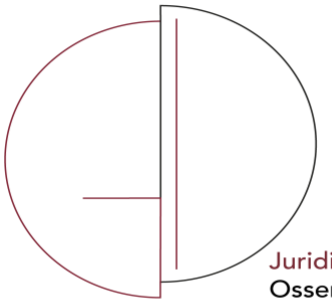

Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

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

9. **2024/2(9)FBe** Approvata la direttiva (UE) 2024/1799 sul diritto alla riparazione "R2R" – **Francesca Bertelli**
10. **2024/2(10)ES** – Entrato in vigore il regolamento (UE, Euratom) 2023/2841 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione – **Emanuele Stabile**
11. **2024/2(11)RA** Le ultime designazioni di VLOPs da parte della Commissione europea (per un totale di 24): Shein e Temu – **Riccardo Alfonsi**
12. **2024/2(12)RA** La risoluzione del Parlamento europeo del 12.12.2023 sulla progettazione dei servizi online che creano dipendenza e sulla tutela dei consumatori – **Riccardo Alfonsi**
13. **2024/2(13)AN** Il report della task force dell'EDPB su ChatGPT del 23.5.2024 – **Arianna Neri**
14. **2024/2(14)BG** I Primi Orientamenti dell'EDPS del 3.6.2024 su IA generativa e dati personali per le istituzioni, gli organi, gli uffici e le agenzie dell'Unione europea – **Beatrice Gallucci**
15. **2024/2(15)VR** Il parere dell'EDPB n. 11/2024 del 24.5.2024 sull'uso delle tecnologie di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree per snellire il flusso dei passeggeri negli aeroporti – **Valentino Ravagnani**
16. **2024/2(16)FDA** La sentenza della CGUE del 14.3.2024 nella causa C-46/23 sul principio per cui le autorità di controllo degli Stati membri possono ordinare di cancellare anche d'ufficio i dati personali raccolti da qualunque amministrazione nazionale in violazione del GDPR – **Filippo D'Angelo**
17. **2024/2(17)GR** La sentenza della CGUE del 30.4.2024 nella causa C-470/21 su lotta alla contraffazione e tutela dei dati personali ai sensi della direttiva e-privacy – **Giorgio Remotti**
18. **2024/2(18)DPDM** La sanzione di oltre 1,8 miliardi di euro irrogata il 04.03.2024 dalla Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in *streaming* su App Store – **Domenico Piers De Martino**
19. **2024/2(19)EMI** La comunicazione della Commissione ad Apple del 24.6.2024 di conclusioni preliminari sulla violazione del DMA ad opera delle regole dell'Apple Store e l'apertura di una nuova indagine per violazione del DMA ad opera dei nuovi obblighi posti da Apple a carico di terzi sviluppatori di app e app stores tra cui la nuova "Core Technology Fee" – **Enzo Maria Incutti**
20. **2024/2(20)RA** La Commissione europea apre una indagine su Meta per la violazione delle norme del DSA in relazione a fenomeni di 'dipendenza social' dei minori sulle piattaforme Facebook e Instagram – **Riccardo Alfonsi**
21. **2024/2(21)RG** Entrata in vigore la legge sul c.d. oblio oncologico (legge 7 dicembre 2023, n. 193) – **Raffaella Grisafi**
22. **2024/2(22)CAT** La modifica dell'art. 110 Codice privacy sul trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico,

ISSN 2239-8570

biomedico o epidemiologico (DL 19/2024) e il provvedimento n. 298 del 9 maggio 2024 del Garante privacy sulle regole deontologiche – **Carmine Andrea Trovato**

23. **2024/2(23)MS** Promulgata la legge 28 giugno 2024, n. 90 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici* – **Marco Scaldaferri**
24. **2024/2(24)MVT** La designazione di AGCOM quale Coordinatore dei servizi digitali ai sensi del DSA (DL 123/2023) – **Maria Vittoria Trinchera**
25. **2024/2(25)FB** La sentenza n. 69/2024 della Corte Costituzionale sulla illegittimità costituzionale per contrasto con le disposizioni sul riparto della potestà legislativa tra Stato e Regioni di una disposizione di una legge regionale in materia di sistemi di videosorveglianza in strutture di cura – **Filiberto Brozzetti**
26. **2024/2(26)ES** Approvato in via preliminare il decreto legislativo di adeguamento al MiCAR (regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività) – **Emanuele Stabile**
27. **2024/2(27)FG** Pubblicato il 15.5.2024 il regolamento AGCOM sull'equo compenso di autori, artisti, interpreti ed esecutori e sulla gestione dei diritti connessi da parte degli OGC e delle EGI– **Francesco Grossi**
28. **2024/2(28)EB** Il nuovo regolamento AGCOM del 5.12.2023 emanato in seguito all'adozione del Codice delle comunicazioni elettroniche, recante disposizioni a tutela degli utenti finali in materia di contratti relativi alla fornitura di servizi di comunicazioni elettroniche – **Emanuela Burgio**
29. **2024/2(29)VP** Le Linee-guida dell'AGCOM del 10.1.2024 sul rispetto del TUSMA da parte degli influencer e l'istituzione di un apposito Tavolo tecnico – **Vincenzo Pittelli**
30. **2024/2(30)EG** Il nuovo documento di indirizzo del Garante privacy italiano del 6.6.2024 sulla gestione della posta elettronica dei lavoratori e sul trattamento dei metadati – **Elisa Grossi**
31. **2024/2(31)SB** La Nota informativa del Garante privacy italiano del 20.5.2024 sul web scraping – **Stefano Bartoli**
32. **2024/2(32)SB** Web scraping e analisi del rischio fiscale: il Parere del Garante privacy italiano dell'11.1.2024 sullo schema del decreto sul concordato fiscale – **Stefano Bartoli**
33. **2024/2(33)GD** Il provvedimento AGCM contro Meta del 21.5.2024 per pratiche commerciali ingannevoli relative ad informazioni fornite ed omesse agli utenti dei servizi Instagram e Facebook (PS12566) – **Giorgia Diotallevi**
34. **2024/2(34)VR** L'ordinanza della Cassazione 12967 del 13.5.2024 sul caso del sistema software di supervisione degli studenti 'Respondus' impiegato dall'Università Bocconi di Milano per le prove scritte di esame – **Valentino Ravagnani**
35. **2024/2(35)EG** Il provvedimento del Garante privacy italiano del 9.5.2024 nei confronti di Wikipedia a proposito del diritto all'oblio – **Elisa Grossi**

ISSN 2239-8570

36. **2024/2(36)VR** Il Garante privacy italiano apre un'istruttoria per il progetto di videosorveglianza con riconoscimento facciale nelle stazioni metro di Roma – **Valentino Ravagnani**
37. **2024/2(37)DI** Il rapporto dell'aprile 2024 del Comitato di esperti nominato dal Presidente della Repubblica francese per studiare gli effetti dell'esposizione dei minori agli schermi: «*À la recherche du temps perdu*» – **Daniele Imbruglia**
38. **2024/2(38)AAM** La legge del 17.4.2024 dello Stato del Colorado sul trattamento dei dati neurali nel contesto dei dispostivi neurotecnologici destinati al mercato dei prodotti di consumo (*Colorado House Bill 24-1058*) e la conseguente modifica del Colorado Privacy Act – **Anna Anita Mollo**
39. **2024/2(39)SM** Il divieto di vendita di prodotti software Kaspersky da parte del Dipartimento del Commercio degli USA **–** **Serena Mirabello**
40. **2024/2(40)ST** L'India e le *Linee guida per la prevenzione e la regolamentazione dei dark patterns* in vigore dal dicembre 2023 **–** **Sara Tommasi**

Una raccolta indicizzata dei numeri della rubrica degli anni 2020-2022 è disponibile su: http://www.personaemercato.it/atlante-storico-del-diritto-dei-dati-anni-2020-2022/

ISSN 2239-8570

2024/2(1)RR

1. Adottato dal Consiglio d'Europa il primo trattato internazionale legalmente vincolante sull'intelligenza artificiale: la Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto del 17.5.2024

Il 17 maggio 2024 il Consiglio d'Europa ha adottato la Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto, il primo trattato internazionale giuridicamente vincolante volto a garantire il rispetto dei diritti umani e dei principi dello Stato di diritto nell'utilizzo dei sistemi di intelligenza artificiale. Il trattato sarà aperto alla firma il 5 settembre del 2024 a Vilnius, in Lituania, ed entrerà in vigore, ai sensi dell'art. 30, il primo giorno del mese successivo al decorso di un periodo di tre mesi dopo che cinque Stati firmatari, di cui almeno 3 Stati membri del Consiglio d'Europa, avranno espresso il loro consenso ad essere vincolati dalla Convenzione. Il testo definitivo della Convenzione costituisce l'esito del lavoro durato più di due anni svolto da un apposito organismo intergovernativo, il Comitato sull'intelligenza artificiale (CAI, *Committe on Artificial Intelligence*), il quale ha riunito i 46 Stati membri del Consiglio d'Europa, l'Unione europea e 11 Stati non membri (Argentina, Australia, Canada, Costa Rica, Giappone, Israele, Messico, Perù, Santa Sede, Stati Uniti d'America, e Uruguay), coinvolgendo inoltre rappresentanti della società civile e del mondo accademico, i quali hanno partecipato in qualità di osservatori. La partecipazione di Stati non membri del Consiglio d'Europa alla Convenzione quadro, e la connessa possibilità che in futuro divengano parti della medesima anche altri Stati non membri che non hanno partecipato ai lavori preparatori (v. art. 31), rende il trattato particolarmente rilevante nella prospettiva di fungere da paradigma normativo globale per la protezione dei diritti umani nell'ambito delle attività che interessano l'intero ciclo di vita dei sistemi di intelligenza artificiale.

Infatti, a differenza dell'altro unico strumento normativo sovranazionale a carattere vincolante (il regolamento dell'Unione europea, c.d. AI Act, o "AIA", ossia il Regolamento (UE) 2024/1689 il cui testo definitivo è stato adottato in data 13 giugno 2024, su cui v. notizia successiva in questo numero di questa Rubrica), la Convenzione quadro si concentra esclusivamente sugli aspetti di tutela dei diritti umani coinvolti dall'utilizzo dei sistemi di IA, e non anche su quelli economici e commerciali. Lo scopo avuto di mira dai redattori del testo è stato quello di creare un quadro normativo utile ad estendere a tutte le fasi del ciclo di vita dei sistemi di IA

ISSN 2239-8570

– quali la progettazione, lo sviluppo, la convalida, l'implementazione, il monitoraggio – gli standard e le obbligazioni già vigenti in materia di diritti umani, sia quando i sistemi siano adottati da soggetti ed enti pubblici sia quando i medesimi siano sfruttati da operatori privati. Tale ambito applicativo disvela la vocazione generale della Convenzione, di qui il nome «Convenzione quadro», destinata a trovare applicazione con riguardo a tutte le fasi del ciclo di vita che può interessare un sistema di IA; non è preclusa pertanto, come chiarito nel preambolo, l'adozione di ulteriori strumenti normativi funzionali a regolare specifici aspetti delle attività dei sistemi di intelligenza artificiale.

La Convenzione è composta da 36 articoli, divisi in 8 capitoli. Il capitolo 1, rubricato «Disposizioni generali», si occupa di definire l'ambito applicativo della Convenzione e di individuare la nozione dei sistemi di intelligenza artificiale. Sotto il primo profilo viene chiarito come non siano create nuove obbligazioni per gli Stati parti rispetto a quelle derivanti da trattati già in vigore, piuttosto i paesi firmatari sono tenuti ad estendere gli obblighi preesistenti in tema di protezione dei diritti umani a tutte le fasi in cui si articola il ciclo di vita di un sistema di IA, attraverso un approccio differenziato basato sul tipo di rischio e sulla più o meno elevata probabilità del verificarsi di un determinato pregiudizio per i principi dello Stato di diritto. In relazione alla definizione dei sistemi di IA, i redattori della Convenzione hanno aderito alla medesima nozione fornita dalle raccomandazioni OCSE – nella versione aggiornata del novembre 2023 – e dall'art. 3 AIA, disponendo all'art. 2 che i medesimi vanno intesi come «sistemi automatizzati che per obiettivi espliciti o impliciti, deducono dall'input che ricevono come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. I sistemi di IA variano in base al livello di autonomia o adattabilità dopo la propria diffusione». In tal modo è stata incoraggiata un'impostazione coerente con gli altri strumenti normativi internazionali al fine di creare una condivisione utile alla creazione di un quadro normativo uniforme, obiettivo centrale nella regolazione dei rapporti digitali e dell'intelligenza artificiale in particolare, i quali si presentano fisiologicamente privi di frontiere nazionali.

Il capitolo 2 si preoccupa di definire le obbligazioni principali gravanti sugli Stati parti, rappresentate dalla tutela dei diritti umani e dal rispetto dell'integrità dei processi democratici e dei principî dello Stato di diritto. Invero sono diverse le posizioni giuridiche fondamentali che sono considerate suscettibili di essere pregiudicate in ragione dell'utilizzo incontrollato della tecnologia in esame: l'intelligenza artificiale può, ad esempio, contribuire alla diffusione di informazioni false che possono manipolare l'opinione pubblica e minare la fiducia della collettività nella correttezza dei processi democratici; lo sfruttamento di algoritmi opachi e inficiati da *input* discriminatori può condizionare il funzionamento del sistema giudiziario e compromettere il diritto ad una tutela giurisdizionale effettiva; la sorveglianza di massa resa possibile dall'utilizzo di strumenti di riconoscimento che si basano sulla raccolta dei dati biometrici reca il rischio di pregiudicare il godimento di alcune libertà fondamentali, tra cui la libertà

ISSN 2239-8570

di assemblea o di espressione. Al fine di arginare i rischi menzionati, l'art. 5 impone il rispetto delle misure necessarie per garantire l'integrità delle istituzioni democratiche, salvaguardando, ad esempio, il principio della separazione dei poteri, dell'indipendenza del potere giudiziario e il diritto di accesso alla tutela giurisdizionale.

Il capitolo 3 è dedicato ai principî che devono informare lo svolgimento delle attività nell'ambito del ciclo di vita dei sistemi di IA, formulati in modo sufficientemente elastico da poter essere applicati in modo flessibile in diversi contesti e circostanze ed adattarsi agli sviluppi futuri della tecnologia. Tali principî sono identificati nella tutela della dignità umana e dell'autonomia individuale (art. 7); nell'obbligo di trasparenza e controllo (art. 8) – particolarmente rilevanti al fine di fronteggiare la fisiologica «opacità» ed autonomia degli strumenti algoritmici; nel principio di responsabilità dei soggetti che detengono il controllo delle varie fasi del ciclo di vita dei sistemi di IA (art. 9); nei principî di eguaglianza e non discriminazione utili a scongiurare probabili distorsioni riconducibili ai c.dd. «*bias* cognitivi» (art. 10); nella protezione dei dati personali (art. 11); nell'affidabilità dei sistemi (art. 12) e nell'innovazione sicura (art. 13).

In forza degli obblighi scolpiti nel capitolo 4, gli Stati firmatari sono tenuti ad adottare misure volte a garantire la disponibilità di rimedi effettivi e accessibili a fronte della violazione dei diritti umani, attraverso strumenti che siano in grado di superare le difficoltà connesse all'asimmetria informativa sussistente tra i soggetti lesi e coloro che sviluppano o utilizzano sistemi di IA. Viene così dedicato un rilievo centrale anche alla fase patologica susseguente alla compromissione dei diritti delle persone, nella prospettiva di assicurare l'azionabilità di rimedi efficaci. A tal riguardo, la Convenzione subordina tale obbligo, e la connessa possibilità per le persone danneggiate di agire in giudizio, alla circostanza che vi sia stata o vi sia il rischio di una violazione significativa dei diritti dei soggetti coinvolti, introducendo un limite all'azionabilità dei rimedi la cui precisa definizione viene attribuita alla discrezionalità degli Stati firmatari.

Tra le disposizioni più rilevanti, nell'ottica della prevenzione dei rischi che possono scaturire dall'impiego dei sistemi di IA, figurano quelle contenute nel capitolo 5, le quali impongono di adottare misure volte all'identificazione, alla valutazione e alla mitigazione dei rischi. Il monitoraggio degli effetti avversi nei confronti dei diritti umani va compiuto attraverso un'attività di documentazione che ne garantisca la comprensione e la verifica da parte di soggetti indipendenti deputati al controllo dell'osservanza delle obbligazioni sancite dalla Convenzione. Là dove le interferenze risultino inaccettabili e tali da non tollerare alcuna deroga, gli Stati parti hanno la possibilità di valutare l'introduzione di appositi divieti.

