati nelle e-mail**. Queste immagini, a seguito dell'apertura del messaggio di posta elettronica e di un sofisticato processo tecnico, **vengono archiviate nella memoria del terminale dell'interessato**. Di conseguenza, il mittente del messaggio o uno dei suoi partner ottiene informazioni utili sui seguenti dati: 1) conferma di apertura della e-mail; 2) indirizzo IP; 3) dati tecnici quali il tipo di dispositivo (computer o smartphone), il sistema operativo e il browser utilizzato; 4) tempo di permanenza dedicato alla lettura di un contenuto, così da desumere

ISSN 2239-8570

gli interessi del destinatario onde potergli rivolgere ulteriori comunicazioni commerciali.

In sostanza, i *tracking pixel* **sono strumenti di tracciamento («marcatori») e di acquisizione di informazioni sui comportamenti degli utenti e sulle modalità di fruizione dei servizi da parte degli stessi**. Il loro utilizzo, come vedremo meglio in seguito, è necessario sia per migliorare il servizio offerto sia per consentire al soggetto tenuto per legge all'invio di messaggi istituzionali o di servizio di avere contezza dell'effettivo adempimento del suo obbligo. Sono, questi, «scopi legittimi» di impiego di tale tecnologia: cfr. cons. 24-25 direttiva 2002/58/CE (**direttiva e-privacy**). Al contempo, però, vi è il rischio connaturato all'impiego dei *tracking pixel* della raccolta di dati personali all'insaputa del destinatario della e-mail, sulla base dei quali si costruiscono profili della personalità, categorizzazioni del singolo utente, identificato tramite il suo IP, funzionali al suo sfruttamento commerciale. Emerge, perciò, il pericolo più allarmante della tecnologia digitale, ossia la strumentalizzazione della persona umana, la quale verrebbe indotta ad acquistare beni, che pure gli interessano, per effetto, però, di un comportamento scorretto da parte del mittente.

La direttiva e-privacy, opportunamente, a proposito di questi strumenti che penetrano nelle apparecchiature terminali degli utenti di reti di comunicazione elettronica, sottolinea la «grave intrusione nella vita privata dell'utente» (cons. 24), qualora non vengano rispettate le prescrizioni di legittimità del loro utilizzo.

Prima di individuare la disciplina applicabile agli strumenti di tracciamento – oltre ai *tracking pixel* ve ne sono altri quali il *cookie*, il *fingerprinting*, il *web beacon*, lo *script*, il *widged* e altri ancora –, le Linee guida sottolineano due aspetti: 1) i pixel di tracciamento non attengono al contenuto del messaggio, monitorando esclusivamente l'evento dell'avvenuta apertura e consultazione della e-mail da parte di un utente specifico (si consideri che il mittente viene a conoscenza anche del tempo della consultazione e del numero di aperture successive della stessa e-mail); 2) il pixel di tracciamento è scaricabile nella e-mail dell'utente solo se è stata mantenuta abilitata la funzione di download delle immagini; diversamente, se è attiva la funzione di lettura della e-mail solo in formato testo, il *tracking pixel*, al pari delle altre immagini, non potrà essere scaricato.

Descritto il fenomeno in sintesi, quanto alla relativa disciplina, le Linee guida richiamano anzitutto l'art. 122 del d.lgs. n. 196/2003 (**codice privacy**), introdotto nell'ordinamento nazionale a seguito del recepimento della direttiva e-privacy. L'**art. 122 comma 2-*bis* codice privacy** pone il divieto di «uso di una rete di comunicazione elettronica per *accedere* a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per *archiviare* informazioni o per *monitorare* le operazioni dell'utente. Emergono, quindi, i profili dell'accesso ai dati altrui e del monitoraggio dell'attività online del destinatario della e-mail. Non è un divieto assoluto, bensì limitato ai casi di utilizzo di strumenti di tracciamento non giustificati da una delle previsioni di cui al comma 1; la disposizione di cui al comma 2-*bis* è infatti preceduta dall'inciso «salvo quanto previsto dal comma 1», che prevede tre casi di deroga al divieto.

ISSN 2239-8570

I casi di deroga previsti dell'art. 122, co. 1 codice privacy sono i seguenti, ai sensi: a) se vi è stato il previo rilascio del consenso da parte del destinatario della comunicazione elettronica, dopo aver ricevuto informazioni sullo strumento di tracciamento «con modalità semplificate» (cfr. *amplius infra*); b) se ricorrono fattispecie in cui il trattamento dei dati personali del destinatario sia *necessario*, *consenta* o *faciliti* l'effettuazione della «trasmissione di una comunicazione su una rete di comunicazione elettronica»; c) se le operazioni di tracciamento appaiano necessarie alla fornitura di un servizio di comunicazione online «esplicitamente richiesto dal contraente o dall'utente».

Il divieto di intrusione nell'apparecchio terminale di un utente, letto unitamente alle condizioni legittimanti l'uso dei *tracking pixel – id est*: le tre deroghe –, segnala il rilievo pubblicistico dei beni giuridici protetti: la libertà di scelta dell'utente, il diritto di non essere sfruttato a propria insaputa e il diritto di essere informato sull'impiego dei marcatori. L'art. 122 codice privacy protegge, quindi, la persona umana, sia come singolo sia come facente parte di una collettività. Al contempo tale articolo favorisce lo sviluppo tecnologico, il miglioramento dei servizi offerti e la comunicazione con i destinatari delle e-mail.

Come si diceva innanzi, poiché l'art. 122 codice privacy è stato introdotto dalla direttiva e-privacy, le Linee guida sottolineano come, per effetto dell'entrata in vigore del GDPR (successivo a tale direttiva), si sia posto un problema di coordinamento tra il GDPR, fonte di carattere generale sul trattamento dei dati personali, e la direttiva e-privacy. Per risolverlo, occorre muovere – lo rilevano le Linee guida – dal cons. 173 GDPR, il quale evoca il criterio *lex specialis derogat legi generali*, nell'affermare che il regolamento «si applic[a] a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE (…), compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche». Si accorda, dunque, la prevalenza alla direttiva e-privacy, la quale, se rende più specifiche le prescrizioni del GDPR, prevarrà sulle disposizioni generali del GDPR. Il quale viene in rilievo soprattutto con le sue disposizioni sui principi fondamentali relativi al trattamento dei dati personali (art. 5) e sugli obblighi informativi (artt. 13 ss.).

Come si vedrà a breve, sono proprio le disposizione di carattere generale del GDPR a essere decisive in punto di liceità del trattamento dei dati personali desunti tramite l'impiego di *tracking pixel*, di doveri informativi propedeutici al consenso quale deroga al divieto di utilizzo di strumenti di tracciamento e dei ruoli dei diversi soggetti coinvolti nell'utilizzo di questa tecnologia.

Venendo ai **soggetti coinvolti nell'impiego dei *tracking pixel* e ai modelli di invio dei messaggi,** le Linee guida richiamano anzitutto due articoli del GDPR: l'art. 26 sui contitolari del trattamento e l'art. 5(2) sul principio di *accountability* rispetto all'attuazione dei principi fondamentali di cui al paragrafo 1 del medesimo articolo. Ciò al fine di sottolineare che i diversi soggetti coinvolti «devono definire i propri ruoli rilevanti dal punto di vista delle norme in materia di protezione dei dati personali, anche eventualmente

ISSN 2239-8570

alla luce della disposizione di cui all'art. 26 del Regolamento [il GDPR] sulla contitolarità del trattamento dei dati» (cfr. § 3 p. 6 Linee guida).
Rinviando per maggiori dettagli alla lettura delle Linee guida, queste ultime individuano sei soggetti a cui riferire il tracciamento e il trattamento dei dati personali ed esattamente: - **il mittente del messaggio di posta elettronica**, ossia il soggetto pubblico o privato che invia la comunicazione, decidendo di usare pixel di tracciamento e determinandone le finalità, sebbene la gestione dello strumento possa essere demandata a terzi; - **il fornitore di servizio di invio e-mail** è colui che rende disponibile al committente la soluzione tecnica, compresa la piattaforma per effettuare l'invio delle e-mail e che agisce su mandato e secondo le istruzioni del mittente, il quale utilizza liste proprie di contatti di destinatari; - **il fornitore di servizi di noleggio di liste di distribuzione e invio di e-mail** è colui che offre in locazione le proprie liste di distribuzione al committente, per conto del quale avviene anche l'invio dei messaggi; - **il fornitore della tecnologia di tracciamento** è colui che predispone lo strumento tecnico utilizzato dal mittente, perciò deve agevolare i titolari e i responsabili del trattamento nell'adempimento dei loro obblighi di protezione dei dati (cons. 78 GDPR), oltre a poter essere coinvolto, il che arricchisce la sua posizione, negli «aspetti decisionali relativi al trattamento dei dati derivante dall'uso dei marcatori in questione» (cfr. § 3 p. 6 Linee guida); il ***content creator*** è colui che cura il messaggio pubblicitario da recapitare al destinatario; **il destinatario del messaggio di posta elettronica** è il soggetto che riceve la comunicazione elettronica con all'interno l'elemento tracciante [qui le Linee guida precisano che l'indirizzo e-mail è acquisito o per effetto di una procedura di autenticazione (es: creazione di un account) oppure nel corso di una transazione commerciale online in attuazione alla deroga al comma 1 prevista dall'art. 130, co. 4, codice privacy].
Dopo l'individuazione dei soggetti, aspetto questo fondamentale per stabilire la catena del valore all'interno della quale riconoscere specifiche responsabilità, le Linee guida individuano 4 modelli ricorrenti di invio di messaggi: - **Newsletter**, consistenti in comunicazioni periodiche di aggiornamento ai destinatari iscritti in una lista di contatti; - **DEM (Direct E-mail Marketing)**, ossia comunicazioni commerciali inviate a gruppi di destinatari selezionati dal cliente della piattaforma, nell'ambito di liste di contatti già nella sua disponibilità, oppure selezionati dal provider dotato di liste proprie a beneficio di terzi committenti a scopo di marketing; - **E-mail transazionali e messaggi automatici** sono comunicazioni inviate automaticamente al verificarsi di certi eventi (come nel messaggio di benvenuto) o a seguito di una specifica azione compiuta dall'utente o di una transazione in corso (come le conferme di registrazione o d'ordine); **E-mail di servizio**, contengono messaggi funzionali a soddisfare specifiche esigenze del singolo o della collettività.
Quanto agli **obblighi informativi**, le Linee guida accentuano l'importanza della preventiva informazione sullo strumento di tracciamento, al fine di ottenere un consenso effettivo all'utilizzo. Il suo nascondimento espone il destinatario di posta elettronica alla etero-direzione del volere e alle conseguenze di una condotta del mittente da ritenersi senz'altro scorretta.