Ai fini di un'applicazione efficace della Convenzione, il capitolo 6 si preoccupa di introdurre obblighi di alfabetizzazione digitale, prevedendo che gli Stati firmatari sono tenuti a promuovere le conoscenze e le competenze necessarie al fine di consentire l'utilizzo e lo sfruttamento consapevole degli strumenti digitali e dei sistemi di IA in particolare. Tali competenze risultano strumentali a creare una consapevolezza diffusa nella

ISSN 2239-8570

collettività da un lato e a contribuire ad un più efficace svolgimento delle attività funzionali alla prevenzione e mitigazione dei rischi dall'altro. Sono inoltre chiariti i rapporti con le altre convenzioni internazionali concernenti la tutela dei diritti umani, tra cui in primo luogo la Convenzione europea dei diritti dell'uomo, disponendo come il nuovo strumento normativo non introduca nuovi obblighi e non deroghi a quelli già ricavabili dai trattati precedenti: la Convenzione quadro risulta funzionale ad estendere le obbligazioni preesistenti al settore del ciclo di vita dei sistemi di intelligenza artificiale.

Gli strumenti di controllo risultano disciplinati nel capitolo 7, ai sensi del quale è istituita la Conferenza delle parti, i cui compiti principali consistono nel monitorare il rispetto degli obblighi scolpiti dalla Convenzione, nel proporre eventuali modifiche necessarie per fronteggiare lo sviluppo tecnologico, nell'esprimere pareri in merito alla corretta interpretazione delle disposizioni della Convenzione e nel favorire la soluzione delle controversie in maniera amichevole. Per consentire alla Conferenza di svolgere le proprie attribuzioni, gli Stati parti sono tenuti a presentare a tale organo una relazione in merito alle iniziative adottate per eseguire gli obblighi della Convenzione, entro il termine di due anni dalla propria adesione.

Le disposizioni finali sono contenute nel capitolo 8, dedicato alla soluzione delle controversie, all'entrata in vigore della Convenzione, all'accesso di nuovi Stati – diversi da quelli membri del Consiglio d'Europa e da quelli che hanno partecipato ai lavori preparatori in seno al CAI – e all'applicazione territoriale.

Entro la fine del 2024, entrerà così in vigore il primo trattato internazionale a vocazione globale volto a sancire il rilievo primario della tutela dei diritti umani nel contesto dell'utilizzo dei sistemi di IA, contribuendo a creare una cultura diffusa a livello internazionale in merito alla gerarchia dei valori che devono presidiare lo sfruttamento di tale tecnologia.

ROBERTO RUOPPO

https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence

2024/2(2)SO

2. Approvato l'AI Act: regolamento (UE) 2024/1689 del 13.6.2024 che stabilisce regole armonizzate sull'intelligenza artificiale

Il 12.7.2024 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione europea il regolamento (UE) 2024/1689 del Parlamento e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive

ISSN 2239-8570

2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (di seguito **AI Act** o **AIA** o il **Regolamento**).

L'iter che ha portato all'approvazione dell'AI Act è durato poco più di tre anni. Dopo la pubblicazione della proposta della Commissione europea del 21.4.2021 (rispettivamente la **Proposta** e la **Commissione**) (su cui v. in questa Rubrica notizia n. 1 nel numero 2/2021: 2021/2(1)SO), il Consiglio dell'Unione europea (il **Consiglio**) ha approvato in data 21.5.2024 il testo della Posizione del Parlamento europeo (il **Parlamento** o il **PE**), votato dal PE il 13.3.2024 ed in seguito sottoposto ad una procedura prevista per le rettifiche dall'art. 241 del Regolamento del Parlamento europeo (con la pubblicazione del testo emendato datato 19.4.2024).

Prima di allora:

- nel 2021, la Proposta aveva formato oggetto di un parere congiunto di EDPB e EDPS datato 21.6.2021 (su cui v. in questa Rubrica v. la notizia n. 3 sul numero 3/2021: 2021/3(3)CR) e di un parere della BCE datato 29.12.2021 (su cui v. in questa Rubrica la notizia n. 8 sul numero 2/2022: 2022/2(8)ES);

- nel 2022, il Consiglio aveva approvato in data 6.12.2022 un testo di orientamento generale datato 25.11.2022 (Council General Approach December 22);

- nel 2023, il Parlamento, in sede di prima lettura nella procedura legislativa ordinaria, il 14.6.2023 aveva approvato 771 emendamenti alla Proposta (gli **Emendamenti del PE**) (su cui v. in questa Rubrica, la notizia n. 4 nel numero 2/2023: 2023/2(4)SO);

- sempre nel 2023, si erano dunque svolti i triloghi, con dichiarazione di avvenuto raggiungimento di un accordo tra i negoziatori nella notte tra l'8 e il 9 dicembre 2023 (su cui v. in questa Rubrica, la notizia n. 2 nel numero 4/2023: 2023/4(2)SO).

L'AI Act contiene un quadro di divieti, di obblighi e di requisiti relativi ai sistemi di IA, come ivi definiti, comprensivo di un apparato sanzionatorio e istituzionale. La sua base giuridica è individuata negli articoli 16 e 114 del Trattato sul funzionamento dell'Unione europea ("**TFUE**").

Il testo dell'AI Act presenta notevoli differenze non solo rispetto a quello della Proposta ma anche rispetto a quello degli Emendamenti del PE.

Nel **primo Considerando** dell'AIA, si afferma che lo scopo del Regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (**IA**) nell'Unione, in conformità dei valori dell'Unione. Si aggiunge che è scopo dell'AIA "promuovere la diffusione di un'intelligenza artificiale […] antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea […], compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione".

Il primo Considerando dell'AIA, si chiude con un divieto agli Stati membri, in particolare dove si legge che il Regolamento "garantisce la

ISSN 2239-8570

libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del [medesimo] regolamento".

L'AIA contiene tredici Capi. Rispetto al testo della Proposta, un nuovo Capo è dedicato ai "modelli di IA per finalità generali" (Capo V).

Il **Capo I (artt. 1-4 AIA)** è intitolato ***Disposizioni generali***. In esso sono contenute anche le definizioni.

La definizione di "**sistemi di IA**" (di seguito anche solo "**sistemi**") riprende quella accolta in ambito OCSE: «un sistema automatizzato [*a machine-based system*] progettato per operare con livelli di autonomia variabili, che può mostrare adattabilità dopo la diffusione [*after deployment*] e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

Rispetto ai termini e alle definizioni delle versioni precedenti, si segnala che nella versione inglese del testo finale del Regolamento la parola "*user*" è stata sostituita con "*deployer*", e che nella versione italiana tale parola non è stata tradotta in lingua italiana. La sua definizione è la seguente: «"**deployer**": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

Il "**fornitore**" è definito come «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito».

Il "**modello di IA per finalità generali**" è definito come «un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato [da] una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato».

L'art. 2 AIA stabilisce che il Regolamento si applica:

- ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo;
- ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione;
- ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo,

ISSN 2239-8570

laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione;
- agli importatori e ai distributori di sistemi di IA;
- ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio;
- ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione;
- alle persone interessate che si trovano nell'Unione.

Sempre l'art. 2 AIA specifica che il Regolamento non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, e che esso non si applica ai sistemi di IA sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale. Inoltre, è disposto che il Regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale.

Sempre nell'art. 2 AIA, è disposto che il Regolamento non si applica alle autorità pubbliche di un paese terzo né alle organizzazioni internazionali che rientrano nell'ambito di applicazione del Regolamento a norma del paragrafo 1, laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri, a condizione che tale paese terzo o organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone.

Il **Capo II (art. 5 AIA)** intitolato ***Pratiche di intelligenza artificiale vietate***, contiene un solo articolo che elenca una serie di sistemi di IA, individuati anche con riferimento a casi d'uso, sottoposti ai divieti di immissione sul mercato, messa in servizio e/o uso.

La "**immissione sul mercato**" è definita come: «la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione».

La "**messa in servizio**" è definita come: «la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista».

L'"**uso**" invece non è definito.

Nel testo finale del Regolamento, sono state soppresse le modifiche introdotte dagli Emendamenti del PE ai Considerando e all'art. 2 della Proposta, volte a vietare l'esportazione fuori dall'Unione europea di sistemi di IA la cui immissione sul mercato, la messa in servizio e/o l'uso sono vietati nella UE ai sensi del Regolamento.

Si tratta, in particolare dei:

- sistemi di IA che utilizzano «tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di

ISSN 2239-8570

prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo» (art 5(1)(a) AIA);

- sistemi di IA «che sfrutta[no] le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo» (art 5(1)(b) AIA);
- «sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:

i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;

ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità» (art 5(1)(c) AIA);

- sistemi di IA «per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»(art 5(1)(d) AIA);
- «sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso»(art 5(1)(e) AIA);
- «sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza»(art 5(1)(f) AIA);
- «sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti

ISSN 2239-8570

legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto»(art 5(1)(g) AIA);

- «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:

i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;

ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'**allegato II**, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni» (art 5(1)(h) AIA).

Per quest'ultima categoria di sistemi è vietato soltanto l'uso, mentre per tutti le altre categorie di sistemi è vietata sia l'immissione sul mercato che la messa in servizio che l'uso.

Il **Capo III (artt. 6-49 AIA)** è intitolato ***Sistemi di IA ad alto rischio*.** Le norme della Sezione 1 (artt. 6-7) definiscono le condizioni alle quali i sistemi di IA debbano qualificarsi ai sensi e per gli effetti dell'AIA come ad alto rischio. Alcune di queste norme sono state modificate più volte durante il processo legislativo.

L'art. 6(1) AIA prevede che siano sistemi ad alto rischio i sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti, o che sono essi stessi prodotti, soggetti a valutazione di conformità *ex ante* da parte di terzi, ai sensi della normativa di armonizzazione dell'Unione di cui all'**allegato I**.

L'allegato I contiene un elenco di 20 fonti di normativa di armonizzazione dell'Unione, divise in due sezioni, la "A" contenente fonti del c.d. "nuovo quadro legislativo", e la "B" contenenti altre normative di armonizzazione dell'Unione.

L'art. 6(2) AIA prevede che in aggiunta ai sistemi di cui all'art. 6(1) AIA, sono considerati ad alto rischio anche quelli elencati all'**allegato III**.

L'allegato III contiene un elenco di sistemi e casi d'uso divisi in 8 settori: 1) Biometria. Questo settore comprende i sistemi di riconoscimento delle emozioni; 2) Infrastrutture critiche; 3) Istruzione e formazione professionale; 4) Occupazione, gestione dei lavoratori e accesso al lavoro autonomo; 5) Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; 6) Attività di contrasto; 7) Migrazione, asilo e gestione del controllo delle frontiere; 8) Amministrazione della giustizia e processi democratici. Quest'ultimo settore comprende i sistemi di IA di marketing politico.

ISSN 2239-8570

Per i settori sub 1), 6) e 7) l'AIA specifica che i sistemi di IA ad alto rischio ivi descritti devono ritenersi inclusi nell'elenco "nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso". In virtù del disposto dell'art. 2(11) AIA, la stessa riserva deve ritenersi disposta dall'AIA anche con riguardo ai sistemi di IA ad alto rischio elencati nel settore 4) (Occupazione, gestione dei lavoratori e accesso al lavoro autonomo).

L'art. 6(3) AIA contiene le più importanti tra le nuove disposizioni. Il primo comma di questo paragrafo prevede che un sistema di IA di cui all'allegato III non può essere considerato ad alto rischio se non è capace di "***influenzare materialmente il risultato del processo decisionale***" o se non presenta altrimenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche. Il secondo comma di questo paragrafo detta un elenco di condizioni al verificarsi anche solo di una delle quali deve ritenersi che il sistema di IA non sia capace di influenzare materialmente il risultato del processo decisionale. Il terzo comma di questo paragrafo prevede infine che, nonostante quanto previsto dal primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui **profilazione** di persone fisiche.

L'art. 6(4) AIA prevede che, fermo restando l'obbligo di registrazione di cui all'art. 49(2) AIA, un fornitore che ritenga che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che il sistema sia immesso sul mercato oppure messo in servizio. Vengono infine dati poteri alla Commissione per compiere anche attraverso atti delegati modifiche al paragrafo 3 dell'art. 6 o modifiche ai casi d'uso previsti nell'allegato III e per fornire orientamenti ed esempi pratici al fine di distinguere tra sistemi ad alto rischio e non ad alto rischio.

La Sezione 2 del Capo III (artt. 7-15) è dedicata ai "requisiti" per i sistemi di IA ad alto rischio. Vi sono contenute le importanti disposizioni sul "sistema di gestione dei rischi" (art. 9), sulla governance dei dati (art. 10), sulla documentazione tecnica (art. 11), sulla registrazione dei dati (art. 12), sulla trasparenza (art. 13), sulla sorveglianza umana (art. 14), nonché sui requisiti di accuratezza, robustezza e cibersicurezza (art. 15).

È importante segnalare che le norme di questa Sezione sono quelle interessate dalla modifica delle prime 8 delle 9 normative che si leggono nell'intestazione dell'AI Act, laddove è previsto che il Regolamento modifica i regolamenti (CE) n. 300/2008 [in materia di aviazione civile], (UE) n. 167/2013 [in materia di veicoli agricoli e forestali], (UE) n. 168/2013 [in materia di veicoli a motore a due o tre ruote e quadricicli], (UE) 2018/858 [in materia di veicoli a motore], (UE) 2018/1139 [in materia di aviazione civile] e (UE) 2019/2144 [in materia di veicoli a motore] e le direttive 2014/90/UE [in materia di equipaggiamento marittimo], (UE) 2016/797 [in materia di interoperabilità del sistema ferroviario] e (UE) 2020/1828 [in materia di azioni rappresentative a tutela degli interessi collettivi dei consumatori]. Si tratta delle stesse 8 normative elencate nella Sezione "B" dell'allegato I del Regolamento (c.d. *Old Approach Legislation*), e richiamate dagli articoli da 102 a 109 AIA. Come si ricava

ISSN 2239-8570

dall'art. 2(2) AIA, ai sistemi di IA classificati ad alto rischio ai sensi dell'art. 6(1) AIA relativamente a prodotti disciplinati da queste 8 normative, l'AI Act non si applica direttamente, e, tuttavia, gli essenziali requisiti *ex-ante* per i sistemi di IA di alto rischio previsti esattamente nella Sezione 2 del Capo III AIA dovranno essere presi in considerazione quando si adotteranno normative attuative o delegate della medesima legislazione (artt. 102-109 AIA).

La Sezione 3 del Capo III (artt. 16-27), sempre con riferimento ai sistemi ad alto rischio, è dedicata non soltanto agli obblighi dei fornitori (art. 16) e dei deployers (art. 26), ma anche agli obblighi dei rappresentanti autorizzati dei fornitori (art. 22), degli importatori (art. 23) e dei distributori (art. 24) - in ciascun caso come definiti nell'art. 3 AIA - nonché al "sistema di gestione della qualità" (art. 17), alla conservazione dei documenti (art. 18), ai log generati automaticamente (art. 19), alle misure correttive e al dovere di informazione (art. 20) e alla cooperazione con le autorità (art. 21). Particolarmente importanti sono le norme dell'art. 25 sulla responsabilità "lungo la catena del valore dell'IA" e quelle dell'art. 27 sulla "valutazione d'impatto sui diritti fondamentali".

La Sezione 4 del Capo III (artt. 28-39) è dedicata, sempre relativamente ai sistemi ad alto rischio, alle "autorità di notifica" (che ciascun Stato membro deve designare o istituire ai sensi dell'AIA, responsabili delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e il relativo monitoraggio, salva la possibilità per gli Stati membri di decidere che la valutazione e il monitoraggio siano eseguiti da un organismo nazionale di accreditamento ex reg. (CE) n. 765/2008) e agli organismi notificati.

La Sezione 5 del Capo III (art. 40-49) è dedicata alla conformità alle norme (ossia agli *standards*) di cui al regolamento (UE) n. 1025/2012 sulla normazione europea (artt. 40-41), alla presunzione e alla valutazione della conformità (artt. 41-42), ai certificati, agli organismi notificati e alla marcatura CE (artt. 44-48) e alla registrazione (art. 49 e allegato VIII).

Il **Capo IV (art. 50 AIA),** intitolato ***Obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di IA***, riguarda i sistemi destinati ad interagire direttamente con le persone fisiche, i sistemi di IA per finalità generali che generano contenuti audio, immagine, video o testuali sintetici, i sistemi di riconoscimento delle emozioni e quelli di categorizzazione biometrica, come definiti all'art. 3 AIA, e i sistemi che generano o manipolano immagini o contenuti audio o video che costituiscono un "deep fake". Per tali sistemi sono previsti obblighi finalizzati a rendere le persone consapevoli della natura di output di sistemi di intelligenza artificiale relativamente a quelli cui le persone sono effettivamente esposte.

Il **Capo V (artt. 51-56 AIA)** è intitolato ***Modelli di IA per finalità generali***. La disciplina, che riguarda i modelli di cui alla definizione dell'art. 3 sopra richiamata, è ripartita in quattro Sezioni, la prima delle quali (artt. 51-52) contiene regole che fissano le condizioni per qualificare i modelli di IA per finalità che comportano un "rischio sistemico", la seconda (artt. 53-54) prevede gli obblighi dei fornitori di modelli di IA per finalità

ISSN 2239-8570

generali, la terza (art. 54) quelli dei fornitori di modelli di IA per finalità generali con rischio sistemico, e la quarta (art. 56) contiene alcune regole sui *"codici di buone pratiche"* relativamente ai modelli di IA per finalità generali.

Il **Capo VI (artt. 57-63 AIA)**, intitolato ***Misure a sostegno dell'innovazione***, contiene la disciplina degli spazi di sperimentazione normativa (*sandboxes*) (artt. 57-59) e delle prove dei sistemi ad alto rischio in condizioni reali al di fuori delle sandboxes (artt. 60-63).

Il **Capo VII (artt. 64-70 AIA)** è intitolato ***Governance***. L'**ufficio per l'IA** della Commissione (**AI Office**) sarà l'organo per l'implementazione dell'AI Act al livello dell'Unione (art. 64), e avrà inoltre – come disposto nei successivi Capi IX e XII - il compito di applicare le norme sui modelli IA per finalità generali (artt. 88, 101). Tre organi consultivi hanno compiti di supporto nell'implementazione delle norme. Il **comitato europeo per l'intelligenza artificiale** (*European Artificial Intelligence Board* **EAIB**), composto da un rappresentante per ogni Stato membro e dall'EDPS come osservatore, fornirà consulenza alla Commissione e agli Stati membri e dovrà assicurare l'applicazione uniforme dell'AI Act negli Stati membri, agendo come organo principale per la cooperazione tra la Commissione e gli Stati membri (artt. 65-66). Un **gruppo di esperti scientifici indipendenti** (*scientific panel*) selezionati dalla Commissione fornirà consulenza tecnica e sostegno all'ufficio per l'IA per l'applicazione dell'AIA. In particolare, potrà offrire consulenza e segnalare rischi relativi ai modelli di IA per finalità generali (artt. 68-69). L'ufficio per l'IA può ricevere indicazioni anche da un **forum consultivo** (*advisory forum*), composto da una selezione equilibrata di stakeholders (portatori di interessi) tra cui industria, start-up, PMI, società civile e mondo accademico (art. 67). Al livello della governance degli Stati membri, ciascuno di essi deve designare le sue autorità competenti per supervisionare l'applicazione delle norme del Regolamento ed esercitare l'attività di sorveglianza: almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. L'AI Act prescrive che tali autorità nazionali "esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi" (art. 70).

Il **Capo VIII (art. 71 AIA)** intitolato ***Banca dati dell'UE per i sistemi di IA ad alto rischio*** riguarda i sistemi ad alto rischio elencati nell'allegato III e registrati conformemente agli artt. 49 e 60 AIA, nonché i sistemi registrati ai sensi dell'art. 6(4) AIA. A cura del fornitore o del rappresentante autorizzato nella banca dati devono essere inseriti i dati elencati nell'**allegato VIII**, sezioni "A" e "B".

Invece se il deployer è un'autorità, un'agenzia o un organismo pubblico, deve inserire nella banca dati i dati elencati nell'allegato VIII, sezione "C". Salvo che per alcune informazioni, la banca dati è accessibile al pubblico. Essa è istituita e mantenuta dalla Commissione, che è anche titolare del trattamento.

Il **Capo IX (artt. 72-94 AIA)** è intitolato ***Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni e vigilanza del mercato.***

ISSN 2239-8570

La Sezione 1 del Capo IX (art. 72) riguarda il *Monitoraggio successivo all'immissione sul mercato* e fa obbligo ai fornitori di sistemi ad alto rischio di istituire e documentare un "sistema di monitoraggio successivo all'immissione sul mercato", che si basa su un "piano di monitoraggio successivo all'immissione sul mercato".

La Sezione 2 del Capo IX (art. 73) intitolata *Condivisione di informazioni su incidenti gravi* prevede e disciplina l'obbligo di comunicazione di incidenti gravi in capo ai fornitori.

La Sezione 3 del Capo IX (artt. 74-84) è intitolata *Applicazione*. È previsto che il regolamento (UE) 2019/1020 sulla vigilanza dei mercati e sulla conformità dei prodotti si applichi ai sistemi disciplinati dall'AI Act, e si prevedono gli adattamenti anche terminologici per tale applicazione (art. 74). Si prevedono norme che fissano i poteri dell'ufficio per l'IA e norme sull'assistenza reciproca tra autorità di vigilanza del mercato e ufficio per l'IA per i casi in cui un sistema di IA si basi su un modello di IA per finalità generali e questo e quello siano sviluppati dallo stesso fornitore (art. 75). Si stabiliscono le competenze e i poteri delle autorità di vigilanza del mercato per il controllo delle prove in condizioni reali (art. 76). Si prevede il potere di autorità ed organismi pubblici di accedere a documenti ed informazioni per la tutela dei diritti fondamentali (art. 77). Si disciplina l'obbligo di riservatezza (art. 78). Si richiama nuovamente il regolamento (UE) 2019/1020 sulla vigilanza dei mercati e sulla conformità dei prodotti a proposito della definizione di "prodotto che presenta un rischio" ivi contenuta, per ricomprendervi i sistemi di IA che presentano un rischio "nella misura in cui presenta[no] rischi per la salute o la sicurezza o per i diritti fondamentali" e si prevede la procedura a livello nazionale per i sistemi di IA che presentano un rischio con particolare attenzione ai sistemi di IA "che presentano rischi per gruppi vulnerabili", stabilendo che laddove non vengano adottate le misure correttive adeguate, l'autorità di vigilanza del mercato possa vietare o limitare la messa in servizio o la messa a disposizione o ritirare il prodotto o il sistema di IA autonomo dal mercato o richiamarlo (art. 79). Si prevede una procedura specifica per i sistemi che il fornitore abbia classificato come non ad alto rischio per il caso in cui l'autorità di vigilanza del mercato sia di diverso parere (art. 80). Si prevede una procedura di "salvaguardia dell'Unione" per i casi in cui l'autorità di vigilanza del mercato di uno Stato membro o la Commissione ritengano che le misure adottate da un'autorità di vigilanza del mercato di uno Stato membro siano contrarie al diritto dell'Unione (art. 81). Si prevede una procedura speciale per i casi in cui l'autorità di vigilanza del mercato di uno Stato membro ritenga che un sistema ad alto rischio pur risultando conforme al Regolamento, nondimeno "rappresenti comunque un rischio per la salute o la sicurezza delle persone, per i diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico" (art. 82). Ancora, si prevede una procedura specifica per far cessare una situazione di non conformità rispetto a requisiti formali elencati specificamente (art. 83). Infine, si prevede che la Commissione designi una o più "strutture di sostegno dell'Unione per la prova dell'IA" per lo svolgimento dei compiti di cui all'art. 21(6) del

ISSN 2239-8570

regolamento (UE) 2019/1020 sulla vigilanza dei mercati e sulla conformità dei prodotti, nel settore dell'IA (art. 84).

La Sezione 4 del Capo IX intitolata *Mezzi di ricorso*, contiene due articoli. Il primo prevede il diritto di qualunque persona fisica o giuridica di presentare un reclamo alla pertinente autorità di vigilanza del mercato laddove ritenga che vi sia stata una violazione del Regolamento (art. 85); il secondo prevede al primo paragrafo il "diritto alla spiegazione dei singoli processi decisionali" (art. 86(1) AIA), e al terzo paragrafo dispone che il medesimo articolo "si applica solo nella misura in cui il diritto di cui al paragrafo 1 non sia altrimenti previsto dal diritto dell'Unione" (art. 86(3) AIA).

La Sezione 5 del Capo IX (artt. 88- 94) riguarda la *Supervisione, indagini, esecuzione e monitoraggio in relazione ai fornitori di modelli di IA per finalità generali* e, inter alia, investe la Commissione di competenze esclusive sulla vigilanza e l'esecuzione del Capo V.

Il **Capo X (artt. 95-96 AIA),** intitolato ***Codici di condotta e orientamenti***, contiene innanzitutto le norme volte ad incoraggiare le imprese ad elaborare codici di condotta e meccanismi di governance intesi a promuovere l'applicazione su base volontarie delle norme di cui alla Sezione 2 del Capo III del Regolamento (ossia le norme sui requisiti ex ante dei sistemi ad alto rischio) per i sistemi di IA diversi dai sistemi ad alto rischio (art. 95). Nell'articolo successivo (art. 96) si prevede che la Commissione debba elaborare orientamenti su una pluralità di aspetti applicativi del Regolamento.

Il **Capo XI (artt. 97-98 AIA),** intitolato ***Delega di potere e procedura di comitato***, prevede le condizioni e i termini temporali alle quali è conferito alla Commissione il potere di adottare atti delegati ai sensi del Regolamento.

Il **Capo XII (artt. 99-101 AIA),** intitolato ***Sanzioni*** contiene tre articoli, il primo riguardante il regime delle sanzioni e delle altre misure di esecuzione che gli Stati membri devono applicare in caso di violazione dell'AI Act da parte di tutti i soggetti cui sono posti obblighi e divieti in relazione ai sistemi di IA ai sensi del Regolamento, comprese le sanzioni pecuniarie che possono essere inflitte a soggetti diversi da istituzioni, organi e organismi dell'Unione (art. 99). Il secondo articolo riguarda le sanzioni amministrative pecuniare che possono essere inflitte dal Garante europeo della protezione dei dati personali (EDPS) alle istituzioni, organi e organismi dell'Unione per la violazione del Regolamento (art. 100). Il terzo articolo riguarda le sanzioni pecuniarie che possono essere inflitte dalla Commissione ai fornitori di modelli di IA per finalità generali per violazioni del Regolamento (art. 101).

Il **Capo XIII (artt. 102-113 AIA)** è dedicato alle ***Disposizioni finali***. In aggiunta alle modifiche delle prime 8 delle 9 normative richiamate nel titolo dell'AI Act, di cui si è detto *supra*, apportate dagli artt. 102-109, l'art. 110 ha modificato la direttiva (UE) 2020/1828 relativa alle azioni rappresentative a tutela degli interessi dei consumatori attraverso l'aggiunta al suo allegato I della menzione del Regolamento. Di conseguenza, la

ISSN 2239-8570

violazione dell'AI Act integra violazione del diritto dell'Unione ai sensi e per gli effetti dell'art. 2(1) della direttiva (UE) 2020/1828.

L'art. 111 detta la disciplina dei sistemi e dei modelli per finalità generali già immessi sul mercato, e distingue cinque ipotesi, senza pregiudizio in ogni caso per l'applicazione dell'art. 5 AIA secondo il suo termine di applicazione: **(1)** sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'**allegato X**, e che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2027: essi devono essere resi conformi all'AI Act entro il 31 dicembre 2030; **(2)** i sistemi di IA, diversi da quelli sub (1) che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2026: non devono essere resi conformi; **(3)** i sistemi di IA, diversi da quelli sub (1) che sono stati immessi sul mercato o messi in servizio prima del 2 agosto 2026 che a decorrere da tale data sono soggetti a modifiche significative della loro progettazione: devono essere resi conformi; **(4)** in ogni caso, i fornitori e deployers di sistemi di IA ad alto rischio destinati a essere utilizzati dalle autorità pubbliche adottano le misure necessarie per conformarsi ai requisiti e agli obblighi del presente regolamento entro il 2 agosto 2030; **(5)** I fornitori di modelli di IA per finalità generali che sono stati immessi sul mercato prima del 2 agosto 2025 adottano le misure necessarie per conformarsi agli obblighi di cui al presente regolamento entro 2 agosto 2027.

L'art. 112 attribuisce alla Commissione determinati poteri e compiti per la valutazione e l'esame dell'allegato III e dell'elenco delle c.d. pratiche vietate di cui all'art. 5

L'art. 113 disciplina l'entrata in vigore e l'applicazione. AI Act è entrato in vigore il 1 agosto 2024. La maggior parte delle norme dell'AI act comincerà ad applicarsi il **2 agosto 2026**.

Prima di allora, tuttavia, le norme del Capo I (*Disposizioni generali*) e del Capo II (*Pratiche di intelligenza artificiale vietate*) si applicheranno a decorrere dal 2 febbraio 2025, e quelle del Capo V (*Modelli di IA per finalità generali*) si applicheranno a decorrere dal 2 agosto 2025, così come altre norme particolari: quelle del Capo III, sezione 4 (*Autorità di notifica ed organismi notificati*), quelle del Capo VII (*Governance*) (gli Stati membri, pertanto hanno termine fino al 2 agosto 2025 per designare le loro autorità competenti per supervisionare l'applicazione delle norme del Regolamento ed esercitare l'attività di sorveglianza), quelle del capo XII (*Sanzioni*) eccezion fatta per l'art. 101, e quelle dell'articolo 78 (*Riservatezza*).

Dopo di allora, le norme dell'art. 6(1) e i corrispondenti obblighi di cui al Regolamento si applicano a decorrere dal 2 agosto 2027, con la conseguenza che nemmeno i sistemi di IA relativi ai prodotti disciplinati dalla normativa di armonizzazione dell'Unione in base al nuovo quadro legislativo di cui alla Sezione "A" dell'allegato I dell'AI Act potranno prima di quella data essere trattati come sistemi di IA ad alto rischio, pur ricorrendone i presupposti ex art. 6(1) AIA.

Co riferimento al periodo di transizione precedente alla piena applicazione del Regolamento, la Commissione ha lanciato l'iniziativa "AI Pact", con la quale si invitano invita gli sviluppatori di IA ad osservare le regole dell'AI Act prima dei suddetti termini.

ISSN 2239-8570

Infine, la Commissione sta anche sviluppando delle linee guida per facilitare strumenti di co-regolazione come le norme tecniche (*standards*) e i codici di buone pratiche (*codes of practice*), e, in proposito ha lanciato un invito a partecipare alla stesura del primo codice di buone pratiche per i modelli di IA per finalità generali (art. 56 AIA) e una consultazione multi-stakeholder.

SALVATORE ORLANDO

AI Act

2024/2(3)SO

3. Il Colorado AI Act del 17.5.2024

Il 17 maggio 2024, dopo un processo legislativo velocissimo, durato poco più di un mese – la relativa proposta essendo stata introdotta il 10 aprile 2024 – il Governatore dello Stato del Colorado (USA), ha promulgato il Senate Bill 24-205 *Concerning Consumer Protections in Interactions with Artificial Intelligence Systems*, c.d. Colorado AI Act (di seguito **CAIA**).

Numerose sono le similitudini e i punti di contatto del CAIA con l'AI Act approvato con il regolamento (UE) 2024/1689 del 13 giugno 2024 (di seguito **EUAIA**) (su cui v. *supra*, in questa Rubrica, notizia n. 2 di questo numero [2024/2(2)SO]).

La definizione di «sistema di intelligenza artificiale» del CAIA è in linea con quella dell'OCSE che troviamo sia nella Convenzione del Consiglio d'Europa del 17.5.2024 (su cui v. in questa Rubrica, notizia n. 1 in questo numero [2024/2(1)RR]) che nell'EUAIA: "*any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments*".

La definizione di «sistemi di intelligenza artificiale ad alto rischio» (di seguito solo **sistemi ad alto rischio**) del CAIA è la seguente: "*any artificial intelligence system that, when deployed, makes, or is a substantial factor in making, a consequential decision*".

In tale definizione, come ben si vede, è centrale la nozione di «decisione consequenziale» (*consequential decision*).

La «decisione consequenziale» è dunque a sua volta definita nel CAIA, e, come può notarsi, è coessenziale alla nozione il settore di attività interessato: "*a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of:*

(a) education enrollment or an education opportunity;
(b) employment or an employment opportunity;
(c) a financial or lending service;
(d) an essential government service;
(e) health-care services;
(f) housing;
(g) insurance; or

ISSN 2239-8570

(h) a legal service".

Con effetto a far data dal 1 febbraio 2026, il CAIA richiede **sia agli sviluppatori** (come definiti nel CAIA: v. *infra*) **che ai *deployers*** (come definiti nel CAIA: v. *infra*) di osservare un obbligo di ragionevole attenzione (*reasonable care*) per proteggere i consumatori da ogni conosciuto o ragionevolmente prevedibile rischio di discriminazione algoritmica (come definita nel CAIA: v. *infra*), e fissa alcune presunzioni relative (*rebuttable presumption*s) per provare l'osservanza di tale obbligo.