ISSN 2239-8570

Viene allora in rilievo il fondamentale principio di **correttezza** di cui all'art. 5 par. 1 lett. a) GDPR. Inoltre – continuano le Linee guida (§ 4) –, valorizzando il riferimento normativo all'informazione di cui all'art. 122, co. 1 codice privacy, si deve ritenere che un sistema di tracciamento, per qualificarsi lecito, «de[bba] essere preventivamente reso noto al destinatario della e-mail, qualunque sia lo scopo della comunicazione o la tipologia del soggetto mittente». C'è uno stretto collegamento tra il principio di correttezza e il principio di **trasparenza** previsto dal medesimo art. 5 par. 1 lett. a) GDPR.

Secondo le Linee guida, l'informativa potrà essere fornita su più livelli: a) attraverso l'inserimento in forma sintetica dell'informativa in un modulo di raccolta dell'indirizzo e-mail, prevedendo un link con un'informazione più dettagliata (anche dentro la *cookie policy*); b) tramite canali video, *pop-up* informativi, interazioni vocali, assistenti virtuali e altro ancora indicato nelle Linee guida.

È onere del titolare del trattamento verificare la completezza, chiarezza espositiva e fruibilità del sistema informativo rispetto al requisito di trasparenza previsto dal GDPR.

Le Linee guida si diffondono sulla questione delle **basi giuridiche del trattamento dei dati personali tracciati diverse dal consenso.** Sono stati già sopra richiamati i tre presupposti legittimanti l'impiego dei sistemi di tracciamento, in deroga al divieto di utilizzo di questi ultimi (art. 122 co. 1 codice privacy). A questo proposito, le Linee guida si soffermano in particolare sui due presupposti diversi dal consenso, soprattutto perché vi è un numero rilevante di casi a essi riconducibile. L'esigenza fondamentale che si pone è quella di contemperare l'impiego dei sistemi di tracciamento con la protezione dei dati personali e quindi della privacy.

I casi di utilizzo dei *tracking pixel* senza il consenso del destinatario della e-mail, indicati nelle Linee guida, sono giustificati dall'esigenza di migliorare il servizio o dalla necessità per il mittente di avere contezza che il destinatario abbia ricevuto certe informazioni. Se ne indicano di seguito alcuni: a) al fine di effettuare indagini statistiche per migliorare i servizi di posta elettronica (*deliverability* delle e-mail). In tale eventualità si devono adottare, tuttavia, tecniche di anonimizzazione delle informazioni, così da non consentire misurazioni personalizzate, ossia concentrate su singoli utenti in modo da desumerne abitudini e gusti. Si suggerisce l'impiego di pixel univoci, cioè di pixel che non siano differenti per ciascun utente, quindi uguali per tutti i destinatari di una stessa campagna, «come pure l'anonimizzazione degli altri dati tecnici correlati» (indirizzo IP, client, etc.); b) se il mittente deve sapere che la e-mail sia stata effettivamente aperta, come nella gestione di una richiesta di modifica della password; c) messaggi istituzionali o di servizio che un determinato soggetto ha l'obbligo di inoltrare (ad es.: una banca) e rispetto ai quali rilevi l'effettiva conoscenza del destinatario; d) notifiche di sicurezza, *reminder* su scadenze e adempimenti contrattuali e contributivi e altro ancora (*amplius* § 5 Linee guida).

In questi e in altri casi riportati dalle Linee guida, la deroga al consenso del destinatario della comunicazione elettronica è giustificata dall'esistenza di un beneficio conoscitivo per il destinatario stesso. Vi è anche un interesse

ISSN 2239-8570

economico-aziendale del mittente ad approntare un sistema di comunicazione elettronica più efficiente, redditizio e sicuro possibile.

Infine, le Linee guida si rivolgono alla base del **consenso.** Qualora il mittente del messaggio non possa prescindere dal consenso per utilizzare i *tracking pixel*, egli deve acquisirlo preventivamente. Le Linee guida si soffermano sui casi che esigono il consenso, individuandone diversi (cfr. *amplius* § 6). Tra questi vi è quello in cui dall'analisi del tasso di apertura delle e-mail, il mittente intenda ricavare «informazioni presunte circa i potenziali gusti, gli interessi e le preferenze attribuibili all'utente allo scopo di creare profili commerciali utilizzabili anche per iniziative diverse». Ancora: gli strumenti di tracciamento sono particolarmente utili, sempre a fini commerciali, qualora l'analisi del dato del tasso di apertura sia adoperato per valutare e migliorare la performance delle campagne promozionali. Così, ad esempio, se vi è un numero basso di aperture delle e-mail, il mittente potrà agire sul messaggio di accompagnamento o sul sito qualora il tempo di navigazione sia esiguo.

A questo punto, le Linee guida tornano sull'acquisizione del consenso, distinguendo due ipotesi comuni a ogni fonte regolativa del diritto: a) se i trattamenti di dati che postulano l'inoltro di e-mail con *tracking pixel* vengano intrapresi successivamente all'entrata in vigore delle Linee guida; b) se questi trattamenti siano già in corso alla data di entrata in vigore delle Linee guida (si pensi al caso dell'inoltro periodico di newsletter).

Nel primo caso, si stabilisce che il consenso si raccolga al momento dell'acquisizione dell'indirizzo di posta elettronica, dopo che l'interessato sia stato debitamente informato nel modo innanzi indicato (*supra* § 3). In questa fase di raccolta, colui che intenda tracciare deve stare attento a procurarsi un consenso valido. A tal proposito sono da evitare «ridondanti richieste di consenso plurime», che si sostanziano in pressioni indebite sul volere. Per una condotta corretta – qui la certezza del diritto è fondamentale per entrambe le parti – è sufficiente ricomprendere il consenso al *tracking pixel* «in quello più generale alla ricezione delle comunicazioni promozionali, in modo da consentire che la persona esprima a tal fine un unico consenso informato». Ciò però deve avvenire «in modo neutro e privo di forzature, nel rispetto della manifestazione di volontà dell'interessato».

Deve, quindi, essere chiaro con immediatezza visiva che la e-mail conterrà meccanismi di tracciamento della propria attività, il che esige di precisare anche la finalità del trattamento dei relativi dati personali (il cons. 25 direttiva e-privacy prescrive di rendere informazioni «sugli scopi dei marcatori», l'art. 5 § 3 della stessa direttiva menziona gli «scopi del trattamento»).

Le Linee guida stabiliscono altresì che deve essere agevolata la **revoca del consenso**, il cui oggetto può essere anche parziale rispetto al consenso originario, ossia con riguardo al solo tracciamento connesso alla ricezione di *tracking pixel* e non anche alle comunicazioni di posta elettronica prive di tale strumento.

La revoca va garantita anche in modo granulare, il che avviene ad esempio inserendo all'interno di ogni messaggio e-mail inviato una icona standardizzata o un link, posizionato nel *footer* (cioè a piè di pagina), che conduca l'utente in un'area specifica dedicata all'esercizio dei diritti. Qui potrà avvenire quella scissione della revoca di cui si è appena detto.

ISSN 2239-8570

Nel secondo caso (tracciamenti già in corso), il titolare del trattamento deve adempiere ai propri obblighi informativi «con il primo invio utile o comunque nel primo momento di discontinuità disponibile allo scopo»; occorre anche implementare e rendere noto agli utenti un meccanismo che permetta loro la revoca, anche granulare, del consenso. Ogni soluzione – è il principio da applicare per sostenere la libertà del consenso – deve essere improntata «alla massima riconoscibilità, visibilità e facilità d'uso a beneficio dell'interessato».
A chi rifiuti il *tracking pixel* dovrà essere comunque garantita la piena fruibilità del servizio.
Le scelte dell'interessato devono essere registrate dal titolare, anche ai fini della prova che quest'ultimo può essere chiamato a fornire, specialmente in caso di controversie, secondo quanto dispone l'art. 7 GDPR sulle condizioni per il consenso.
Le Linee guida si concludono con un suggerimento agli utilizzatori di mezzi di tracciamento, a protezione dei destinatari della comunicazione elettronica; una protezione sul piano della privacy e della non induzione al consumo, basata su un'insufficiente protezione dei dati personali. Il mittente potrà generare «un identificativo inintellegibile e non sequenziale e associ[arlo] all'indirizzo di posta elettronica del destinatario, mantenendo tale corrispondenza in un *layer* interno e separato della piattaforma utilizzata». In questo modo l'indirizzo e-mail non sarà ricompreso nella richiesta tecnica generata dal caricamento del pixel. Con la conseguenza di ridurre l'esposizione dell'indirizzo e-mail e di minimizzare il rischio di identificabilità dei dati che transitano nella rete.
I destinatari delle Linee guida hanno a disposizione **6 mesi dalla pubblicazione in Gazzetta ufficiale, avvenuta il 29 aprile 2026**, per adeguarsi a quanto previsto.

ANTONIO GORGONI

Testo ufficiale

2026/2(21)GD
La Corte di giustizia dell'Unione europea conferma in via definitiva la maxi-sanzione da 4,1 miliardi di euro inflitta a Google per abuso di posizione dominante nel caso Android (sentenza del 2.7.2026, causa C-738/22 P, *Google e Alphabet c. Commissione – Google Android*)

Con la sentenza del 2.7.2026, la Corte di giustizia dell'Unione europea, Seconda Sezione (la **Corte UE**), ha respinto integralmente l'impugnazione proposta da Google LLC (**Google**) e dalla capogruppo Alphabet Inc. avverso la sentenza del Tribunale dell'Unione europea del 14.9.2022 (causa T-604/18), rendendo così definitiva la sanzione di 4,125 miliardi di euro per abuso di posizione dominante ex art. 102 TFUE nell'ambito del sistema operativo Android. Si chiude così, dopo otto anni, uno dei più rilevanti contenziosi antitrust promossi dalla Commissione europea nei confronti di una Big Tech.

ISSN 2239-8570

La vicenda trae origine dalla decisione della Commissione europea del 18.7.2018 (caso AT.40099 – *Google Android*), con cui era stata irrogata a Google un'ammenda di 4.342.865.000 euro per aver abusato della propria posizione dominante imponendo ai produttori di dispositivi mobili Android e agli operatori di rete mobile una serie di restrizioni contrattuali volte a proteggere e rafforzare la posizione del motore di ricerca Google Search.

In particolare, la Commissione aveva censurato: (1) gli accordi di distribuzione delle applicazioni (*Mobile Application Distribution Agreements* – MADA), che subordinavano la licenza del Play Store alla pre-installazione di Google Search e del browser Chrome (c.d. *tying*); (2) gli accordi c.d. anti-frammentazione (*Anti-Fragmentation Agreements* – AFA), che impedivano ai produttori di commercializzare dispositivi basati su versioni di Android non approvate da Google (c.d. *fork*); (3) gli accordi di ripartizione dei ricavi (*Revenue Share Agreements* – RSA), che condizionavano taluni pagamenti alla pre-installazione esclusiva di Google Search.

In primo grado, il Tribunale UE aveva sostanzialmente confermato l'impianto della decisione, qualificando le condotte come infrazione unica e continuata, ma aveva annullato la parte relativa agli RSA c.d. "di portafoglio", rideterminando la sanzione – nell'esercizio della propria competenza estesa al merito – in 4,125 miliardi di euro, di cui 1,521 miliardi a carico di Alphabet in solido con Google.

Con la pronuncia in commento, la Corte UE ha respinto tutti i motivi di impugnazione, in linea con le conclusioni dell'Avvocata generale Juliane Kokott del 19.6.2025. Tre passaggi meritano particolare attenzione.

In primo luogo, la Corte UE ha stabilito che il Tribunale non è incorso in errori di diritto nel valutare gli effetti anticoncorrenziali delle condizioni di preinstallazione, potendo legittimamente considerare il contesto economico nella sua interezza (ivi compresi gli RSA) senza dover svolgere sistematicamente un'analisi controfattuale per accertare l'abuso. La Corte UE ha altresì confermato l'esistenza di una distorsione a favore dello *status quo* (c.d. *status quo bias*): gli utenti tendono a utilizzare le applicazioni preinstallate sui propri dispositivi, sicché la preinstallazione costituisce di per sé un potente vantaggio competitivo, che Google non ha dimostrato essere riconducibile alle preferenze degli utenti o alla superiore qualità dei propri prodotti.

In secondo luogo, la Corte UE ha chiarito che il test del concorrente altrettanto efficiente (*as-efficient competitor test*) non costituisce un elemento obbligatorio dell'onere probatorio della Commissione: nei mercati digitali di tipo "ecosistema" – caratterizzati da effetti di rete, accesso ai dati, plurilateralità ed elevate barriere all'ingresso – la stessa emersione di un concorrente altrettanto efficiente può risultare, in concreto, impossibile, sicché pretendere la prova della sua esclusione priverebbe di effettività il divieto di cui all'art. 102 TFUE.

In terzo luogo, la Corte UE ha respinto le giustificazioni obiettive addotte da Google a sostegno degli obblighi anti-frammentazione, confermando che la tutela dell'integrità dell'ecosistema Android non poteva legittimare restrizioni che ostacolavano lo sviluppo e la distribuzione di sistemi operativi concorrenti.

ISSN 2239-8570

Google ha preso atto della decisione – avverso la quale non sono esperibili ulteriori mezzi ordinari di impugnazione, salvi i rimedi straordinari (*e.g.*, la revocazione ex art. 44 dello Statuto, esperibile solo in caso di scoperta di un fatto decisivo anteriore alla sentenza e ignoto alla Corte e alla parte) – criticandone il merito e osservando che la sentenza non riconoscerebbe gli investimenti compiuti per mantenere Android aperto, interoperabile e gratuito. Di segno opposto la reazione delle associazioni dei consumatori: il BEUC ha parlato di un chiaro messaggio alle imprese dominanti, sottolineando al contempo la necessità di strumenti di regolazione *ex ante* come il *Digital Markets Act* per prevenire sul nascere le pratiche sleali.

La pronuncia in commento si presta ad alcune riflessioni comparatistiche rispetto alla parallela vicenda statunitense *Stati Uniti d'America c. Google LLC*. Come illustrato in questa Rubrica (v. contributo n. 27 del numero 4/2025 [2025/4(27)GD], in *PeM* 2025, p. 1114), la Corte del Distretto della Columbia, con la sentenza del 5.8.2024, ha accertato l'abuso di posizione dominante di Google nelle ricerche online e, con la successiva pronuncia sui rimedi del 2.9.2025, ha escluso la cessione forzata di Chrome, imponendo la condivisione di parte dei dati di ricerca con i concorrenti e il divieto di accordi di distribuzione esclusiva.

Il primo parallelismo attiene all'oggetto: su entrambe le sponde dell'Atlantico il nodo centrale è il medesimo, ossia l'uso della distribuzione predefinita di Google Search e Chrome – mediante preinstallazione, esclusive e pagamenti ai partner – quale leva per proteggere la posizione dominante nella ricerca generale online. Ed entrambe le giurisdizioni riconoscono il potere dei *default*: lo *status quo bias* valorizzato dalla Corte UE trova un preciso omologo nell'accertamento del giudice Mehta circa l'efficacia escludente dei contratti che assicuravano a Google la posizione di motore di ricerca predefinito.

Il secondo profilo – di divergenza – attiene ai rimedi. Il modello statunitense è puramente comportamentale e prospettico: nessuna sanzione pecuniaria, ma obblighi di condivisione dei dati, divieto di esclusive e monitoraggio affidato a un Comitato tecnico per sei anni. Il modello europeo, per contro, si fonda sulla sanzione pecuniaria dissuasiva (qui la più elevata mai irrogata in materia antitrust dalla Commissione) accompagnata dall'ordine di cessazione della condotta, cui si affianca oggi – in chiave preventiva – l'apparato di obblighi *ex ante* del *Digital Markets Act*. Non a caso, la sanzione in commento si aggiunge a quelle già inflitte a Google nei casi *Google Shopping* (2,42 miliardi di euro, confermata definitivamente nel 2024) e *ad tech* (2,95 miliardi di euro, settembre 2025).