Lo sviluppatore (*deployer*) è definito nel CAIA come una persona che esercita un'attività per scopo di lucro nello Stato del Colorado ("*a person doing business in this State*") e sviluppa o modifica intenzionalmente e sostanzialmente un sistema ad alto rischio.

Il *deployer* è definito nel CAIA come una persona che esercita un'attività per scopo di lucro nello Stato del Colorado e che utilizza un sistema ad alto rischio.

La discriminazione algoritmica (*algorithmic discrimination*) è definita nel CAIA come "qualsiasi condizione in cui l'uso di un sistema di IA ha come risultato un trattamento differenziato illegittimo o in un effetto che sfavorisce un individuo o un gruppo di individui sulla base della loro effettiva o percepita età, colore della pelle, disabilità, etnia, informazioni genetiche, scarsa padronanza della lingua inglese, origine nazionale, razza, religione, salute riproduttiva, genere sessuale, stato di veterano, o altre classificazioni protette dalle leggi del Colorado o federali".

Per quanto riguarda gli sviluppatori, il CAIA presume (presunzione relativa) che lo sviluppatore di un sistema ad alto rischio abbia adempiuto al dovere di ragionevole attenzione per proteggere i consumatori da ogni conosciuto o ragionevolmente prevedibile rischio di discriminazione algoritmica se lo sviluppatore ha posto in essere determinati comportamenti previsti dal CAIA, tra cui:

- aver reso disponibile al deployer una dichiarazione che rivela le informazioni specifiche riguardanti il sistema ad alto rischio;
- aver reso disponibile al deployer le informazioni e la documentazione necessarie per completare una valutazione di impatto (*impact assessment*) del sistema ad alto rischio;
- aver fatto una dichiarazione aperta al pubblico che riassume i tipi di sistemi ad alto rischio che lo sviluppatore ha sviluppato o che ha intenzionalmente e sostanzialmente modificato e che attualmente mette a disposizione di un deployer o di altro sviluppatore e che indichi come lo sviluppatore gestisce i rischi conosciuti o prevedibili di discriminazione algoritmica che possono sorgere dallo sviluppo o dalla intenzionale e sostanziale modifica di ciascuno di tali sistemi ad alto rischio; e
- aver rivelato all'*attorney general* e ad ogni deployer o altro sviluppatore conosciuti del sistema ad alto rischio tutti i rischi conosciuti o prevedibili di discriminazione algoritmica, entro 90 giorni dalla scoperta o dal ricevimento di un attendibile rapporto del deployer che il sistema ad alto rischio ha causato o ha probabilmente causato rischi di discriminazione algoritmica.

ISSN 2239-8570

Similmente, per quanto riguarda i deployers, il CAIA presume (presunzione relativa) che il deployer di un sistema ad alto rischio abbia adempiuto al dovere di ragionevole attenzione per proteggere i consumatori da ogni conosciuto o ragionevolmente prevedibile rischio di discriminazione algoritmica se il deployer ha posto in essere determinati comportamenti previsti dal CAIA, tra cui:

- aver implementato un programma e una procedura di gestione del rischio per il sistema ad alto rischio;
- aver completato una valutazione di impatto del sistema ad alto rischio;
- aver rivisto con cadenza annuale l'uso del sistema ad alto rischio per assicurarsi che non stia causando una discriminazione algoritmica;
- aver specificamente avvertito i consumatori in modo dettagliato se il sistema ad alto rischio prende o costituisce un fattore rilevante nel prendere una decisione consequenziale che concerne il consumatore;
- aver dato ai consumatori la possibilità di correggere qualsiasi dato personale inesatto trattato dal sistema ad alto rischio per prendere una decisione consequenziale;
- aver dato ai consumatori la possibilità di impugnare, attraverso una revisione umana se tecnicamente possibile, una decisione consequenziale avversa che concerne i consumatori che origina dall'uso di un sistema ad alto rischio;
- aver fatto una dichiarazione aperta al pubblico che riassume i tipi di sistemi ad alto rischio che il deployer attualmente usa e che indichi come il deployer gestisce i rischi conosciuti o prevedibili di discriminazione algoritmica che possono sorgere dall'uso di ciascuno di tali sistemi ad alto rischio e la natura, la fonte e la portata delle informazioni raccolte e utilizzate dal deployer; e
- aver rivelato all'*attorney general* la scoperta della discriminazione algoritmica che il sistema ad alto rischio ha causato, entro 90 giorni dalla scoperta.

Ogni persona che esercita un'attività per scopo di lucro nello Stato del Colorado ("*a person doing business in this State*"), compresi il deployer o altro sviluppatore, che sviluppa o rende disponibile un sistema di intelligenza artificiale progettato per interagire con i consumatori, deve assicurarsi che venga rivelato a ciascun consumatore che interagisce con un sistema di intelligenza artificiale, che il consumatore sta interagendo con un sistema di intelligenza artificiale.

Il CAIA specifica che esso non limita la capacità dello sviluppatore o del deployer di:

- osservare obblighi di legge;
- cooperare ad indagini se richiesto dalla legge;
- adottare misure urgenti per proteggere la vita o l'integrità fisica di un consumatore;
- porre in essere specifiche attività di ricerca, come meglio definite nel CAIA; e
- porre in essere richiami di prodotti o rimediare ad errore tecnici che pregiudicano la funzionalità di prodotti.

ISSN 2239-8570

Il CAIA prevede disposizioni idonee a consentire allo sviluppatore, al deployer o ad altre persone una difesa in giudizio, se:

- lo sviluppatore, il deployer o un'altra persona diversa dallo sviluppatore e dal deployer, coinvolta in un giudizio sull'asserita violazione del CAIA, osserva le regole sulla gestione del rischio dei sistemi di intelligenza artificiale riconosciute a livello nazionale o internazionale, come individuate nel CAIA o dall'*attorney general* (in proposito, è interessante segnalare che il CAIA cita espressamente l' *Artificial Intelligence Risk Management Framework* pubblicato dal National Institute of Standards and Technology in the United States Department of Commerce e lo standard *ISO/IEC 42001* della International Organization For Standardization); e
- lo sviluppatore, il deployer o un'altra persona diversa dallo sviluppatore e dal deployer adottano specifiche misure per individuare e correggere le violazioni del CAIA.

Ancora, è previsto che un assicuratore (come definito), una *fraternal benefit society* (come definita), o uno sviluppatore di un sistema di intelligenza artificiale usato da un assicuratore deve ritenersi in piena osservanza del CAIA se tale ente è assoggettato a leggi speciali che disciplinano il trattamento da parte degli assicuratori dei dati dei consumatori e le fonti di informazioni, algoritmi, e modelli predittivi e alle regole adottate dal *commissioner of insurance* come previsto dalla norme speciali richiamate dal CAIA.

Similmente, è previsto che le banche e le altre entità nel settore bancario (come meglio individuate e definite nel CAIA) devono ritenersi in piena osservanza del CAIA se sono assoggettate allo scrutinio di un'autorità statale o federale ai sensi della legislazione applicabile e le relative norme o linee guida hanno ad oggetto l'uso di sistemi ad alto rischio e prevedono requisiti comparabili a quelli del CAIA o più severi, come meglio specificato nel CAIA.

Infine, dal punto di vista dell'inquadramento sistematico del CAIA e del suo *enforcement*, è notevole segnalare che la violazione delle disposizioni del CAIA costituisce una *deceptive trade practice* ai sensi del "*Colorado Consumer Protection Act*" (in particolare ai sensi della Sezione 6-1-105 del *Colorado Revised Statutes*, rubricata *Unfair or deceptive trade practices*); e che all'*attorney general* sono attribuiti poteri regolatori per implementare, e l'autorità esclusiva per applicare, gli obblighi e i divieti contenuti nel CAIA.

SALVATORE ORLANDO

https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf

2024/2(4)LC

ISSN 2239-8570

4. Il discorso di Papa Francesco alla sessione del G7 sull'intelligenza artificiale (13-15.6.2024) "*Uno strumento affascinante e tremendo*"

Dal 13 al 15 giugno 2024 ha avuto luogo il vertice del G7 a Borgo Egnazia nel comune di Fasano, in Puglia. Per la prima volta, al consesso internazionale ha preso parte anche il Papa che, con l'occasione, ha portato al tavolo di discussione del 14 giugno, dedicato segnatamente al tema dell'intelligenza artificiale, il punto di vista della Chiesa. Il discorso del Vescovo di Roma al Gruppo dei Sette (che, lo ricordiamo, è composto da Canada, Francia, Germania, Giappone, Italia, Regno Unito e Stati Uniti d'America) reca l'eloquente titolo "Uno strumento affascinante e tremendo" ed è volto a far emergere l'ambivalenza che pervade l'intelligenza artificiale, o meglio l'uso che di questo strumento può essere fatto dall'uomo. Per il Pontefice, la stessa IA è frutto del potenziale creativo che Dio gli ha donato, attraverso il quale è stato in grado di creare «uno strumento estremamente potente, impiegato in tantissime aree dell'agire umano: dalla medicina al mondo del lavoro, dalla cultura all'ambito della comunicazione, dall'educazione alla politica». Da qui l'ambivalenza sottolineata a più riprese che, da un lato, entusiasma l'uomo per le possibilità che offre; dall'altro, genera timore per le conseguenze che lascia presagire. Dal testo emerge la consapevolezza di trovarsi nel pieno di una vera e propria rivoluzione cognitivo-industriale, che contribuirà alla creazione di un nuovo sistema sociale caratterizzato da complesse trasformazioni epocali. Dopo aver sviluppato simili premesse, l'analisi si concentra sulla natura strumentale di questa nuova tecnologia, dalla quale è possibile inferire che i benefici o i danni che ne possono derivare per l'umanità dipenderanno dal suo impiego. Particolarmente interessante in questo passaggio argomentativo è la profondità con cui Papa Francesco tratteggia un concetto non banale, ovvero la "condizione di ulteriorità" che l'uomo vive rispetto al suo "essere biologico": «siamo esseri sbilanciati verso il-fuori-di-noi», sottolinea il Papa, «anzi radicalmente aperti all'oltre […]. La tecnologia è così una traccia di questa nostra ulteriorità». Non manca di rilevare, tuttavia, che l'umanità, proprio in forza di questa radicale libertà, ha spesso «pervertito i fini del suo essere trasformandosi in nemica di se stessa e del pianeta», disattendendo il mandato che ha ricevuto di "coltivare e custodire" il creato (cfr. *Gen* 2,15). Stessa sorte possono avere gli strumenti tecnologici, se degli stessi non viene garantita la vocazione al servizio dell'uomo; garanzia che si rinviene solo nel bilanciamento tra libertà e responsabilità offerto dall'etica. Diversamente, le peculiarità dell'intelligenza artificiale, definita come strumento complesso e *sui generis*, mettono a rischio la stessa dignità della persona, in particolare quando la stessa tecnologia è in grado di rendersi autonoma al punto da operare scelte indipendentemente dalla volontà dell'uomo o addirittura contro di essa o contro la sua dignità. Da questa prospettiva, il Papa avverte delle aberrazioni che un uso scorretto dei dati di cui l'intelligenza artificiale si alimenta potrebbe condurre a pregiudizi o formalizzare categorizzazioni basate su errori. Inoltre, nel discorso papale, la complessità di questo

ISSN 2239-8570

strumento è evidente nella c.d. intelligenza artificiale generativa, dove si ripropone il medesimo problema, ma con contorni più allarmanti. L'IA generativa, infatti, non sviluppa concetti o analisi nuove, ma ripete e rielabora ciò che trova, con il rischio di rafforzare nozioni o ipotesi, seppur non valide o illegittime. In questo modo, sottolinea Francesco, più che "generativa", essa è "rafforzativa", «nel senso che riordina i contenuti esistenti, contribuendo a consolidarli, spesso senza controllare se contengano errori o preconcetti». Aspetto questo ancora più dannoso, ad avviso del Santo Padre, poiché potenzialmente in grado di minare il processo educativo *in nuce*. Il Papa conclude rimarcando la necessità di mettere al centro la persona umana con la sua dignità e di recuperare un'ispirazione etica per la costruzione e la salvaguardia del bene comune. Nel farlo ha ricordato la firma a Roma della *Rome Call for AI Ethics* nel 2020 (su cui v. in questa Rubrica la notizia n. 7 del numero 1/2020 [2020/1(7)LC]), ha sottolineato il suo sostegno a quella forma di moderazione etica degli algoritmi e dei programmi di intelligenza artificiale (definita "algoretica") e ha ribadito al più importante vertice intergovernativo l'urgenza di una "sana" azione politica che muova in questa direzione.

LUCIO CASALINI

https://press.vatican.va/content/salastampa/it/bollettino/pubblico/2024/06/14/0504/01030.html#integrale

2024/2(5)TDMCDV

5. Approvata la nuova Direttiva sulla responsabilità per danno da prodotti difettosi (nuova "PLD")

Il 12 marzo 2024 il Parlamento europeo ha approvato il testo della nuova direttiva sulla responsabilità da prodotto difettoso ("**nuova PLD**"), in sostituzione della Direttiva 85/374/CEE (la *Product Liability Directive*, di seguito anche "**PLD**"). Dopo l'approvazione del Consiglio, la nuova PLD ed entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale dell'Unione europea. La nuova PLD è stata discussa ed infine adottata per iniziativa della Commissione europea (la **Commissione**), in particolare a seguito della proposta della Commissione del 28.9.2022 (su cui v. in questa Rubrica, notizia n. 2 del terzo numero del 2022 [2022/3(2)TDMCDV]).

La revisione della PLD risponde all'esigenza di aggiornare la disciplina della responsabilità del produttore alla luce delle moderne evoluzioni della tecnologia, con particolare riguardo ai sistemi di Intelligenza Artificiale e alle loro capacità di autoapprendimento e adattamento successivamente all'immissione sul mercato o alla messa in servizio. Si riportano di seguito i tratti salienti della nuova PLD.

ISSN 2239-8570

Per quanto riguarda il suo ambito di applicazione, la nuova PLD si applica ai prodotti immessi sul mercato o messi in servizio dopo la data della sua entrata in vigore (art. 2 nuova PLD). L'art. 4 nuova PLD si occupa, poi, di aggiornare le definizioni di cui alla PLD alla luce delle recenti evoluzioni del contesto tecnologico e produttivo. In particolare, si segnala la nuova definizione di «prodotto», che ora include ogni bene mobile, anche se integrato in un altro bene mobile o in un bene immobile o interconnesso con questi, inclusi i file per la fabbricazione digitale e il software. Similmente, la nozione di «fabbricante» viene ulteriormente articolata e specificata, includendo ora non solo chi sviluppa, produce, fabbrica un prodotto o vi appone il proprio marchio per la sua messa in circolazione, ma anche chi sviluppa, produce o fabbrica un prodotto per uso proprio.

L'art. 6 nuova PLD estende il contenuto del diritto al risarcimento del danno, che ora può essere richiesto – oltre che in caso di morte, lesioni personali e per danneggiamento o distruzione di qualsiasi bene diverso dal prodotto in sé (da cui viene eliminata la franchigia di 500 ECU) – anche per danni psicologici riconosciuti da un punto di vista medico, distruzione o corruzione di dati non usati a fini professionali e, in generale, per le perdite immateriali derivanti dal danno di cui al paragrafo 1 del medesimo articolo, nella misura in cui possono essere risarcite in base al diritto nazionale.

La nozione di «prodotto difettoso» continua, invece, a fondarsi su di una concezione "relazionale", essendo cioè parametrata sulle legittime aspettative del consumatore. Essa viene ulteriormente precisata dall'art. 7, ai sensi del quale un prodotto è considerato difettoso se non offre la sicurezza che un consumatore può legittimamente attendersi o che è prevista dal diritto dell'Unione o nazionale. Rispetto alla versione iniziale della proposta, però, il testo approvato elimina il riferimento al "grande pubblico" come parametro soggettivo delle legittime aspettative nell'accertamento della difettosità.

Inoltre, viene ampliato l'elenco di circostanze di cui il giudice nazionale deve tenere conto nel valutare la difettosità del prodotto, con particolare riguardo alle caratteristiche dei nuovi prodotti dell'era digitale e della possibilità per i produttori di mantenere il controllo su tali prodotti successivamente alla loro immissione sul mercato. Tra queste si evidenziano: c) gli effetti sul prodotto della sua capacità di continuare a *imparare* o acquisire nuove funzionalità dopo la sua immissione sul mercato o messa in servizio; d) gli effetti ragionevolmente prevedibili sul prodotto di altri prodotti che ci si può attendere siano utilizzati insieme al prodotto, anche mediante l'*interconnessione*; e) il momento in cui il prodotto è stato immesso sul mercato o messo in servizio oppure il momento in cui il prodotto è uscito dal *controllo* del fabbricante.