Il terzo profilo attiene ai tempi e allo stato dei rispettivi contenziosi: mentre la vicenda europea giunge a un approdo definitivo dopo otto anni dalla decisione della Commissione (e a distanza di oltre un decennio dall'avvio delle condotte contestate, risalenti al 2011), la battaglia americana è ben lontana dall'essere conclusa, avendo Google annunciato l'impugnazione della pronuncia sui rimedi. Il confronto evidenzia, peraltro, un limite comune ai due sistemi: la fisiologica lentezza dell'enforcement antitrust rispetto alla rapidità evolutiva dei mercati digitali, oggi già trasformati dall'avvento dell'intelligenza artificiale generativa – fattore che il giudice Mehta ha

ISSN 2239-8570

espressamente valorizzato nella calibrazione dei rimedi e che rende il quadro competitivo della ricerca online assai diverso da quello in cui le condotte sanzionate furono poste in essere.

GIORGIA DIOTALLEVI

Testo ufficiale
Press release

2026/2(22)GB
La sentenza della Corte di giustizia UE nelle cause riunite C-188/24 (WebGroup Czech Republic e NKL Associates) e C-190/24 (Coyote Systems) su servizi della società dell'informazione: gli Stati membri possono esigere la verifica dell'età degli utenti di siti pornorafici e vietare la diffusione di informazioni relativi a determinati controlli operati, per motivi di ordine pubblico, sicurezza o incolumità pubblica, sul traffico stradale

Con la sentenza del 16 giugno 2026 nelle cause riunite C-188/24 e C-190/24 (la **Sentenza**), la Corte di giustizia dell'Unione europea (**CGUE** o la **Corte**) è intervenuta su alcune questioni rilevanti in materia di servizi della società dell'informazione, e perciò per le attività degli *Internet service provider* regolati a livello unionale dalla dir. 2000/31/CE (**direttiva sul commercio elettronico** o la **Direttiva**), e a livello statale da specifiche norme di settore degli Stati membri.
La Sentenza trae origine da due distinte domande di pronuncia pregiudiziale del Conseil d'État (**Consiglio di Stato**) originate in altrettante controversie francesi relative alla legittimità e annullamento di due decreti ministeriali rispetto al diritto dell'Unione: 1) il decreto n. 2021-1306, del 7 ottobre 2021, attuativo della legge n. 2020-936, del 30 luglio 2020 volta a proteggere le vittime di violenza domestica, che è relativo alle modalità di attuazione delle misure volte a tutelare i minori dall'accesso a siti che diffondono contenuti pornografici, e che in particolare precisa l'operatività della diffida ad un servizio di comunicazione al pubblico online che consente l'accesso ai minori in violazione dell'articolo 227-24 del codice penale francese che punisce la creazione, il trasporto e la diffusione di messaggi pornografici; 2) il decreto n. 2021-468, del 19 aprile 2021, recante l'applicazione dell'articolo L. 130-11 del codice della strada francese, che autorizza l'autorità amministrativa competente, in presenza di minaccia per l'ordine e la sicurezza pubblica, a vietare ad un operatore di un servizio elettronico di ausilio alla guida o alla navigazione mediante geolocalizzazione di diffondere informazioni che informino l'utente di un controllo pubblico in atto, in modo da evitare comportamenti elusivi di tale controllo. **In Francia i prestatori di servizi dell'informazione che forniscono contenuti pornografici sono così tenuti a predisporre dispositivi per la verifica dell'età e impedire efficacemente ai minori di accedere ai contenuti**. **Gli operatori che forniscono servizi alla guida, invece, possono essere soggetti a divieti di diffondere informazioni su controlli pubblici compiuti dallo stato sul territorio in modo da evitare le condizioni utili all'utente ad eludere la norma**, ad esempio quando ricercato o sottoposto a provvedimento.

ISSN 2239-8570

Il primo decreto è oggetto del caso tra WebGroup Czech Republic, a.s. e la NKL Associates s.r.o., ossia due editori di siti Internet che diffondono contenuti pornografici accessibili in Francia, ma stabiliti nella Repubblica ceca a Praga, e, dall'altro, il Ministre de la Culture (Ministro della Cultura) e il Premier ministre (Primo ministro) della Repubblica. Nel 2021 queste società ricevettero una diffida ai sensi del decreto n. 2021-1306 sulla base del fatto che l'accesso al loro servizio conseguiva ad una mera dichiarazione di avere almeno diciotto anni di età. Le società contestarono la diffida adendo in prima e ultima istanza il Consiglio di Stato sostenendo la violazione dell'articolo 3 della direttiva sul commercio elettronico per mancata notifica della normativa interna (legge e decreto) alla Commissione e alla Repubblica Ceca e per il mancato rispetto degli obiettivi della regolazione europea che tutelano la libera circolazione dei servizi. I ricorrenti sostenevano che le regole francesi imponevano dispostivi tecnici di blocco dell'accesso ai servizi di contenuto pornografico ai minori in violazione della Direttiva e alla libera circolazione dei servizi. Il Consiglio di Stato perciò rivolgeva alla Corte le tre questioni pregiudiziali così riassunte in estrema sintesi: 1) se le disposizioni di diritto penale francese dovevano essere considerate rientranti nell'oggetto di applicazione della direttiva sul commercio elettronico, potendo applicarsi anche ad un prestatore di servizi della società dell'informazione, o se fossero non applicabili perché il settore penale non è stato oggetto di armonizzazione; 2) se l'imposizione di predisporre dispositivi destinati a prevenire l'accesso di minori a contenuti pornografici doveva considerarsi rientrante nell'ambito della Direttiva, limitato a specifici ambiti armonizzati, come la responsabilità dei prestatori, la cooperazione tra gli Stati e, quindi non riguardanti il comportamento concreto dell'operatore; 3) in caso di risposta affermativa alle precedenti questioni, come l'adozione di tali misure verso un singolo servizio si poteva conciliare con la tutela dei diritti fondamentali prevista nella Carta di Nizza, che comprende anche la tutela della dignità umana e l'interesse del minore (artt. 1 e 24).

Il secondo decreto è invece oggetto della controversia tra la Coyote System, con sede in Francia, che fornisce un servizio rientrante nell'ambito dell'articolo L. 130-11 del codice della strada francese, quale operatore di un servizio elettronico di ausilio alla guida o alla navigazione tramite geolocalizzazione, e il Ministre de l'Intérieur et des Outre-mer (Ministro dell'Interno) e il Primo ministro. La società adiva il Consiglio di stato per l'annullamento del secondo decreto e dell'articolo del codice della strada in quanto incompatibili per la Direttiva e in particolare con la non presenza di un obbligo generale di sorveglianza sulle informazioni trasmesse dai prestatori di servizi della società dell'informazione (art. 15). Anche in questo caso il Consiglio di Stato rivolgeva tre questioni pregiudiziali qui sinteticamente richiamabili: 1) se il divieto imposto agli operatori di un servizio elettronico di ausilio alla guida o alla navigazione mediante geolocalizzazione di diffondere le informazioni sui controlli in atto doveva considerarsi rientrante nell'ambito della Direttiva benché relativo al comportamento del fornitore e non agli aspetti specifici armonizzati; 2) se il menzionato divieto doveva considerarsi rientrante nell'ambito degli obblighi relativi all'esercizio dell'attività di servizi della società dell'informazione che

ISSN 2239-8570

uno Stato membro non può imporre a fornitori provenienti da un altro Stato membro; 3) se il divieto di imporre un obbligo generale di sorveglianza previsto dalla Direttiva poteva considerarsi ostacolo all'applicazione di un dispositivo di limitazione alla diffusione di categorie di informazioni all'utente, senza che l'operatore conosca il contenuto.

La Corte decide di esaminare congiuntamente le cause perché sostiene che in sintesi il Consiglio di Stato si domanda se la Direttiva sia di ostacolo ad uno Stato membro nell'imporre ai prestatori di servizi della società dell'informazione stabiliti in altri Stati membri un obbligo generale e astratto rientrante nel diritto penale (causa C-188/24), e a prevedere un divieto di diffusione di informazioni relative a determinati controlli stradali (causa C-190/24).

La Corte richiama, in primo luogo, il **principio del controllo dello Stato membro di origine e di riconoscimento reciproco, da cui si rileva che i prestatori sono soggetti al diritto dello Stato membro di stabilimento** (nel primo caso concreto la Repubblica ceca e non la Francia). Successivamente la Corte analizza l'«**ambito regolamentato**» come definito dall'art. 2, let. h) della Direttiva e chiarisce che la norma comprende **«tutte le prescrizioni previste dagli ordinamenti giuridici degli Stati membri in relazione all'accesso all'attività di servizi della società dell'informazione o al suo esercizio, ad eccezione di prescrizioni come quelle applicabili alle merci in quanto tali, alla consegna delle merci e ai servizi non prestati per via elettronica»**. L'ambito non è limitato alle materie regolamentate per non pregiudicare gli obiettivi della Direttiva. Le normative generali e astratte rientranti nel diritto penale e quelle che perseguono obiettivi di ordine pubblico, sicurezza o incolumità pubblica fanno così parte dell'ambito e sono connesse all'accesso all'attività di servizi della società dell'informazione e loro esercizio. Non riguardando le merci, non sono esplicitamente escluse e non rientrano nelle altre deroghe di applicazione previste nell'Allegato alla Direttiva, le quali hanno carattere esaustivo. **Le normative di diritto penale, pur essendo escluse dall'armonizzazione, possono rientrare nell'ambito regolamentato che peraltro lascia liberi gli stati nazionali ad applicare le loro norme penalistiche agli *Internet service provider*. Gli Stati membri possono adottare provvedimenti necessari alla salvaguardia dell'ordine pubblico e della pubblica sicurezza ai sensi dell'articolo 3 della Direttiva.**

La Corte, perciò, adotta un'**interpretazione ampia dell'ambito regolamentato ai sensi della direttova sul commercio elettronico, perché considera la disciplina non limitata alle prescrizioni e materie armonizzate, ma comprendente qualsiasi prescrizione sull'esercizio e accesso ai servizi della società dell'informazione. La Corte sostiene che un dispositivo di verifica dell'età degli utenti condiziona l'accesso degli utenti e il divieto imposto agli operatori di diffondere delle informazioni limita il servizio condizionandone il contenuto**.