L'art. 8 nuova PLD offre una ricca articolazione dei soggetti responsabili identificati dalla formula «operatori economici», che comprende: a) il fabbricante di un prodotto difettoso; b) il fabbricante di un componente difettoso, se tale componente è stato integrato in un prodotto o interconnesso con un prodotto sotto il controllo del fabbricante e lo ha reso difettoso, fatta salva la responsabilità del fabbricante di cui alla lettera a); c)

ISSN 2239-8570

nel caso di un fabbricante di un prodotto o di un componente stabilito al di fuori dell'Unione, e fatta salva la responsabilità di tale fabbricante, l'importatore, il rappresentante autorizzato o il fornitore di servizi di logistica. Al fabbricante è equiparato chiunque modifichi in maniera sostanziale un prodotto al di fuori del controllo del fabbricante e lo metta successivamente a disposizione sul mercato o in servizio. L'art. 12 nuova PLD completa l'articolazione dei soggetti responsabili, optando ancora una volta per una forma di responsabilità solidale tra tutti i soggetti coinvolti nel processo di produzione, fatto sempre salvo il diritto di rivalsa secondo la legislazione nazionale (art. 14 nuova PLD).

Una delle principali novità del nuovo testo risiede nella *divulgazione* degli elementi di prova introdotta dall'art. 9 nuova PLD. Su richiesta di un danneggiato che, in un procedimento dinanzi ad un giudice nazionale, ha presentato fatti e prove sufficienti a sostenere la plausibilità della domanda di risarcimento, il convenuto è tenuto, conformemente al diritto nazionale, a divulgare i pertinenti elementi di prova a sua disposizione, purché tale divulgazione sia limitata a quanto necessario e proporzionato tenendo conto dei legittimi interessi di tutte le parti, specialmente per quanto riguarda la protezione delle informazioni riservate e dei segreti commerciali.

Altre serie di novità vengono introdotte dall'art. 10 nuova PLD in tema di onere della prova. Il contenuto dell'onere della prova gravante sul danneggiato rimane sostanzialmente il medesimo, dovendo questi provare il carattere difettoso del prodotto, il danno subito e il nesso di causalità tra difetto e danno. Tuttavia, nei paragrafi successivi vengono introdotti due meccanismi presuntivi finalizzati ad alleviare l'onere della prova sul consumatore.

La prima presunzione riguarda il carattere difettoso del prodotto, che scatta qualora sia soddisfatta una delle seguenti condizioni: a) il convenuto omette di divulgare i pertinenti elementi di prova a norma dell'articolo 9 nuova PLD; b) l'attore dimostra che il prodotto non rispetta i requisiti obbligatori di sicurezza del prodotto stabiliti dal diritto dell'Unione o nazionale intesi a proteggere dal rischio del danno subito dal danneggiato; o c) l'attore dimostra che il danno è stato causato da un malfunzionamento evidente del prodotto durante l'utilizzo ragionevolmente prevedibile o in circostanze ordinarie.

La seconda presunzione concerne il nesso di causalità tra difetto e danno e scatta nel caso in cui sia stato provato che il prodotto è difettoso e che la natura del danno cagionato è generalmente coerente con il difetto in questione. In ogni caso, il giudice può presumere tanto la difettosità quanto il nesso di causalità qualora, nonostante la divulgazione di prove a norma dell'articolo 9 e tenuto conto di tutte le circostanze pertinenti del caso, l'attore incontri difficoltà eccessive nel provare tali elementi a causa della complessità tecnica o scientifica, purché dimostri probabile che il prodotto sia difettoso o che esista un nesso di causalità tra il carattere difettoso e il danno. Tutte le presunzioni introdotte dall'art. 10 nuova PLD sono superabili dal convenuto, che quindi è autorizzato a fornire la prova contraria.

ISSN 2239-8570

L'art. 11 nuova PLD in tema di esenzione dalla responsabilità ripercorre quasi pedissequamente l'art. 7 PLD, ma articola alcune prove liberatorie rispetto alle specifiche categorie di soggetti responsabili considerate. Costituisce assoluta novità, invece, quanto previsto dal secondo paragrafo, che esclude l'esenzione da responsabilità per il cd. "difetto sopravvenuto" (lett. c) qualora il difetto, in costanza di controllo da parte del fabbricante, sia stato causato da: a) un servizio correlato; b) un software, compresi i relativi aggiornamenti o migliorie; c) la mancanza degli aggiornamenti o delle migliorie del software necessari per mantenere la sicurezza; d) una modifica sostanziale del prodotto.

Ancora in punto di esenzione da responsabilità, l'art. 18 nuova PLD introduce un'articolata disciplina in tema di deroga all'esonero basato sui rischi di sviluppo. Infatti, gli Stati membri possono mantenere, introdurre o modificare nei loro regimi giuridici le misure esistenti che ammettono la responsabilità degli operatori economici anche se dimostrano che lo stato oggettivo delle conoscenze scientifiche e tecniche non permetteva di scoprire l'esistenza del difetto. Tuttavia, nel caso di introduzione e modificazione di tali misure, esse dovranno: a) essere limitate a specifiche categorie di prodotti; b) essere giustificate da obiettivi di interesse pubblico; c) essere proporzionate, ovvero idonee a garantire il raggiungimento degli obiettivi perseguiti. Di tali misure lo Stato membro che intenda introdurne o modificarne dovrà dare avviso alla Commissione europea la quale, entro sei mesi dal ricevimento della notifica, potrà formulare un parere sul testo della misura proposta e sulla motivazione di tale misura, tenendo conto di eventuali osservazioni ricevute da altri Stati membri.

Sostanzialmente invariati rimangono, infine, i termini di prescrizione e di decadenza e le disposizioni sul c.d. periodo di scadenza (artt. 16 e 17 nuova PLD), se non per il coordinamento dell'individuazione del *dies a quo* dei vari termini con le caratteristiche dei prodotti nell'era digitale.

TOMMASO DE MARI CASARETO DAL VERME

https://www.europarl.europa.eu/news/it/press-room/20240308IPR18990/prodotti-difettosi-proteggere-meglio-i-consumatori-dai-danni

2024/2(6)EWDM

6. Approvato l'eIDAS2 regolamento (UE) 2024/1183 che modifica il regolamento (UE) n. 910/2014 sul quadro europeo per l'identità digitale

A partire dal 30 aprile 2024 è entrato in vigore il Regolamento (UE) 2024/1183 dell'11 aprile 2024 (di seguito "**Regolamento eIDAS 2**" – acronimo di *electronic IDentification Authentication and Signature 2*- o il "**Regolamento**") che, modificando il Regolamento (UE) n. 2014/910 (di

ISSN 2239-8570

seguito "**Regolamento eIDAS**" o "**il primo Regolamento**"), introduce un nuovo quadro normativo per l'identità digitale.

L'obiettivo del Regolamento è di dare accesso ai cittadini europei a servizi fiduciari digitali altamente sicuri e a identità digitali spendibili in tutto il territorio dell'Unione.

L'art. 1 precisa che il Regolamento eIDAS 2:

- fissa le condizioni alle quali gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche, che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro e forniscono e riconoscono i portafogli europei di identità digitale;
- stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;
- istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato, i servizi relativi ai certificati di autenticazione di siti web, l'archiviazione elettronica, gli attestati elettronici di attributi, i dispositivi di una firma elettronica, i dispositivi per la creazione di sigilli elettronici e i registri elettronici.

In particolare, le novità sono due:

- la creazione del portafoglio europeo di identità digitale ("**EDIW**" – *European Digital Identity Wallet*), e
- la revisione e l'ampliamento dei servizi fiduciari stabiliti dal primo Regolamento, coinvolgendo in misura maggiore i fornitori di servizi digitali e i *Qualified Trust Service Provider*. Viene infatti inserita tra i servizi fiduciari la conservazione digitale (o "conservazione a norma"). Ad essi vanno aggiunti i servizi di archiviazione elettronica di dati e documenti elettronici, la registrazione dei dati in registri elettronici, il rilascio e la convalida di attestati elettronici di attributi, la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza.

L'EDIW permette di introdurre un'identità digitale unica, sicura e interoperabile su tutto il territorio dell'Unione. Si configura come un'identità digitale a tutti gli effetti, proprio come lo SPiD, ma sarà valida obbligatoriamente in tutti i Paesi membri e avrà la struttura di un "portafoglio" digitale in cui potranno essere raccolte informazioni risultanti da certificazioni e documenti verificabili e verificati – i cosiddetti "attributi" – quali estremi di passaporto, certificato di nascita, patente e tessera elettorale. Viene in rilievo in proposito la definizione di "attributo", come "la caratteristica, la qualità, il diritto o l'autorizzazione di una persona fisica o giuridica o di un oggetto" (nuovo articolo 3, n. 43 del Regolamento eIDAS introdotto dal Regolamento eIDAS 2).

Inoltre, l'inserimento della c.d. "conservazione a norma" tra i servizi fiduciari qualificati permette il riconoscimento degli effetti giuridici e dell'ammissibilità come prova in giudizio, se conservati in archivi digitali,

ISSN 2239-8570

di dati, documenti elettronici e documenti analogici trasformati in digitale tramite scansione elettronica.

Gli attributi indicati nell'EDIW, contenuti nell'Allegato VI del Regolamento eIDAS2 sono: l'indirizzo, l'età, il genere, lo stato civile, la composizione del nucleo familiare, la nazionalità e cittadinanza, i titoli e licenze di studio, qualifiche e licenze professionali, poteri e mandati di rappresentanza di persone fisiche e giuridiche, permessi e licenze pubblici per le persone giuridiche.

Con il Regolamento eIDAS 2 gli Stati membri sono obbligati ad accettare le identità digitali degli altri Paesi e risulta definito, a livello euro-unitario, chi e quanti sono i gestori di *wallet* che devono offrire un'interfaccia comune per tutti gli utenti in ordine all'autenticazione per la fruizione dei servizi.

Sarà quindi possibile non solo accedere ai servizi pubblici con la propria identità digitale in ogni Paese UE, ma anche, aprire un conto corrente, o eseguire operazioni bancarie, interagire con i trasporti, con le imprese energetiche, con i servizi finanziari, della sicurezza e previdenza sociale, della sanità, dell'acqua potabile, servizi postali, istruzione e telecomunicazioni.

Altro elemento rilevante sono le nuove sanzioni previste all'art. 16 del Regolamento eIDAS 2 in forza del quale gli Stati membri provvedono affinché le violazioni del medesimo Regolamento da parte di prestatori di servizi fiduciari qualificati e non qualificati siano soggette a sanzioni amministrative pari a un importo massimo di almeno:

a) euro 5.000.000 se il prestatore di servizi fiduciari è una persona fisica; oppure
b) se il prestatore di servizi fiduciari è una persona giuridica, euro 5.000.000 o pari all'1% del fatturato mondiale totale annuo dell'impresa a cui apparteneva il prestatore di servizi fiduciari nell'esercizio precedente l'anno in cui si è verificata la violazione, se superiore.

A seconda dell'ordinamento giuridico degli Stati membri, le regole in materia di sanzioni amministrative possono essere applicate in modo tale che la procedura sanzionatoria sia avviata dall'organismo di vigilanza competente e la sanzione pecuniaria sia irrogata dai tribunali nazionali competenti. L'applicazione di tali regole in tali Stati membri garantisce che tali mezzi di ricorso siano efficaci e abbiano un effetto equivalente alle sanzioni amministrative imposte direttamente dalle autorità di controllo.

ETTORE WILLIAM DI MAURO

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401183

2024/2(7)BP

7. Approvato il regolamento (UE) 2024/900 sulla trasparenza e il targeting della pubblicità politica

ISSN 2239-8570

Il 13 marzo 2024 è stato adottato il Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio relativo alla trasparenza e al targeting della pubblicità politica, (di seguito il **Regolamento**). La relativa proposta COM(2021) 731 *final*, era stata pubblicata il 25 novembre 2021 (v. in questa Rubrica la notizia n. 6 del numero 1/2022 [2022/1(6)SO]).

Come sancito dal suo art. 1(4), gli obiettivi perseguiti dal Regolamento sono: garantire, attraverso la previsione di norme armonizzate, il corretto funzionamento del (frammentario ed eterogeneo – cfr. Considerando 7-9 Regolamento) mercato interno della pubblicità politica (art. 1(4)(a) Regolamento) e «tutelare i diritti e le libertà fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla vita privata e la protezione dei dati personali» (art. 1(4)(b) Regolamento), assicurando - come più ampiamente esplicitato nei considerando - un elevato livello di trasparenza affinché i cittadini possano «esercitare i diritti democratici in maniera consapevole», giacché «una pubblicità politica trasparente aiuta l'elettore e gli individui in generale a capire meglio quando è in presenza di un messaggio di pubblicità politica, per conto di chi è fatta quella pubblicità nonché come e perché è diventato il target di un prestatore di servizi pubblicitari, ponendolo così in condizioni migliori per una scelta informata» (cfr. Considerando 4 Regolamento).

Sul piano strutturale, ai 114 Considerando, seguono 30 articoli, suddivisi in 5 Capi. Nel Capo I (artt. 1-5), come di consueto, si trovano le disposizioni generali. Seguono - come espone l'art. 1(1), dando conto dell'oggetto del Regolamento - norme sugli obblighi di trasparenza e sugli obblighi relativi al dovere di diligenza per i servizi di pubblicità politica (Capo II, artt. 6-17); norme sull'uso delle tecniche di targeting e consegna del messaggio pubblicitario che comportano il trattamento di dati personali (Capo III, artt. 18-20); norme sul controllo e sull'esecuzione del Regolamento (Capo IV, artt. 21-26). Chiudono le disposizioni finali (Capo V, artt. 27-30).

L'art. 2 Regolamento definisce l'ambito di applicazione. Come pure per gli altri atti che interessano il "mercato unico digitale", il Regolamento tende ad avere portata "extraterritoriale", applicandosi non solo «alla pubblicità politica laddove il messaggio di pubblicità politica sia diffuso nell'Unione» e «sia reso di dominio pubblico in uno o più Stati membri», ma anche quando «sia rivolto ai cittadini dell'Unione, indipendentemente dal luogo di stabilimento del prestatore di servizi di pubblicità politica o dal luogo di residenza o stabilimento dello sponsor, e a prescindere dai mezzi utilizzati».

All'art. 3 Regolamento sono, poi, sancite le fondamentali definizioni che scandiscono la materia. Tra queste, si segnalano specialmente le seguenti:

- "pubblicità politica": «la preparazione, collocazione, promozione, pubblicazione, consegna o diffusione, con qualsiasi mezzo, di un messaggio fornito normalmente dietro retribuzione o tramite attività interne o nell'ambito di una campagna di pubblicità politica: a) di, a favore o per conto di un attore politico, salvo se di natura meramente privata o meramente commerciale; oppure b) che possa e sia inteso a influenzare l'esito di un'elezione o referendum, un comportamento di voto o un processo

ISSN 2239-8570

legislativo o regolamentare, a livello dell'Unione, nazionale, regionale o locale» (art. 3, n. 2 Regolamento); peraltro, oltre alle esclusioni previste dalla stessa definizione dell'art. 3, n. 2, cui si rinvia, si rilevano come espressamente escluse, ai sensi dell'art. 1(2) Regolamento, anche le «opinioni politiche e altri contenuti editoriali soggetti alla responsabilità editoriale, indipendentemente dal mezzo attraverso cui sono espressi, […] a meno che non siano previsti un pagamento specifico o altra remunerazione per la loro preparazione, collocazione, promozione, pubblicazione, consegna o diffusione da parte di terzi o in relazione a tali attività»;

- "servizio di pubblicità politica": «un servizio che offre pubblicità politica, diverso da un servizio intermediario online ai sensi dell'articolo 3, lettera g), del regolamento (UE) 2022/2065 [il *Digital Services Act*], fornito senza corrispettivo per la preparazione, collocazione, promozione, pubblicazione, consegna o diffusione del messaggio specifico» (art. 3, n. 5 Regolamento; sul *Digital Services Act*, v. in questa Rubrica la notizia n. 1 del numero 4/2022 [2022/4(1)ST]);

- "messaggio di pubblicità politica": «un esempio di pubblicità politica indipendentemente dal mezzo utilizzato per la pubblicazione, la consegna o la diffusione» (specificandosi poi oltre, all'art. 8, una serie di esemplificativi parametri in virtù dei quali poter determinare se un messaggio debba qualificarsi come tale, i quali sono segnatamente: a) il contenuto del messaggio; b) lo sponsor del messaggio; c) la lingua utilizzata per trasmettere il messaggio; d) il contesto in cui il messaggio è trasmesso, compreso il periodo di diffusione; e) i mezzi con cui il messaggio è preparato, collocato, promosso, pubblicato, consegnato o diffuso; f) i destinatari; g) l'obiettivo del messaggio);

- "sponsor": «la persona fisica o giuridica su richiesta della quale o per conto della quale è preparato, collocato, promosso, pubblicato, consegnato o diffuso un messaggio di pubblicità politica» (art. 3, n. 10 Regolamento);

- "tecniche di targeting": «le tecniche usate per rivolgere un messaggio di pubblicità politica solo a una persona specifica o a un gruppo specifico di persone, o per escludere tale persona o gruppo di persone, sulla base del trattamento di dati personali» (art. 3, n. 11 Regolamento);

- "tecniche di consegna del messaggio pubblicitario": «tecniche di ottimizzazione utilizzate per aumentare la circolazione, la portata o la visibilità di un messaggio di pubblicità politica sulla base del trattamento automatizzato di dati personali e che possono servire a consegnare il messaggio di pubblicità politica a una persona specifica o a un gruppo specifico di persone» (art. 3, n. 12 Regolamento);

- "editore di pubblicità politica": «il prestatore di servizi di pubblicità politica che pubblica, consegna o diffonde pubblicità politica con qualsiasi mezzo» (art. 3, n. 13 Regolamento).

L'art. 4 Regolamento segna l'imperatività della normativa approntata dal Regolamento, da un lato, vietando agli Stati membri di mantenere o introdurre «per motivi di trasparenza della pubblicità politica disposizioni o misure divergenti da quelle stabilite nel regolamento» e, dall'altro lato, prescrivendo che «non può essere vietata né limitata per motivi di trasparenza, neppure a livello geografico, la prestazione di servizi di

ISSN 2239-8570

pubblicità politica conforme alle prescrizioni» del medesimo. Il successivo art. 5 altresì vieta ai prestatori di servizi di pubblicità politica di subordinare «la prestazione dei loro servizi a restrizioni discriminatorie basate unicamente sul luogo di residenza o di stabilimento dello sponsor».

Passando all'analisi della più corposa parte della disciplina, quella di cui al capo II sugli obblighi di trasparenza e diligenza, l'art. 7 Regolamento si occupa anzitutto della «individuazione dei servizi di pubblicità politica», imponendo agli sponsor e ai prestatori di servizi pubblicitari che agiscono per conto di questi di «dichiarare se il servizio pubblicitario che hanno chiesto al prestatore di servizi pubblicitari configura un servizio di pubblicità politica».

Mentre, poi, gli artt. 9 e 10 Regolamento pongono obblighi di trasparenza in capo ai prestatori di servizi di pubblicità politica, gli artt. 11 e 12 Regolamento dettano invece puntuali obblighi in capo all'editore in relazione al singolo "messaggio di pubblicità politica" diffuso. Più in particolare, ai primi è richiesto di tenere dei «registri» (art. 9 Regolamento) per la conservazione delle informazioni concernenti: «a) il messaggio di pubblicità politica o la campagna di pubblicità politica cui sono connessi il servizio o i servizi; b) il servizio o i servizi specifici che hanno fornito in relazione alla pubblicità politica; c) gli importi fatturati per il servizio o i servizi che hanno fornito e il valore di altre prestazioni percepite in cambio parziale o integrale di detto servizio o servizi; d) informazioni circa l'origine pubblica o privata degli importi e delle altre prestazioni di cui alla lettera c), nonché informazioni sulla loro provenienza dall'interno o dall'esterno dell'Unione; e) l'identità e i dati di contatto dello sponsor del messaggio di pubblicità politica e, ove applicabile, dell'entità che in ultima istanza controlla lo sponsor nonché, per le persone giuridiche, il luogo di stabilimento; e f) ove applicabile, l'indicazione dell'elezione, del referendum o del processo legislativo o regolamentare cui è connesso il messaggio di pubblicità politica». Tali medesime informazioni, devono essere trasmesse dai prestatori di servizi di pubblicità politica agli editori «in modo tempestivo, completo e accurato» (art. 10 Regolamento).

Quanto invece agli obblighi in capo agli editori, gli artt. 11 e 12 Regolamento, già richiamati, sembrano rispettivamente predisporre un meccanismo di trasparenza informativa, per così dire, "stratificata", che distingue, potrebbe cioè dirsi, tra due "livelli di specificità informativa crescente". In primo luogo, infatti, è fatto obbligo agli editori di provvedere affinché ciascun messaggio di pubblicità politica riporti in modo chiaro, ben visibile e privo di ambiguità, sotto forma di etichette che consentono alle persone di identificare facilmente come tale un messaggio di pubblicità politica (art. 11(1) e (3) Regolamento), le seguenti informazioni (in parte coincidenti con quelle di cui all'art. 9 Regolamento): «a) una dichiarazione attestante che si tratta di un messaggio di pubblicità politica; b) l'identità dello sponsor del messaggio di pubblicità politica e, ove applicabile, dell'entità che in ultima istanza controlla lo sponsor; c) ove applicabile, l'indicazione dell'elezione, del referendum o del processo legislativo o regolamentare cui è connesso il messaggio di pubblicità politica; d) ove applicabile, una dichiarazione attestante che il messaggio di pubblicità

ISSN 2239-8570

politica è stato oggetto di tecniche di targeting o di consegna del messaggio; e) un avviso di trasparenza che contenga le informazioni di cui all'articolo 12(1) Regolamento, oppure l'indicazione chiara di dove lo si possa reperire facilmente e in modo diretto». Il secondo "livello informativo" è appunto costituito invece dalle più specifiche informazioni elencate dall'art. 12 Regolamento e contenute nel c.d. «avviso di trasparenza». Tra queste, si segnalano: «a) l'identità dello sponsor e, ove applicabile, dell'entità che in ultima istanza controlla lo sponsor, compresi il nome, l'indirizzo e-mail e, se reso pubblico, l'indirizzo postale nonché, se lo sponsor non è una persona fisica, l'indirizzo presso il quale ha il suo luogo di stabilimento; b) le informazioni di cui alla lettera a) sulla persona fisica o giuridica che fornisce una retribuzione in cambio del messaggio di pubblicità politica […]; c) il periodo durante il quale è prevista la pubblicazione, la consegna o la diffusione del messaggio di pubblicità politica; d) gli importi aggregati e il valore aggregato di altre prestazioni percepiti dai prestatori di servizi di pubblicità politica, compresi quelli percepiti dall'editore, in cambio parziale o integrale dei servizi di pubblicità politica e se del caso, della campagna di pubblicità politica; e) informazioni circa l'origine pubblica o privata degli importi e delle altre prestazioni di cui alla lettera d), nonché informazioni sulla loro provenienza dall'interno o dall'esterno dell'Unione; […] l) ove applicabile, una dichiarazione attestante che il messaggio di pubblicità politica è stato oggetto di tecniche di targeting o di consegna del messaggio pubblicitario sulla base dell'uso di dati personali, comprese le informazioni di cui all'articolo 19(1)(c) ed (e); m) ove applicabile e tecnicamente fattibile, la portata del messaggio di pubblicità politica in termini di numero di visualizzazioni e reazioni». Se tali informazioni non possono essere completate senza indebito ritardo, è fatto divieto all'editore di rendere disponibile il messaggio e, in caso di precedente diffusione, ne deve interrompere la pubblicazione, informando gli sponsor o i prestatori di servizi di pubblicità politica interessati della decisione adottata (art. 12(2) Regolamento).

Ancora, a finalità di trasparenza, per così dire, "diffusa" rispondono altresì le disposizioni di cui agli artt. 13 e 14 Regolamento. La prima prevede che la Commissione istituisca un «registro europeo» dei messaggi di pubblicità politica online, ovvero «un registro pubblico di tutti i messaggi di pubblicità politica online pubblicati nell'Unione o diretti a cittadini o residenti dell'Unione», che consenta «l'accesso del pubblico ai messaggi di pubblicità politica online, unitamente alle informazioni fornite dagli editori di pubblicità politica di cui all'art. 12(1) Regolamento, in relazione a ciascun messaggio di pubblicità politica online». Ai sensi della seconda disposizione, si impongono invece agli editori di pubblicità politica «relazioni periodiche sui servizi di pubblicità politica» che includano «informazioni sugli importi fatturati o sul valore di altre prestazioni percepite in cambio parziale o integrale dei servizi forniti, compreso l'uso di tecniche di targeting e di consegna del messaggio pubblicitario».

L'art. 15 Regolamento, proseguendo, fa obbligo agli editori di predisporre meccanismi «gratuiti, di facile uso e facilmente fruibili» (par. 2) «per consentire alle persone fisiche o giuridiche di segnalare che un

ISSN 2239-8570

determinato messaggio di pubblicità politica di loro pubblicazione non è conforme» al Regolamento (par. 1). Una differenza si rileva sul piano strettamente letterale circa gli obblighi successivi alla segnalazione, a seconda che gli editori siano o meno "piattaforme online di dimensioni molto grandi" o "motori di ricerca online di dimensioni molto grandi" secondo le nozioni di cui al *Digital Services Act*: nel primo caso, essi «esaminano e trattano le segnalazioni ricevute» (par. 5); nel secondo, «si adoperano in ogni modo per esaminare e trattare le segnalazioni ricevute» (par. 6).

Se, infine, ai sensi dell'art. 16 Regolamento è previsto che le autorità nazionali competenti abbiano facoltà di chiedere ai prestatori di servizi di pubblicità politica di trasmettere le informazioni necessarie a verificare la conformità alle disposizioni regolamentari, senz'altro di interesse è altresì la previsione di un'analoga facoltà posta dal successivo art. 17 in capo ad alcune categorie di «soggetti interessati» (tra cui ricercatori, giornalisti e attori politici – cfr. art. 17(2) Regolamento, i quali possono appunto chiedere che gli siano trasmesse «tempestivamente e gratuitamente e, ove tecnicamente possibile in formato leggibile da dispositivo automatico» le informazioni di cui agli artt. 9, 11 e 12 Regolamento.

Volgendo lo sguardo al Capo III in materia di «targeting e consegna del messaggio di pubblicità politica online», tali pratiche sono anzitutto consentite, ai sensi dell'art. 18 Regolamento, solo se rispettano i seguenti stringenti limiti: a) il titolare del trattamento ha raccolto i dati personali presso l'interessato; b) l'interessato ha prestato il proprio consenso esplicito al trattamento a fini di pubblicità politica; c) tali tecniche non comportano la "profilazione" (ne significato di cui all'art. 4(4) GDPR) utilizzando le "categorie particolari" di dati personali di cui all'art. 9 GDPR. Il paragrafo secondo del medesimo articolo, poi, vieta «le tecniche di targeting o di consegna del messaggio pubblicitario che comportano il trattamento dei dati personali di un soggetto di cui il titolare del trattamento sa, con ragionevole certezza, che è almeno un anno al di sotto dell'età per l'esercizio del voto prestabilita dalle norme nazionali». I titolari del trattamento, inoltre, devono assicurare, ai sensi dell'art. 18(4) Regolamento, che «a) all'interessato non sia richiesto il consenso se ha già indicato con mezzi automatizzati che non acconsente al trattamento dei dati a fini di pubblicità politica, a meno che la richiesta non sia giustificata da un mutamento sostanziale delle circostanze; b) all'interessato che non presta il proprio consenso sia offerta un'alternativa equivalente per l'utilizzo del servizio online senza ricevere pubblicità politica».

Confinata l'attività di targeting entro il rispetto dei richiamati requisiti e divieti, l'art. 19 Regolamento prevede quindi degli «obblighi di trasparenza addizionali» oltre a quelli sopra riportati previsti dal Capo II del Regolamento. Segnatamente, è fatto obbligo ai titolari del trattamento di: a) adottare e rendere pubblico «un documento di strategia interna che descriva chiaramente e con linguaggio semplice come tali tecniche sono utilizzate»; b) conservare registri sull'uso di tali tecniche, sui meccanismi e i parametri applicati; c) trasmettere, «contestualmente all'indicazione che si tratta di un messaggio di pubblicità politica, informazioni supplementari per permettere

ISSN 2239-8570

all'interessato di comprendere la logica utilizzata e i principali parametri delle tecniche applicate, ivi compreso se per indirizzare o consegnare la pubblicità politica sia stato utilizzato un sistema di intelligenza artificiale e se siano state usate altre tecniche analitiche»; d) preparare «una valutazione interna annuale dei rischi dell'uso di tali tecniche di targeting o di consegna del messaggio pubblicitario sui diritti e le libertà fondamentali, i cui risultati devono essere resi pubblici; e) fornire «un riferimento ai mezzi effettivi di cui dispone l'interessato per l'esercizio dei propri diritti» e in particolare «un riferimento ai diritti dell'interessato di modificare i dati personali o revocare il consenso». Tali informazioni, prevede poi l'art. 20 Regolamento, devono essere trasmesse, su richiesta e gratuitamente, ai già menzionati "soggetti interessati" di cui all'art. 17 Regolamento.

Quanto al Capo IV, recante disposizioni su «controllo ed esecuzione», esso anzitutto richiede che il prestatore di servizi di pubblicità politica non stabilito nell'Unione designi «per iscritto una persona fisica o giuridica come suo rappresentante legale in uno degli Stati membri in cui offre servizi», il quale sia «competente per il rispetto degli obblighi» previsti dal Regolamento, potendo «essere ritenuto responsabile di qualsiasi inosservanza» dei medesimi (art. 21(1) e (2) Regolamento).

Gli artt. 22-25 Regolamento prevedono una serie di disposizioni che riguardano le autorità competenti.

In particolare, l'art. 22 assegna il monitoraggio del rispetto delle disposizioni del capo III sul targeting al Garante per la protezione dei dati personali di cui al GDPR o al Garante europeo della protezione dei dati di cui al regolamento (UE) 2018/1725 (di seguito **EUDPR**) (par. 1); richiede, quindi, (par. 3) agli Stati membri di designare le autorità competenti a controllare l'osservanza degli obblighi del capo II da parte dei prestatori di servizi intermediari di cui al *Digital Services Act*, (le quali, si prevede, possono anche coincidere con le stesse autorità competenti designate a norma del medesimo Regolamento (UE) 2022/2065); e impone infine, in via "residuale", (par. 4) di designare «una o più autorità competenti incaricate dell'applicazione e dell'esecuzione degli aspetti del regolamento non contemplati ai paragrafi 1 e 3» (dunque, primariamente, deve ritenersi, incaricate del controllo circa l'osservanza degli obblighi di cui al capo II da parte di prestatori di servizi che *non siano* gli intermediari di cui al *Digital Services Act*), le quali autorità possono coincidere o meno con le autorità già nominate. L'art. 23 Regolamento disciplina la «cooperazione transfrontaliera» tra autorità competenti dei diversi Stati membri. L'art. 24 Regolamento sancisce il diritto di presentare un reclamo alle autorità competenti per qualsiasi violazione del Regolamento.

Il successivo art. 25 si occupa delle sanzioni. Per quanto attiene all'inosservanza degli obblighi di cui agli artt. 18 e 19 Regolamento in materia di targeting online, si rinvia al potere delle autorità di controllo di cui al GDPR e all'EUDPR di imporre sanzioni pecuniarie «nei limiti delle loro competenze» e si prevede che le sanzioni pecuniarie siano «in linea» con quelle previste dalle disposizioni del GDPR e dell'EUDPR e a concorrenza degli importi massimi ivi previsti (art. 25(5) e (6) Regolamento). Per quanto riguarda invece l'inosservanza degli obblighi di

ISSN 2239-8570

cui al Capo II, è demandato agli Stati membri di stabilire «le norme relative alle sanzioni o alle altre misure necessarie», le quali «devono essere effettive, proporzionate e dissuasive», tenendo conto «delle norme che disciplinano la libertà di stampa e la libertà di espressione in altri mezzi di comunicazione e delle norme o dei codici che disciplinano la professione di giornalista» (art. 25(1) Regolamento). La libertà lasciata ai singoli Stati, si rileva, è comunque vincolata al rispetto di taluni "massimali", particolarmente elevati, per le "sanzioni finanziarie" (art. 25(2) Regolamento), pari: a) al 6 % delle entrate o del bilancio annui dello sponsor o del prestatore di servizi di pubblicità politica, a seconda dei casi e in funzione del valore più elevato, oppure b) al 6 % del fatturato mondiale annuo dello sponsor o del prestatore di servizi di pubblicità politica nell'esercizio precedente. Infine, l'art. 25(5) Regolamento contiene una disposizione che autorizza gli Stati membri a prevedere sanzioni periodiche per violazioni reiterate che si verifichino a ridosso di appuntamenti di voto, considerate per ciò stesso particolarmente gravi, e, nel far ciò, include nella previsione la violazione dell'art. 18 Regolamento, in materia di targeting online.