In secondo luogo, la Sentenza si occupa di verificare se le normative francesi limitino la libera circolazione dei servizi protetta dalla Direttiva. Le regole risultano di fatto e in diritto limitazioni, ma l'**art. 3(4)(a) della Direttiva** consente di derogare al principio, quindi ad uno Stato diverso da quello di origine, e a determinate condizioni, ossia **per la tutela dell'ordine pubblico,**

ISSN 2239-8570

della sanità pubblica, della pubblica sicurezza e della tutela dei consumatori e solo per determinati individuali servizi. Ai sensi della disposizione di cui alla successiva lettera (**art. 3(4)(b) della Direttiva**) si richiede la notifica dei provvedimenti nazionali alla Commissione e al diverso Stato membro, che porterebbe all'invito a quest'ultimo a adottare provvedimenti e non rimanere inattivo.

A parere della Corte, **sia la normativa a tutela dei minori che quella sulla circolazione stradale corrispondono alle condizioni della deroga per varie ragioni**. Esse **riguardano l'ordine pubblico che comprende la tutela dei minori e la pubblica sicurezza**, a cui si può ricollegare il limite alla diffusione di informazioni. Le norme statali sono **proporzionate** rispetto agli obiettivi della Direttiva e sono **dedicate a particolari servizi**. In particolare, **un dispositivo di verifica dell'età dell'utente per i siti pornografici è proporzionato allo scopo di tutelare i minori e la dignità umana, mentre il sopra specificato divieto di diffusione di informazioni è proporzionato all'obiettivo di ordine pubblico, sicurezza e incolumità pubblica**. La Corte ha poi motivato a proposito dell'orientamento giurisprudenziale per il quale provvedimenti generali non sono conformi alla normativa. In proposito, la Corte ha argomentato che l'articolo del codice penale francese è sì generale e astratto, e quindi non risulta rientrante nella portata della lett. a), ma il primo decreto **prevede una modalità individuale con l'invio di una diffida**. Questa modalità è perciò conforme alla **Direttiva e anche confinata ai particolari servizi di contenuti pornografici** governati dalla legge di cui il decreto è attuazione. Un sistema di verifica dell'età per tutti i siti non apparirebbe allora possibile.

La mancata notifica di cui alla lett. b) e richiesta all'altro Stato membro di provvedere a regolare è un obbligo procedurale. La Corte rileva che uno Stato membro può derogare all'obbligo in caso di urgenza e poi notificare al più presto. Spetterà al Consiglio di Stato la verifica di questa circostanza nel caso concreto.

Infine, la Sentenza di occupa del tema spinoso riguardante l'assenza di un obbligo di sorveglianza sulle informazioni trasmesse dai prestatori. La Corte ricorda che la Direttiva stabilisce che un *hosting provider* è esonerato dalla responsabilità se non è a conoscenza delle informazioni trasmesse e non controlla tali informazioni. Si tratta, come noto, di condizioni alternative e autonome. Da ciò rileva che anche solo il controllo, ma non conoscenza, delle informazioni, è fonte di responsabilità dell'*Internet service provider*. **La gestione tramite algoritmo delle condizioni di diffusione di informazioni all'utente è prova di controllo**, come peraltro sostenuto dall'Avvocato generale. Anche in assenza di interventi supplementari di monitoraggio, la predisposizione dell'algoritmo su quali condizioni, in quale ordine e priorità le informazioni sono diffuse è sufficiente a considerare l'operatore un prestatore di *hosting* che non può essere esonerato da responsabilità. Il divieto francese non obbliga il prestatore a una valutazione autonoma del contenuto memorizzato, come stabilito nella causa C-18/18, in cui la medesima Corte ha statuito che l'ingiunzione rivolta a un prestatore di servizi di *hosting* di rimuovere elementi precisi delle informazioni non impone a tale prestatore un obbligo di sorvegliare. L'operatore soggetto all'articolo L. 130-11 del

ISSN 2239-8570

codice della strada può conformarsi al divieto senza prendere conoscenza del divieto e con strumenti automatizzati. La Direttiva non osta al divieto di diffusione di informazioni a operatori che possono considerarsi *hosting provider* per motivi di ordine pubblico, sicurezza o incolumità pubblica.

In sintesi, **la Sentenza chiarisce che il principio del paese d'origine può riguardare anche disposizioni penali e può essere derogato per motivi di ordine pubblico, tra cui la tutela dei minori, e quindi uno Stato membro può imporre un sistema di verifica dell'età per l'accesso a siti pornografici, governato tramite una diffida anche a *Internet service provider* stabiliti in altri Stati membri, ma determinate condizioni devono essere seguite**. La regola limitativa della libertà di circolazione dei servizi deve essere proporzionata, giustificata da obiettivi generali rientranti nella Direttiva sul commercio elettronico, e deve essere individuale per un determinato servizio, non generale e astratta. Gli Stati membri dovranno quindi verificare la normativa interna di settore, soprattutto con riferimento al criterio individuale e per determinato servizio.

L'esenzione di responsabilità per chi svolge attività di *hosting* è limitata a prestatori meramente passivi, mentre l'utilizzo di algoritmi per governare lo scambio di informazioni con l'utente è considerata prova di controllo. Se vengono diffuse delle informazioni in modo illecito controllandone la modalità o quando non consentito come dal codice della strada francese, quindi, si può essere dichiarati responsabili. In particolare, nella Sentenza si trova affermato, a proposito degli - ora soppressi (v. *infra*) - artt. 14 e 15 della Direttiva, che «l'operatore di un servizio della società dell'informazione consistente in particolare nella memorizzazione di informazioni fornite da un destinatario del servizio che, mediante un algoritmo, determina, nel proprio interesse o in quello del suo servizio, a quali condizioni, in che modo e con quale ordine di priorità tali informazioni siano diffuse o meno nell'ambito di tale servizio, esercita un controllo su tali informazioni, cosicché non può essere qualificato come prestatore di un 'servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio', ai sensi di tale articolo 14, paragrafo 1, e detto articolo 15, paragrafo 1, non gli è quindi applicabile». Questa lettura della clausola di esonero della responsabilità induce a considerare ad una possibile estensione di quest'ultima rispetto al passato che la vedeva costantemente ed estremamente limitata perché riconosce che lo sviluppo e uso di algoritmi è forma di controllo. L'algoritmo non è neutrale e passivo di per sé, quindi, e si dovrà compiere una valutazione in concreto.

Si rileva, infine, che la Direttiva è stata modificata dal reg. (UE) 2022/2065 (**Digital Service Act** o **DSA**). In particolare, il DSA ha soppresso gli articoli da 12 a 15 della direttiva sul commercio elettronico (e gli artt. 14-17 del suo decreto attuativo, il d.lgs. 9 aprile 2003, n. 70, sono stati abrogati dall'art. 3(4) del d.lgs. 25 marzo 2024, n. 50), e la corrispondente nuova disciplina sulla responsabilità dei prestatori di servizi intermediari si trova negli articoli 4, 5, 6 e 8 del Digital Services Act. Di conseguenza, le questioni generali riportate e analizzate sulla responsabilità dovranno essere nuovamente confrontate con quanto prescritto dalla nuova normativa, la quale comunque mantiene le condizioni menzionate di esonero per gli *hosting provider* e il non obbligo di

ISSN 2239-8570

sorveglianza attiva. Tuttavia, al cons. 22 del DSA viene dichiarato che l'indicizzazione automatizzata e le funzioni di ricerca delle informazioni non sono considerate prove dell'attività. Inoltre, il cons. 89 del DSA indica la necessaria protezione dei minori da parte dei fornitori di piattaforme online di grandi dimensioni. Si dovrà attendere l'adeguamento nazionale e la verifica da parte degli Stati membri sulla compatibilità delle norme interne esistenti con il nuovo assetto. In ogni caso, si può anche richiamare, come ha fatto in un punto la Corte, la dir. (UE) 2018/1808 sui servizi di media audiovisivi che già considera gli strumenti per la verifica dell'età dei minori come misure a protezione del loro sviluppo fisico, mentale e morale.