L'art. 26 Regolamento, infine, prevede che gli Stati membri pubblichino «in maniera facilmente accessibile le date di elezioni e referendum e, se del caso, dei rispettivi periodi elettorali» (par. 1) e che la Commissione metta a disposizione un portale accessibile al pubblico attraverso il quale gli Stati membri comunicano le date delle rispettive elezioni, referendum e, se del caso, periodi elettorali (par. 2).

Il Capo V, come già riferito, reca le disposizioni finali. L'art. 27 Regolamento prevede che entro due anni da ciascuna elezione del Parlamento europeo, la Commissione presenti al Parlamento e al Consiglio «una relazione sulla valutazione e sul riesame» del Regolamento, al fine di, appunto, valutare l'eventuale necessità di modificarlo, in particolare relativamente agli aspetti seguenti: a) l'ambito di applicazione del Regolamento e la definizione di pubblicità politica; b) l'efficacia del Regolamento rispetto a mezzi specifici di pubblicità politica; c) l'efficacia delle misure di trasparenza; d) l'efficacia delle norme che limitano il trattamento dei dati personali ai fini delle tecniche di targeting e di consegna del messaggio pubblicitario; e) l'efficacia della struttura di controllo e applicazione. Gli artt. 28 e 29 Regolamento disciplinano invece rispettivamente l'esercizio del potere della Commissione di adottare atti delegati e l'assistenza da parte di un comitato ai sensi del regolamento (UE) n. 182/2011. L'art. 30 Regolamento, infine, prevede che esso si applichi in via differita rispetto all'entrata in vigore (ad eccezione delle disposizioni di cui agli artt. 3 e 5(1) Regolamento), a decorrere dal 10 ottobre 2025.

BENIAMINO PARENZO

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202400900

ISSN 2239-8570

8. Approvata la direttiva sui lavoratori delle piattaforme online

Dopo uno stallo politico durato più di due anni, il 24 aprile 2024 il Parlamento europeo ha approvato definitivamente la "direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro tramite piattaforme digitali" (di seguito la "**Direttiva**"), che, dopo l'approvazione del Consiglio, attende ora solo la pubblicazione sulla Gazzetta Ufficiale dell'Unione europea. Tale iniziativa legislativa si inserisce nel piano d'azione del Pilastro Europeo dei Diritti Sociali, un documento programmatico proposto dalla Commissione Juncker e proclamato dal Consiglio dell'Unione europea, dalla Commissione e dal Parlamento al vertice di Göteborg del 2017 teso a ridare una rinnovata centralità alla dimensione sociale dell'Unione europea.

Come indicato nel terzo Considerando, la Direttiva persegue il diritto di accesso a eque condizioni di lavoro, indipendentemente dal tipo di rapporto, nonché il diritto di informazione e quello di protezione della salute e dei dati personali sul posto di lavoro.

Più nel dettaglio, la Direttiva affronta in primo luogo il problema della qualificazione del rapporto giuridico intercorrente tra i lavoratori e le piattaforme digitali. È, infatti, noto a tutti che sia in Italia che negli altri Paesi dell'Unione europea è sorto un vasto contenzioso sull'inquadramento giuridico del rapporto di lavoro dei *riders* e di chiunque svolga una prestazione in favore di una piattaforma di lavoro digitale, anche da remoto (v. in questa Rubrica la notizia n. 12 nel numero 2/2022 sulla sentenza Trib. Milano n. 1018/2022 a proposito della qualificazione del rapporto di lavoro nei confronti di Deliveroo [2022/2(12)VP]).

La Direttiva offre, innanzitutto, la definizione di "piattaforma di lavoro digitale", che viene definita dall'articolo 2 come qualsiasi soggetto che fornisca un servizio commerciale che rispetta i seguenti requisiti: a) è fornito almeno in parte a distanza con mezzi elettronici; b) è fornito su richiesta del destinatario; c) comporta, quale componente necessaria ed essenziale, l'organizzazione del lavoro di persone fisiche; d) comporta l'uso di sistemi di monitoraggio automatizzato o di sistemi decisionali automatizzati.

Questo ultimo requisito è stato inserito nel corso dell'*iter* di approvazione del testo con l'evidente obiettivo di limitare notevolmente il campo di applicazione della direttiva anche se, secondo i primi commentatori, l'efficacia pratica dell'inserimento potrebbe essere molto inferiore alle aspettative.

Il cuore della direttiva era ed è l'introduzione di una presunzione legale di subordinazione che, tuttavia, nel corso dell'iter di approvazione del testo, è stata notevolmente edulcorata.

Nella sua versione originale la direttiva prevedeva la presunzione di subordinazione del rapporto di lavoro ogniqualvolta venisse riscontrata la presenza di almeno due di cinque parametri, o indici presuntivi, tra i quali la "determinazione effettiva del livello della retribuzione" e la "effettiva

ISSN 2239-8570

limitazione della possibilità di costruire una propria clientela o di svolgere lavori per terzi".

Nel testo finale, invece, tale meccanismo automatico e vincolante è stato notevolmente ridimensionato e l'attuale articolo 4 della Direttiva si limita a prevedere che gli Stati membri debbano stabilire misure effettive per accertare l'esistenza di un rapporto di lavoro per come definito dalla legge, dalla contrattazione collettiva o dalla prassi del singolo Paese, "tenendo conto della giurisprudenza della Corte di giustizia".

Poco più di un nulla di fatto per tutti quei Paesi, come Italia, Spagna e Francia, in cui è già presente nell'ordinamento giuridico il principio di indisponibilità del tipo contrattuale lavoro subordinato che consente al lavoratore, a prescindere dalla veste formale data al rapporto di lavoro, di chiedere in via giudiziale l'accertamento della natura subordinata della relazione di lavoro.

Gli Stati membri dovranno comunque stabilire una presunzione relativa di subordinazione, con inversione dell'onere della prova nel caso in cui siano accertati "fatti che indichino controllo e direzione".

Il set di tutele predisposte per i lavoratori delle piattaforme, oltre a quanto già detto sulla presunzione di subordinazione, prevede poi misure volte a migliorare la trasparenza e la protezione dei dati personali dei lavoratori soggetti al management algoritmico, ossia, all'automazione dell'esercizio di uno o più poteri datoriali (per un caso problematico v. in questa Rubrica la notizia n. 9 nel numero 3/2021 per il provvedimento del 22.7.2021 del Garante Privacy nei confronti di Deliveroo per il trattamento dei dati personali dei riders [2021/3(9)AN]).

In questo contesto si prevede che i lavoratori, i loro rappresentanti e, su richiesta, le autorità competenti devono ricevere informazioni sull'uso di sistemi decisionali o di monitoraggio automatizzati, tra cui lo scopo di tali sistemi e i parametri utilizzati per adottare le decisioni.

Si prevede, poi, il divieto di trattare dati personali relativi allo stato emotivo e psicologico dei lavoratori, dati relativi a conversazioni private, in particolare con rappresentanti sindacali, e dati che permettano di prevedere il futuro esercizio di diritti fondamentali.

Più nel dettaglio, l'art. 7 della Direttiva vieta alle piattaforme di lavoro digitali di trattare mediante sistemi decisionali o di monitoraggio automatizzati: (a) dati personali relativi allo stato emotivo o psicologico della persona che svolge un lavoro mediante piattaforme digitali; (b) dati personali relativi a conversazioni private; (c) dati personali quando la persona che svolge un lavoro mediante piattaforme digitali non sta svolgendo un lavoro mediante le stesse o non si sta offrendo per svolgerlo; (d) dati personali per prevedere l'esercizio di diritti fondamentali, compresi il diritto di associazione, il diritto di negoziazione e di azioni collettive o il diritto all'informazione e alla consultazione, quali definiti nella Carta dei diritti fondamentali della Unione europea; (e) dati personali per desumere l'origine razziale o etnica, lo status di migrante, le opinioni politiche, le convinzioni religiose o filosofiche, la disabilità, lo stato di salute, comprese le malattie croniche o la sieropositività, lo stato emotivo o psicologico, l'adesione a un sindacato, la vita sessuale o l'orientamento sessuale di una

ISSN 2239-8570

persona; (f) i dati biometrici, come definiti nel regolamento (UE) 2016/679 (il GDPR), di una persona che svolge un lavoro mediante piattaforme digitali per stabilirne l'identità confrontandoli con i dati biometrici di persone memorizzati in una banca dati.

L'art. 17 della Direttiva introduce, poi, un diritto di accesso delle autorità nazionali a informazioni quali il numero delle persone che lavorano tramite la piattaforma, il loro inquadramento contrattuale, la remunerazione media, etc. Si tratta, senza dubbio, di poteri già oggi esercitabili dalle autorità ma la previsione appare senza dubbio utile a rafforzare il controllo pubblico sul lavoro tramite piattaforma.

Infine, appare degno di nota il tentativo di "umanizzare" il management algoritmico contenuto negli artt. 10 e 11 della Direttiva che prevedono l'obbligo di supervisione umana per i sistemi automatizzati e il diritto del lavoratore di spiegazione e revisione delle decisioni da parte di un agente umano.

RICCARDO MARAGA

https://www.europarl.europa.eu/news/it/press-room/20240419IPR20584/riders-il-parlamento-adotta-la-direttiva-sul-lavoro-delle-piattaforme

2024/2(9)FBe

9. Approvata la direttiva (UE) 2024/1799 sul diritto alla riparazione "R2R"

Con la direttiva (UE) 2024/1799 del 13 giugno 2024 recante norme comuni che promuovono la riparazione dei beni e che modifica il regolamento (UE) 2017/2394 e le direttive (UE) 2019/771 e (UE) 2020/1828, il legislatore europeo ha istituito per alcune categorie di beni il diritto del consumatore alla riparazione per difetti del bene che si verificano o si manifestano al di fuori della responsabilità del venditore ai sensi della direttiva (UE) 2019/771 (di seguito la **Direttiva** o la **direttiva R2R**, da Right to Repair, "R2R").

La direttiva R2R è stata adottata nello stesso giorno in cui è stato adottato il regolamento (UE) 2024/1781 del 13 giugno 2024 che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili, modifica la direttiva (UE) 2020/1828 e il regolamento (UE) 2023/1542 e abroga la direttiva 2009/125/CE ("**Regolamento ecodesign**").

Per la definizione di «riparazione», la direttiva R2R rimanda a quella contenuta nel Regolamento ecodesign: «una o più azioni effettuate per ripristinare il prodotto difettoso o il rifiuto [*waste* in lingua inglese] a una condizione in cui consegue la finalità cui è destinato» (art. 2, n. 20 Regolamento ecodesign).

Nonostante alcune scelte di compromesso adottate nell'intervenire sulla direttiva (UE) 2019/771 (sul cui recepimento in Italia, v. in questa Rubrica

ISSN 2239-8570

notizia n. 1 nel numero 4/2021 [2021/4(1)FB]), l'istituzione del diritto alla riparazione del bene rappresenta un passo in avanti nel percorso verso la sostenibilità di produzione e consumo (obiettivo 12 dei *Sustainable Development Goals*, SDGs, dell'Agenda 2030 per lo sviluppo sostenibile adottata il 25.9.2015 dall'Assemblea Generale delle Nazioni Unite) e l'instaurazione di un'economia circolare (Considerando 5 direttiva R2R).

La direttiva R2R stabilisce infatti norme comuni per rafforzare le disposizioni relative alla riparazione dei beni, mirando a migliorare il funzionamento del mercato interno sia sul versante dell'innalzamento del livello di protezione dei consumatori, sia su quello della riduzione dell'impatto dei prodotti sull'ambiente mediante l'allungamento del loro possibile ciclo di vita e la facilitazione del c.d. "ricondizionamento" (Considerando 1, 3 direttiva R2R).

Dalla necessità di tentare di rispondere alle istanze di sostenibilità in modo uniforme all'interno dell'Unione deriva quella di assicurare che le modalità con cui gli Stati membri daranno attuazione alla direttiva R2R non ostacolino l'operatività transfrontaliera e anzi consentano a produttori e venditori di operare in uno scenario di certezza. Il grado di armonizzazione prescelto dal legislatore europeo risponde a entrambe le esigenze: in linea con la parabola evolutiva della normativa consumeristica a partire dalla direttiva 2005/29/CE sulle pratiche commerciali sleali, la direttiva R2R segue la linea della *full harmonisation* (art. 3 direttiva R2R).

L'art. 3 della Direttiva preclude infatti agli Stati membri di mantenere o adottare disposizioni "divergenti" da quelle stabilite all'interno della normativa europea. In questa prospettiva, l'armonizzazione massima dovrebbe accrescere la fiducia dei consumatori circa i propri diritti e fugare i dubbi sulla responsabilità dei professionisti in ciascuno Stato Membro, nell'interesse di tutti gli attori del mercato.

In vista del recepimento, non vanno inoltre trascurate né la dimensione programmatica dei Considerando che precedono l'articolato normativo, né quanto disposto dall'art. 13 direttiva R2R, dove si prevede che gli Stati membri debbano adottare «almeno una misura volta a promuovere la riparazione», da leggersi insieme al Considerando 36 direttiva R2R, che divide tali misure tra quelle di carattere finanziario e quelle di carattere non finanziario. Nel contesto valoriale che ispira il Green Deal europeo, la *ratio* dell'intervento e le maglie larghe della norma da ultimo richiamata (art. 13 direttiva R2R) hanno infatti indotto ad ipotizzare che ciascuno Stato membro possa introdurre norme di recepimento che non ricalchino pedissequamente quelle europee, nella misura in cui – in conformità con gli obiettivi di sviluppo sostenibile – queste contribuiscano ad una più significativa riduzione dell'impatto ambientale del prodotto o della produzione. Tale lettura potrebbe stimolare l'avvio di una riflessione più ampia sulla possibilità di individuare un principio di "maggior tutela dell'ambiente", capace di giustificare eventuali scostamenti dalla normativa europea, ma richiederebbe preliminarmente di chiarire il significato da riconoscere all'attributo "divergenti" all'interno della legislazione dell'Unione.

ISSN 2239-8570

Per quanto attiene ai limiti soggettivi di applicazione delle nuove disposizioni, l'art. 1 direttiva R2R si allinea all'impostazione della normativa europea consumeristica dedicata al difetto di conformità e alla responsabilità del produttore, prevedendo che la Direttiva si applichi alla riparazione dei beni acquistati dai soli consumatori.

Dal punto di vista dell'ambito oggettivo di applicazione, va chiarito che, come disposto dagli artt. 1(2), 1(3) e 5(1) direttiva R2R, l'obbligo di riparazione del fabbricante introdotto dalla direttiva R2R trova applicazione:

- «in caso di difetto del bene che si verifica o si manifesta al di fuori della responsabilità del venditore ai sensi dell'art. 10 della direttiva (UE) 2019/771»; e
- solo con riferimento a quei prodotti per i quali requisiti di riparabilità siano specificati all'interno degli atti giuridici dell'Unione elencati nell'Allegato II della direttiva stessa.

Sotto il primo aspetto, si ricorda che ai sensi dell'art. 10(1) direttiva (UE) 2019/771, il venditore è responsabile nei confronti del consumatore di qualsiasi «difetto di conformità sussistente al momento della consegna del bene e che si manifesta entro 2 anni da tale momento», salve le disposizioni particolari per i beni con elementi digitali e la facoltà degli Stati membri di mantenere in vigore o introdurre termini più lunghi.

Sotto il secondo aspetto, la limitazione concerne prodotti già coperti da requisiti di riparabilità ai sensi del diritto dell'UE, che riguardano soprattutto gli elettrodomestici (lavatrici, asciugatrici, lavastoviglie, frigoriferi, televisori, aspirapolveri). L'elencazione di cui all'Allegato II della direttiva R2R è ovviamente suscettibile di essere modificata e ampliata, soprattutto via via che saranno introdotti e integrati i requisiti di *ecodesign* per altre tipologie di dispositivi e gruppi di prodotti tecnologici.

Legibus sic stantibus, tuttavia, l'obbligo di riparazione di cui all'art. 5 direttiva R2R e il correlato obbligo informativo *ex* art. 6 della medesima Direttiva sussiste solo per un limitato gruppo di beni attualmente individuabili tramite il detto Allegato II. L'obbligo, dunque, non sussiste per altri prodotti (per esempio quelli tessili) la cui produzione e il cui smaltimento, allo stato attuale, hanno un forte impatto ambientale.