GIORGIA BINCOLETTO

Testo ufficiale

2026/2(23)RMa-MCG
Il provvedimento del Garante privacy italiano n. 342 del 14.5.2026 di avvertimento nei confronti di Myndoor s.r.l. per possibile violazione del GDPR e del Codice privacy in relazione a un componente aggiuntivo per le piattaforme di messaggistica aziendale Slack e Teams finalizzato a rilevare linguaggio, emozioni e livello di stress psicologico dei lavoratori

Con il provvedimento n. 342 del 14.5.2026, il Garante per la protezione dei dati personali (il **Garante**) ha emesso un avvertimento nei confronti di *Myndoor S.r.l.*, *start-up* italiana che **ha sviluppato un *plug-in* integrabile nelle piattaforme di messaggistica aziendale *Microsoft Teams* e *Slack***.
L'applicativo utilizza **tecniche di IA e di analisi semantica – la c.d. *sentiment analysis* – per esaminare il contenuto testuale dei messaggi degli utenti e stimarne il livello di *stress* psicologico, restituendo indicazioni personalizzate per il benessere**. Il lavoratore sceglie volontariamente se attivare il servizio.
L'istruttoria, avviata d'ufficio a seguito di notizie di stampa, ha escluso che un ente pubblico inizialmente indicato avesse acquistato il servizio, spostando l'attenzione del Garante sulle modalità con cui il *plug-in* potrebbe essere impiegato dalle imprese che decidano di metterlo a disposizione del proprio personale. ***Myndoor* ha dichiarato di operare quale autonomo titolare del trattamento: il rapporto si instaura direttamente tra la società e i lavoratori che scelgono di utilizzarlo, senza che il datore di lavoro possa accedere ai contenuti delle comunicazioni né ai risultati individuali**. Il Garante ha assimilato questa configurazione ad **altri servizi di *welfare* aziendale - come le assicurazioni sanitarie o i servizi di assistenza psicologica** - in cui il datore sostiene il costo della prestazione senza acquisire informazioni sulla sua concreta fruizione.
Il principale profilo critico è la funzionalità di reportistica aggregata: **l'impresa cliente può richiedere un *report* settimanale sul livello di *stress* della propria popolazione aziendale, generabile solo in presenza di almeno dieci utenti attivi**. Nell'unico caso esaminato, non sono emersi elementi che consentissero all'azienda destinataria di risalire all'identità dei

ISSN 2239-8570

singoli lavoratori, sicché il Garante non ha accertato una comunicazione illecita né individuato specifiche responsabilità. Tuttavia, **la soglia di dieci utilizzatori non garantisce in assoluto l'anonimato**, atteso che nelle realtà di ridotte dimensioni, anche un dato statistico potrebbe consentire inferenze sullo stato psicologico dei singoli.

L'avvertimento *ex* **art. 58(2)(a) GDPR** si fonda proprio su tale rischio. Orbene, il Garante ha invitato *Myndoor* ad adottare misure tecniche e organizzative idonee a impedire che gli enti e le imprese clienti possano venire a conoscenza, anche indirettamente e attraverso i *report* aggregati, delle informazioni trattate. L'intervento richiama i principi di responsabilizzazione e di protezione dei dati fin dalla progettazione (artt. 24 e 25 GDPR): le funzionalità prive di idonea base giuridica o incompatibili con le finalità del trattamento devono essere valutate ed eventualmente disattivate già in sede di progettazione del prodotto.

In tale contesto, l'art. 113 del d.lgs. 196/2003 (**codice privacy** o il **Codice**), rinviando al divieto di raccogliere dati non pertinenti rispetto all'attività lavorativa previsto dall'**art. 8 l. n. 300/1970** (**Statuto dei lavoratori**), comporta che **le informazioni relative alla sfera emotiva dei dipendenti, e quindi al loro stato di benessere o *stress* psicologico, non possano essere conosciute dal datore di lavoro**. **Analogamente precluse sono le finalità di "medicina preventiva, diagnosi e assistenza"** indicate nell'informativa di *Myndoor*: l'**art. 5 dello Statuto dei lavoratori** vieta al datore di compiere autonomamente accertamenti sanitari sui dipendenti, e la normativa sulla salute e sicurezza (**d.lgs. n. 81/2008**) riserva tali funzioni al solo medico competente.

Il provvedimento richiama altresì l'art. 5(1)(f) del reg. (UE) 2024/1689 (**AI Act** o **AIA**), che vieta l'immissione sul mercato, la messa in servizio per tale specifica finalità o l'uso di sistemi di intelligenza artificiale destinati a inferire le emozioni nei luoghi di lavoro. Il Garante non afferma che *Myndoor* abbia violato tale disposizione - tanto più che l'**AI Act definisce il "sistema di riconoscimento delle emozioni" facendo riferimento a dati biometrici** (art. 2, nn. 39) e 34) AIA)**, mentre il *plug-in* realizza analisi di testo** (messaggi scambiati dai lavoratori) - ma sembra averla utilizzata in funzione sistematica e rafforzativa, confermando che gli *output* emotivi non devono raggiungere il datore di lavoro.

RICCARDO MARAGA/MARIA CHIARA GAROFALO

Provvedimento del 14 maggio 2026

2026/2(24)AGa
Il provvedimento sanzionatorio n. 419 del 28.5.2026 adottato dal Garante privacy italiano nei confronti di AgID per violazione del GDPR in relazione alla migrazione da INI-PEC a INAD

Con il provvedimento n. 419 del 28.5.2026 (doc. web n. 10259701), il Garante per la protezione dei dati personali (il **Garante**) ha dichiarato illecito il trattamento effettuato dall'Agenzia per l'Italia digitale (**AgID**) nell'ambito

ISSN 2239-8570

dei trattamenti degli indirizzi PEC (di posta elettronica certificata) in occasione della creazione e della gestione dell'Indice nazionale dei domicili digitali (**INAD**), così applicando una sanzione amministrativa pecuniaria di 55.000 euro, in ragione della violazione degli obblighi previsti dal reg. (UE) 2016/679 (**GDPR**).

La decisione riguarda il trasferimento nell'INAD degli indirizzi di posta elettronica certificata dei professionisti iscritti nell'INI-PEC. I due indici rispondono a funzioni collegate, ma non coincidenti. L'INI-PEC contiene gli indirizzi PEC comunicati da imprese e professionisti per l'esercizio dell'attività professionale, mentre l'INAD è il pubblico elenco dei **domicili digitali** delle persone fisiche, dei professionisti e degli altri enti non tenuti all'iscrizione nel registro delle imprese o in albi professionali. Il domicilio digitale iscritto nell'INAD può essere utilizzato anche per comunicazioni e notificazioni che riguardano la persona nella sua sfera privata.

L'**art. 6-quater(2)**, del d.lgs. 82/2005 (**codice dell'amministrazione digitale** o **CAD**) prevede che, per i professionisti iscritti in albi ed elenchi, il domicilio digitale corrisponda inizialmente all'indirizzo già presente nell'INI-PEC. La norma riconosce tuttavia al professionista il diritto di eleggere un indirizzo diverso. In attuazione di tale disciplina, **dal giugno 2023, AgID ha proceduto all'acquisizione automatica degli indirizzi dei professionisti dall'INI-PEC e, dal successivo mese di luglio, li ha pubblicati nell'INAD, diventando consultabili da chiunque senza autenticazione**.

Proprio perché l'indirizzo PEC professionale era destinato, ai sensi del già citato art. 6-quater(2) CAD, a essere utilizzato anche come domicilio digitale personale, le Linee guida adottate dalla stessa AgID riguardanti le regole tecniche e organizzative per la gestione dell'INAD, avevano previsto una specifica garanzia. **L'indirizzo trasferito dall'INI-PEC avrebbe dovuto essere inserito nell'INAD in via provvisoria e non essere pubblicato per trenta giorni. Durante tale periodo il professionista avrebbe dovuto ricevere l'informativa sul trattamento e le istruzioni necessarie per modificare l'indirizzo o impedirne la pubblicazione**. La misura recepiva una condizione formulata dal Garante nel **parere del 22 luglio 2021**, diretto a ridurre i rischi derivanti dall'automatica trasformazione di un recapito professionale in un domicilio utilizzabile anche per comunicazioni personali. L'istruttoria, avviata anche in seguito a reclami e segnalazioni, ha accertato che tale procedura non era stata applicata in modo adeguato. **I professionisti non avevano ricevuto**, prima della pubblicazione, **alcuna informazione** in merito al loro trasferimento nell'INAD del proprio indirizzo PEC. La **comunicazione inviata da AgID nel giugno 2023 ad alcuni Ordini e Collegi professionali** non è stata ritenuta sufficiente dal Garante. Non comprendeva tutte le categorie presenti nell'INI-PEC, non imponeva ai destinatari una diffusione capillare presso gli iscritti e non consentiva ad AgID di verificare che l'informazione fosse effettivamente giunta agli interessati.

Il Garante ha rilevato come la carenza informativa assume rilievo anche sotto il profilo sostanziale. L'indirizzo PEC, raccolto e pubblicato nell'INI-PEC per esigenze connesse all'attività professionale, viene utilizzato nell'INAD

ISSN 2239-8570

anche per ricevere comunicazioni relative alla vita privata. Il professionista, non conoscendo il trasferimento, non era posto nella condizione di valutare se mantenere tale indirizzo o eleggerne uno diverso. Inoltre, **la casella professionale poteva essere accessibile a collaboratori di studio**, con il rischio che questi venissero a conoscenza di comunicazioni personali destinate esclusivamente all'interessato.

Su queste basi, il Garante ha ritenuto violati i principi di liceità, correttezza e trasparenza previsti dall'art. 5(1(a) GDPR, nonché del principio di limitazione della finalità, di cui alla lettera b) dello stesso articolo, in quanto il dato era stato originariamente raccolto per finalità professionali ed era poi divenuto utilizzabile anche come recapito personale, senza l'applicazione delle garanzie previste.

La condotta ha integrato anche la violazione degli articoli 12 e 14 del GDPR in relazione all'assenza di informativa quando i dati non sono raccolti direttamente presso l'interessato. AgID aveva invocato l'esenzione prevista dal paragrafo 5, sostenendo che una comunicazione individuale a circa due milioni di professionisti avrebbe richiesto uno sforzo sproporzionato e che il trasferimento era previsto dalla legge. Tuttavia, il Garante ha escluso l'applicabilità di tali eccezioni. La successiva diffusione di un comunicato tramite il Ministero e gli Ordini professionali dimostrava che erano disponibili modalità informative più efficaci. Inoltre, la garanzia prevista dalle Linee guida costituiva proprio la misura necessaria affinché il trasferimento imposto dalla legge fosse compatibile con la tutela degli interessati.

È stata infine accertata la violazione dell'articolo 25 GDPR, relativo alla *privacy by design* e *by default*, poiché il sistema avrebbe dovuto impedire la pubblicazione immediata degli indirizzi e consentire agli interessati di esercitare preventivamente le proprie scelte. La tardiva allegazione delle misure informative adottate, avvenuta solo dopo due anni di istruttoria, ha comportato anche la violazione del principio di accountability di cui all'articolo 5, paragrafo 2 del GDPR.

ANDREA GABRIELLI

Provvedimento del 28 maggio 2026

2026/2(25)CI
Il provvedimento sanzionatorio dell'AGCM di 2 milioni di euro a Deghi S.p.A. per pratica commerciale scorretta per promozioni e sconti a termine sollecitati con "contatori alla rovescia"

Con il provvedimento n. 31999 del 23 giugno 2026, l'Autorità garante della concorrenza e del mercato (**AGCM** o l'**Autorità**) ha irrogato alla società Deghi S.p.A. (**Deghi**) una sanzione di 2 milioni di euro per aver mostrato, per quasi due anni, nelle pagine dedicate ai prodotti del proprio sito internet, un "contatore alla rovescia" (o *countdown*) volto a pubblicizzare sconti a termine che, alla scadenza, venivano riproposti alle medesime condizioni economiche mediante il riavvio del contatore. Secondo l'Autorità, tale condotta integrava

ISSN 2239-8570

una pratica commerciale scorretta, in quanto idonea a rappresentare in modo ingannevole la durata degli sconti e la convenienza economica dei prezzi applicati.

La decisione giunge all'esito di un'istruttoria avviata nel 2025 a seguito di alcune segnalazioni dei consumatori. Deghi è una società italiana specializzata nell'*e-commerce* di prodotti per l'arredamento di interni, il bagno e il giardino, che svolge la propria attività principalmente attraverso il proprio sito internet www.deghi.it. Il procedimento concerne un'unica pratica commerciale, posta in essere almeno dall'inizio di gennaio 2024 fino alla fine di dicembre 2025, consistente nella prospettazione ingannevole di prezzi e sconti promozionali, in violazione degli articoli 20, 21, 22 e 23(1)(g) del d.lgs. 206/2005 (**codice del consumo** o **c.cons.**).

Il *countdown timer* costituisce uno dei più noti esempi di *dark pattern*, ossia tecniche di progettazione delle interfacce di siti web e applicazioni digitali che, attraverso la configurazione dell'ambiente di scelta, sono idonee a falsare il processo decisionale degli utenti-consumatori. In particolare, il *countdown* indica il tempo residuo per beneficiare di un'offerta e, prospettandone l'imminente scadenza, fa leva sulla pressione temporale e sul timore di perdere condizioni economiche apparentemente favorevoli per accelerare la decisione di acquisto.

Nel caso Deghi, tuttavia, il profilo di scorrettezza non derivava dall'impiego del conto alla rovescia in quanto tale, né dalla sua capacità di generare un senso di urgenza. Le promozioni limitate nel tempo costituiscono infatti una tecnica commerciale di per sé lecita, purché la scadenza indicata corrisponda all'effettiva cessazione delle condizioni promozionali. Nel caso di specie, invece, una volta decorso il termine, il medesimo prezzo continuava ad essere applicato e il *countdown* veniva nuovamente avviato. La scadenza prospettata risultava, pertanto, fittizia e idonea a indurre il consumatore ad anticipare la decisione di acquisto per non perdere lo sconto. Il *countdown* costituiva dunque parte integrante della rappresentazione ingannevole della durata e delle condizioni dell'offerta.

Particolare rilievo assumono, sotto il profilo probatorio, gli elementi acquisiti nel corso dell'istruttoria. Dalla documentazione interna emergeva che il ricorso al contatore era consapevolmente diretto a sollecitare l'acquisto, facendo leva sull'"impazienza" del consumatore. A ciò si aggiungevano le dichiarazioni rese dal Presidente del Consiglio di amministrazione della società, dalle quali risultava che il *countdown* veniva rinnovato fino all'esaurimento dei prodotti da smaltire.

Il provvedimento affronta inoltre la prospettazione dei prezzi promozionali. L'Autorità ha rilevato che, per diversi prodotti, lo sconto veniva calcolato rispetto al prezzo pieno, anziché rispetto al prezzo più basso applicato nei trenta giorni precedenti. Il reiterato rinnovo del *countdown* contribuiva così a rappresentare l'offerta come eccezionale e temporanea, sebbene il medesimo prezzo fosse già stato applicato nel periodo precedente.

Nel corso del procedimento, Deghi ha contestato la rilevanza e l'idoneità decettiva della condotta. La società ha sostenuto che le promozioni riguardassero soltanto una quota limitata dei prodotti e fossero impiegate

ISSN 2239-8570

principalmente per lo smaltimento di giacenze, articoli stagionali o prodotti acquistati a condizioni economicamente sfavorevoli.
Quanto alla reiterazione del *countdown*, Deghi ha qualificato la prosecuzione delle offerte non come l'avvio di nuove promozioni, bensì come una proroga della campagna originaria, resa necessaria dal mancato esaurimento delle scorte. Su tale presupposto, la società riteneva legittimo continuare a calcolare la riduzione rispetto al prezzo applicato prima dell'inizio della campagna, anziché rispetto al prezzo promozionale praticato nei trenta giorni precedenti.
Deghi ha inoltre escluso che il contatore fosse idoneo a esercitare una pressione significativa sui consumatori. A sostegno di tale tesi, ha rilevato che il *countdown* aveva normalmente una durata di trenta giorni, non era accompagnato da espressioni quali "ultima occasione" o "offerta irripetibile" e lasciava, pertanto, un intervallo temporale sufficiente per confrontare le offerte. La società ha altresì richiamato dati interni dai quali emergeva che soltanto una parte degli acquisti era stata conclusa negli ultimi cinque giorni della promozione, sostenendo, più in generale, la portata circoscritta della condotta e l'assenza di un concreto pregiudizio per i consumatori.
L'Autorità ha tuttavia respinto le argomentazioni formulate da Deghi. Quanto alla qualificazione della prosecuzione dell'offerta come mera "proroga", ha osservato che la società non aveva informato i consumatori che, alla scadenza del contatore, le medesime condizioni economiche sarebbero rimaste applicabili. La rappresentazione dell'offerta lasciava, al contrario, intendere che lo sconto sarebbe cessato al termine indicato. Dalle risultanze istruttorie emergeva inoltre che, una volta scadute, le promozioni venivano riattivate manualmente mediante l'inserimento di nuove date di inizio e di fine. Ai fini della valutazione della pratica rilevava, pertanto, il modo in cui l'offerta era presentata al consumatore, e non la qualificazione attribuita internamente dalla società alla sua prosecuzione.
L'AGCM ha altresì escluso che la durata di trenta giorni del *countdown* fosse sufficiente a escludere il carattere ingannevole della pratica. Il profilo rilevante non era infatti la durata della promozione considerata isolatamente, bensì la falsa rappresentazione della sua scadenza. Il consumatore era indotto a ritenere che l'offerta sarebbe cessata al termine indicato, mentre, una volta decorso tale termine, essa veniva riproposta alle medesime condizioni.
Neppure i dati relativi agli acquisti conclusi negli ultimi giorni della promozione sono stati ritenuti decisivi. L'Autorità ha osservato che tali dati non dimostravano che l'induzione all'acquisto si producesse soltanto in prossimità della scadenza e che, in ogni caso, ai fini dell'accertamento della scorrettezza non era necessario dimostrare che il *countdown* avesse concretamente determinato uno specifico numero di operazioni, essendo sufficiente la sua idoneità a incidere sulla decisione commerciale del consumatore.
L'Autorità ha infine respinto la tesi secondo cui, trattandosi di un'unica campagna promozionale prorogata nel tempo, lo sconto potesse continuare a essere calcolato rispetto al prezzo pieno antecedente al suo avvio. Poiché i consumatori non erano stati informati né della durata complessiva della campagna né delle successive proroghe, il prezzo di riferimento avrebbe dovuto coincidere con il prezzo più basso applicato nei trenta giorni

ISSN 2239-8570

precedenti, ai sensi dell'articolo 17-bis c. cons. Il prezzo barrato e la percentuale di riduzione calcolata rispetto al prezzo pieno erano, pertanto, idonei a rappresentare una convenienza economica superiore a quella effettiva.
Alla luce delle valutazioni svolte, l'Autorità ha ritenuto che la condotta integrasse un'unica pratica commerciale scorretta ai sensi degli articoli 20, 21, 22 e 23(1)(g) c. cons., vietandone la reiterazione. Ai fini della quantificazione della sanzione, l'AGCM ha tenuto conto delle condizioni economiche della società, della particolare gravità della violazione e della sua durata. In particolare, ha attribuito rilievo alla consapevolezza con cui Deghi aveva utilizzato il *countdown* per rendere maggiormente attrattive le promozioni e indurre i consumatori all'acquisto, nonché al carattere particolarmente insidioso di tale tecnica, basata sull'urgenza e sull'euristica della scarsità. L'Autorità ha inoltre considerato le ambiguità e le omissioni informative riscontrate nella presentazione dei prezzi, degli sconti e dell'effettiva convenienza economica dei prodotti. Sulla base di tali elementi, ha irrogato a Deghi una sanzione pecuniaria complessiva di 2 milioni di euro.

CECILIA ISOLA

Testo ufficiale

2026/2(26)AR
L'ordinanza della Cassazione n. 20945/2026 sul requisito della sottoscrizione a parte e con firma digitale ai sensi dell'art. 1341 c.c.

Con l'ordinanza n. 20945 del 20 giugno 2026, la Terza Sezione civile della Corte di Cassazione si è pronunciata sulla sottoscrizione delle clausole vessatorie nei contratti telematici conclusi tra professionisti.
In particolare, la controversia decisa dalla Suprema Corte trae origine da un contratto di fornitura di energia elettrica concluso mediante **procedura *touch point***, ossia mediante adesione all'offerta commerciale pubblicata sul sito web del fornitore con perfezionamento del consenso attraverso la **«spunta»** — con un *click* del *mouse* — di una serie di caselle (i *flag*) ciascuna corrispondente a una determinata condizione contrattuale.
Allegando che il fornitore avesse unilateralmente modificato le condizioni economiche del contratto, aumentando illegittimamente il costo del servizio reso, l'altra parte del negozio lo ha citato in giudizio dinanzi al Tribunale di Viterbo — quale foro del luogo in cui l'obbligazione era sorta e doveva essere eseguita ex art. 20 c.p.c. — chiedendo la condanna alla restituzione delle somme indebitamente percepite.
Costituito in giudizio, il fornitore ha tuttavia eccepito l'incompetenza territoriale del giudice adito, invocando la clausola delle condizioni generali che fissava la competenza esclusiva presso il foro di Roma.
A supporto di tale eccezione il fornitore ha rilevato che l'onere della doppia sottoscrizione richiesto dall'art. 1341, comma 2, c.c. fosse stato correttamente assolto mediante il **«*doppio flag*»**, ossia la duplice selezione della casella dedicata all'approvazione specifica della clausola di competenza

ISSN 2239-8570

convenzionale contenuta nel documento predisposto dalla medesima società convenuta.
Il Tribunale di Viterbo, pur reputando la clausola inefficace per difetto della specifica approvazione, ha nondimeno declinato la propria competenza in favore del Tribunale di Roma, individuando in quella città — sede del fornitore, creditore dell'obbligazione pecuniaria — il luogo di adempimento dell'obbligazione di pagamento e, dunque, il foro competente ai sensi dell'art. 20 c.p.c.
Avverso tale decisione il cliente ha proposto regolamento di competenza, devolvendo la questione alla Corte di Cassazione.
Nel giudizio di legittimità, il fornitore, con la memoria difensiva, ha riproposto la questione della validità della clausola sul foro convenzionale, per l'ipotesi in cui il regolamento fosse risultato fondato.
Investita della questione, dunque, **la Corte ha anzitutto premesso che nella specie non veniva in rilievo la disciplina consumeristica, stante la pacifica natura di professionisti di entrambe le parti e, dunque, il carattere *B2B* del contratto. Il problema, a giudizio del Collegio, si riduceva pertanto a stabilire se l'art. 1341, comma 2, c.c. trovasse applicazione anche ai negozi del commercio elettronico**: questione che la Corte — in adesione alla requisitoria del Procuratore Generale — ha ritenuto di dover risolvere alla luce della disposizione di cui al **primo comma dell'art. 13del d.lgs. 70/2003** (recante le norme di attuazione della direttiva sul commercio elettronico 2000/31/CE), rubricato *Inoltro dell'ordine*, a mente del quale **le norme sulla conclusione dei contratti si applicano anche nei casi in cui il destinatario di un bene o di un servizio della società dell'informazione inoltri il proprio ordine per via telematica**.
Sulla base di tale disposizione, la Corte ha concluso che **anche le clausole vessatorie contenute nei contratti stipulati per via telematica** — tra cui quella sul foro convenzionale — **richiedono, per essere efficaci, la doppia firma secondo i canoni dell'art. 1341, comma 2, c.c.**
Una volta chiarita la astratta applicabilità della disciplina delle condizioni generali di contratto al negozio in esame (concluso *on line*), la Corte si è occupata della idoneità del sistema predisposto dalla società convenuta (vale a dire la procedura *touch point*) a soddisfare il requisito della doppia sottoscrizione di cui all'art. 1341, comma 2, c.c., pronunciandosi in negativo.
Sul piano generale, il Collegio ha anzitutto chiarito che l'approvazione di simili clausole richiede la sottoscrizione mediante firma elettronica, reputando sufficiente quella c.d. leggera (di regola apposta mediante l'inserimento sulla piattaforma web di un codice OTP trasmesso via sms o *e-mail*) ogniqualvolta il contratto non sia soggetto a forma scritta *ad substantiam*.
La Corte ha però precisato come **in ogni caso non si possa prescindere dalla consapevolezza del consenso e dal carattere specifico dell'approvazione, secondo quanto l'elaborazione giurisprudenziale ha da tempo coniato riguardo alle modalità tradizionali di sottoscrizione delle clausole vessatorie, anche nei contratti non formali**.
Grava perciò sul prestatore del servizio l'onere di predisporre, nel percorso di conclusione del contratto *on line*, un apposito *form* riservato

ISSN 2239-8570

alla clausola vessatoria — o alle clausole vessatorie, se richiamate o raggruppate — ove il firmatario possa approvarle apponendo la propria firma elettronica.
Solo così la clausola può spiegare efficacia, non essendo a tal fine sufficiente la mera spunta della casella.
Applicando tale regola alla vicenda in esame, la Corte ha escluso che la procedura *touch point* predisposta dal fornitore potesse dirsi compatibile con il precetto di cui all'art. 1341(2) c.c., data la mancanza di autonoma e specifica sottoscrizione, nelle forme sopra indicate, della clausola vessatoria.
A giudizio della Corte, dunque, occorre tenere distinta la spunta della casella dalla sottoscrizione elettronica. La prima attesta soltanto che l'utente ha compiuto un'azione nel percorso di adesione; la seconda imputa al firmatario una manifestazione di volontà riferita a quella determinata clausola. Solo la seconda integra l'approvazione per iscritto richiesta dall'art. 1341, comma 2, c.c.
In definitiva, la Corte ha dichiarato la competenza per territorio del Tribunale di Viterbo, fissando il termine di tre mesi dalla comunicazione dell'ordinanza per la riassunzione e enunciando il seguente principio di diritto:
"*in tema di contratti conclusi telematicamente tra professionisti ed aventi ad oggetto beni o servizi della società dell'informazione, poiché l'art. 13, comma 1, del D.Lgs. n. 70 del 2003 stabilisce che si applicano le ordinarie regole sulla conclusione dei contratti, la clausola vessatoria deve essere specificamente approvata per iscritto dall'acquirente, ai sensi dell'art. 1341, comma secondo, c.c., mediante firma digitale — che nel caso di contratti non soggetti a forma ad substantiam ex art. 1350 c.c. può assumere la veste della firma elettronica (o c.d. digitale leggera), di cui all'art. 3, punto 10, del Regolamento UE n. 910 del 2014 (c.d. eIDAS) —, non essendo di per sé sufficiente la mera "spunta" (o "flaggatura") della casella corrispondente alla clausola stessa*".

ALFREDO ROCCHI

Testo ufficiale

ISSN 2239-8570