In termini generali, le disposizioni di cui agli artt. 4 - 7 direttiva R2R sono comuni a tutti i fornitori di servizi di riparazione. L'art. 4 della Direttiva è infatti dedicato al "modulo europeo di informazioni sulla riparazione" (di cui all'Allegato I della direttiva R2R), che – salva la facoltà di addebitare i costi per i servizi di diagnostica del difetto necessari – deve essere fornito gratuitamente al consumatore. Il modulo di informazioni deve essere rilasciato su un supporto durevole entro un periodo di tempo ragionevole dalla richiesta del consumatore, e in ogni caso prima che questi sia vincolato da un contratto per la fornitura di servizi di riparazione. La previsione sottolinea – come già accade all'interno della direttiva 2011/83/UE sui diritti dei consumatori, e in armonia con la *ratio* della direttiva 2005/29/CE sulle pratiche commerciali sleali tra imprese e consumatori – l'importanza che le informazioni fornite al consumatore siano accurate, chiare e comprensibili, così da consentire al consumatore di comparare le offerte sul mercato e di compiere una scelta consapevole e

ISSN 2239-8570

ponderata. La trasparenza informativa, nel caso di specie, è funzionale all'agevole individuazione, *inter alia*, dell'identità del riparatore e dei suoi recapiti, del bene da riparare, della natura del difetto e del tipo di riparazione proposta; del prezzo (o delle relative modalità di calcolo) e dei tempi della riparazione, nonché dell'eventuale disponibilità di beni sostitutivi.

Gli effetti della trasmissione del modulo europeo al consumatore, tuttavia, non paiono esaurirsi sul piano della *compliance* informativa. Il disposto dell'art. 4(5) direttiva R2R consente di ipotizzare che la consegna del modulo produca effetti procedimentali sottratti alla disponibilità del riparatore. La norma stabilisce che il riparatore non possa modificare le condizioni di riparazione specificate nel modulo europeo di informazioni sulla riparazione per almeno 30 giorni (ovvero per il più esteso termine eventualmente indicato). Prevede inoltre che la notifica dell'accettazione del consumatore entro il periodo di validità del modulo impegni il riparatore ad eseguire il servizio di riparazione a tali condizioni. Pertanto, pare che la previsione non si limiti ad elevare le condizioni di riparazione a parte integrante del contratto concluso: una formulazione siffatta induce a chiedersi se, all'atto del recepimento, il nostro legislatore sceglierà di riconoscere *expressis verbis* alla trasmissione del modulo europeo di informazione gli effetti di una proposta irrevocabile *ex* art. 1329 c.c.

Anche l'art. 6 direttiva R2R coinvolge il profilo informativo, demandando agli Stati membri il compito di imporre ai soggetti obbligati alla riparazione (*ex* art. 5(3) direttiva R2R: il fabbricante o, qualora questi sia stabilito al di fuori dell'Unione, il suo rappresentante autorizzato e, in subordine, l'importatore o il distributore) di rendere gratuitamente disponibili e facilmente fruibili le informazioni sui servizi di riparazione, almeno per durata dell'obbligo di riparazione.

Secondo l'art. 5 direttiva R2R, il fabbricante – tenuto *ex* art. 6 della medesima Direttiva ad informare il consumatore del diritto alla riparazione – è obbligato ad effettuare gli interventi per riparare il bene su richiesta del consumatore, salvo che questi siano impossibili da un punto di vista tecnico o giuridico (Considerando 24).

In assenza di un riferimento al criterio della proporzionalità di tenore analogo a quello contenuto nell'art. 10(2) della direttiva (UE) 2019/771, che limita la libertà di scelta del consumatore tra il rimedio della sostituzione e quello della riparazione quando la scelta imponga al venditore costi sproporzionati rispetto all'alternativa, il fabbricante non dovrebbe poter rifiutare la riparazione per motivi esclusivamente economici. La differenza sembra doversi al fatto che per la riparazione prevista dalla direttiva R2R può essere richiesto al consumatore un "prezzo ragionevole" (art. 5(2)(a) direttiva R2R), mentre la riparazione come al rimedio al difetto di conformità prevista dalla direttiva (UE) 2019/771 è gratuita (art. 14(1)(a) direttiva (UE) 2019/771). Ciononostante, la circostanza che, a fronte dell'impossibilità della riparazione il fabbricante possa offrire al consumatore un bene ricondizionato induce a ritenere che la facoltà riconosciuta al fabbricante sia in ultima analisi anche funzionale ad agevolare la sostituzione in tutti i casi in cui gli interventi di riparazione siano eccessivamente gravosi. Del resto, il *gap* informativo e tecnico che

ISSN 2239-8570

caratterizza la posizione del consumatore, difficilmente potrebbe consentire di contestare l'asserita impossibilità della riparazione o la ragionevolezza del prezzo richiesto per la riparazione. Riletta in questi termini, l'obbligazione del fabbricante potrebbe configurarsi, sostanzialmente, come facoltativa.

Da un punto di vista operativo, la riparazione potrà essere subappaltata dal soggetto obbligato, che continuerà ad essere però responsabile della riparazione anche nel caso in cui incarichi terzi dell'esecuzione materiale dell'intervento.

Le previsioni che vietano ai fabbricanti di rifiutare la riparazione per il solo fatto che siano già stati eseguiti tentativi di riparazione precedenti e quelle che non consentono di impedire l'utilizzo di ricambi di seconda mano o compatibili (purché conformi ai requisiti previsti dal diritto dell'Unione o nazionale), stimolano la concorrenza nel mercato della riparazione e l'interoperabilità dei componenti in un contesto nel quale ai consumatori è assicurato il diritto di rivolgersi a qualsiasi riparatore loro gradito (art. 5(8) direttiva R2R).

Relativamente a questa linea di politica legislativa, può ricordarsi che l'apertura del mercato dei servizi di riparazione e post-vendita costituisce una delle *rationes* anche della disciplina del Capo II del Data Act (il Regolamento (UE) 2023/2854) sulla condivisione dei dati generati dall'uso dei prodotti connessi e dei servizi correlati (su cui v., in questa Rubrica, notizia n. 1 del numero 4/2023 [2023/4(1)SO]), come dichiarato nel Considerando 32 del Data Act.

Venendo ora a commentare il disposto del paragrafo 2 dell'art. 5 direttiva R2R, può osservarsi, in via generale, come il criterio della ragionevolezza appaia ispirare le condizioni di riparazione per quanto riguarda tempistiche, costi diretti e costi indiretti eventualmente collegati a beni sostitutivi. Infatti, l'art. 5(2) direttiva R2R non regola nel dettaglio il contenuto dell'obbligo di riparazione, ma rimette alle dinamiche di mercato l'individuazione di parametri indicativi e ragionevoli per tempi e costi della riparazione, in particolare disponendo che:

a) la riparazione è eseguita a titolo gratuito o a un prezzo ragionevole;

b) la riparazione è eseguita entro un periodo di tempo ragionevole dal momento in cui il fabbricante prende fisicamente possesso del bene, riceve il bene o ottiene l'accesso al bene da parte del consumatore;

c) il fabbricante può fornire in prestito al consumatore un bene sostitutivo, a titolo gratuito o a un costo ragionevole, per la durata della riparazione; e

d) nei casi in cui la riparazione è impossibile, il fabbricante può offrire al consumatore un bene ricondizionato.

La direttiva R2R ulteriormente mira a rendere liberamente accessibili ai consumatori tramite appositi portali *online* le informazioni sui suddetti elementi per favorire dinamiche di mercato aperte e concorrenziali. Viene in evidenza in proposito l'art. 7 direttiva R2R che aspira a realizzare sotto questo aspetto una connessione tra la transizione ecologica e quella digitale. La norma istituisce infatti una «piattaforma online europea per la riparazione», per consentire ai consumatori di trovare riparatori e, se del

ISSN 2239-8570

caso, venditori di beni ricondizionati, acquirenti di beni difettosi a fini di ricondizionamento o iniziative di riparazione di tipo partecipativo. È inoltre previsto che la piattaforma online europea sia costituita da sezioni nazionali predisposte dagli Stati membri e accomunate da un'unica interfaccia.

Deve tuttavia segnalarsi che l'impiego di risorse pubbliche, necessarie a tal fine, ha indotto a criticare la razionalità di una scelta siffatta alla luce del rapporto costi-benefici, soprattutto in ragione del fatto che la maggior parte dei riparatori e di venditori di prodotti ricondizionati opera già *online* ed è indicizzata su comuni motori di ricerca.

Nella prospettiva di rafforzare i diritti dei consumatori e di favorire altresì una produzione sostenibile, si vieta al fabbricante di inserire clausole contrattuali volte a limitare la possibilità di riparazione dei beni contemplati dagli atti giuridici dell'Unione di cui all'allegato II (art. 5(6) direttiva R2R) e si stabilisce l'inefficacia di qualsiasi pattuizione che, a danno del consumatore, escluda l'applicazione delle disposizioni nazionali di recepimento della direttiva R2R o vi deroghi *in peius* (art. 14 direttiva R2R). Inoltre, anche al fine di stimolare il miglioramento delle caratteristiche di riparabilità dei beni, si vietano tecnologie che impediscano la riparazione dei beni identificabili mediante gli atti dell'Unione di cui all'allegato II. Il divieto trova espresso temperamento ove l'applicazione della tecnologia *software* o *hardware* che ha per effetto la limitazione o l'esclusione della riparabilità del bene sia una soluzione ragionevole per bilanciare gli interessi particolari coinvolti nella fattispecie concreta (ad esempio, quello di protezione della proprietà intellettuale).

Il quadro muta radicalmente per la riparazione e la riparabilità di quei beni che non rientrano tra quelli menzionati negli atti dell'Unione elencati nell'Allegato II della direttiva R2R.

Per essi, la riparazione è una semplice facoltà, e i fabbricanti possono evitare alla radice di predisporre e fornire lo stesso modulo informativo di cui all'art. 4 direttiva R2R qualora non intendano offrire la riparazione. In questi casi, i riparatori non sono perciò obbligati a erogare servizi di riparazione alle condizioni di cui all'art. 5 direttiva R2R, né in via generale ad effettuare interventi sul bene venduto.

Oltre ad introdurre un obbligo di riparazione che opera al di fuori dalle ipotesi di responsabilità del venditore per eventuali difetti di conformità, la direttiva R2R interviene altresì direttamente sulla direttiva (UE) 2019/771 apportandovi alcune modifiche, come disposto dall'art. 16 direttiva R2R, che le elenca in quattro punti.

In particolare, per effetto del punto 1) dell'art. 16 direttiva R2R, i requisiti oggettivi di conformità di cui all'art. 7(1)(d) direttiva (UE) 2019/771 sono integrati con le qualità e le caratteristiche di «riparabilità» (laddove nel testo emendato si parlava solo di quelle di «durabilità, funzionalità, compatibilità e sicurezza») «normali in un bene del medesimo tipo e che il consumatore può ragionevolmente aspettarsi, tenuto conto della natura del bene e delle dichiarazioni pubbliche fatte dal o per conto del venditore, o da altre persone nell'ambito dei passaggi precedenti della catena di transazioni commerciali».

ISSN 2239-8570

Il punto 2) dell'art. 16 direttiva R2R dispone tre modifiche all'art. 10 direttiva (UE) 2019/771 rubricato *Responsabilità del venditore*. Si tratta di tre modifiche collegate una all'altra. La prima consiste nell'introduzione del comma 2-bis dell'art. 10 direttiva (UE) 2019/771, con la previsione che se, ai sensi dell'articolo 13(2) direttiva (UE) 2019/771, si effettua una riparazione come rimedio per rendere conformi i beni, il periodo di responsabilità è esteso una volta di dodici mesi. La seconda e la terza modifica dell'art. 10 direttiva (UE) 2019/771 consistono nella sostituzione del comma 3 e nell'introduzione del comma 5-bis. Il comma 3 è sostituito nel senso di prevedere che ciascuno Stato membro può mantenere o introdurre termini di responsabilità del venditore nei confronti del consumatore per difetti di conformità più lunghi rispetto a quelli minimi di due anni dalla consegna del bene o del più esteso periodo di tempo durante il quale il contenuto o il servizio digitale sono forniti al consumatore. Il nuovo comma 5-bis opera insieme alle altre nuove disposizioni. Il combinato disposto che ne risulta consiste nella previsione secondo cui gli Stati membri che non prevedono termini fissi per la responsabilità del venditore per il difetto di conformità del bene consegnato, o prevedono solo un termine di prescrizione applicabile ai rimedi esperibili a fronte della difformità, potranno derogare all'estensione di responsabilità del venditore di ulteriori dodici mesi, prevista dal nuovo comma 2-bis per il caso in cui sia eseguito un intervento di riparazione, purché ciò assicuri in ogni caso la copertura di un periodo di prescrizione minimo di 3 anni.

Sul versante rimediale, le modifiche agli artt. 13 e 14 direttiva (UE) 2019/771 - disposte ai punti 3) e 4) dell'art. 16 direttiva R2R - impongono al venditore di informare il consumatore circa il diritto di scegliere tra riparazione e sostituzione e in merito all'estensione del periodo di responsabilità del venditore nel caso il bene venga riparato, nonché a chiarire le condizioni che devono essere assicurate nell'adempimento dell'obbligo di riparare o sostituire il bene da parte del venditore, prevedendo inoltre che, nel corso della riparazione, il venditore può fornire gratuitamente al consumatore un bene sostitutivo, compreso un bene ricondizionato, in prestito, e che, su esplicita richiesta del consumatore, il venditore può fornire un bene ricondizionato per adempiere al suo obbligo di sostituire il bene.

Pertanto, i beni ricondizionati, nel disegno dei rimedi per il difetto di conformità della disciplina della direttiva (UE) 2019/771, dopo le modifiche introdotte dalla direttiva R2R, rilevano sotto un duplice profilo: quello dei beni sostitutivi temporanei che il venditore può mettere a disposizione del consumatore durante l'esecuzione dell'intervento di riparazione; ovvero – a richiesta del consumatore – quello del bene sostitutivo vero e proprio, di cui il consumatore acquisterà la titolarità dopo aver restituito il bene non conforme al venditore.

All'interno del perimetro di responsabilità del venditore per la non conformità del bene consegnato, ai sensi della disciplina della direttiva (UE) 2019/771, dunque, sebbene la riparazione ivi prevista sia stata incoraggiata sul piano formale attraverso le predette modifiche apportate dalla direttiva R2R (in particolare: attraverso la diffusione di maggiori informazioni ad

ISSN 2239-8570

essa relative, l'estensione del periodo di responsabilità del venditore e la previsione relativa a possibili beni sostitutivi durante l'esecuzione dell'intervento), il venditore potrà continuare a rifiutarsi - ex art. 13(3) direttiva (UE) 2019/771 - di rendere conformi i beni non solo qualora la riparazione sia impossibile, ma anche quando i costi che dovrebbe sostenere per la stessa siano "sproporzionati". In questa dimensione, è marginale l'incentivo offerto alla produzione di beni facilmente riparabili da parte delle modifiche alla direttiva (UE) 2019/771, perché saranno la sensibilità ecologica dei consumatori e la loro propensione ad accettare prodotti riparati e/o ricondizionati a determinare l'effettivo impatto della vendita di beni di consumo sulla transizione ecologica.

Infine, dal punto di vista dell'*enforcement*, l'art. 17 della direttiva R2R modifica la direttiva (UE) 2020/1828 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, prevedendo che l'Allegato di tale direttiva menzioni anche la direttiva R2R.

A tal proposito, nel Considerando 39 della direttiva R2R, si specifica che le disposizioni di applicazione di cui alla medesima direttiva lasciano impregiudicata la direttiva (UE) 2020/1828.

Nella consapevolezza che l'effettività dei diritti riconosciuti ai consumatori non può prescindere da adeguati meccanismi di tutela, la direttiva R2R demanda perciò agli Stati membri il compito di garantire che esistano mezzi adeguati ed efficaci per assicurare il rispetto delle nuove previsioni, anche attraverso interventi che legittimino enti pubblici o loro rappresentanti, organizzazioni aventi un legittimo interesse a proteggere i consumatori o l'ambiente e associazioni di categoria ad adire le autorità competenti al fine di assicurare l'applicazione delle disposizioni nazionali di recepimento.

FRANCESCA BERTELLI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401799

2024/2(10)ES

10. Entrato in vigore il regolamento (UE, Euratom) 2023/2841 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione

Il 7 gennaio 2024 è entrato in vigore il regolamento (UE, Euratom) 2023/2841 (da ora anche il "**Regolamento**") del 13 dicembre 2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione Europea (da ora anche i "**Soggetti dell'Unione**").

Il Regolamento chiarisce fin da principio che le minacce informatiche ai Soggetti dell'Unione evolvono costantemente aumentando di complessità (Considerando n. 1).

ISSN 2239-8570

Il Regolamento si applica a tutti i Soggetti dell'Unione e si propone di raggiungere un livello comune elevato di sicurezza cibernetica. Gli obiettivi della disciplina in commento, dunque, sono: i) la definizione da parte di ciascuno di suddetti Soggetti "*di un quadro interno di gestione, di governance e di controllo dei rischi per la cibersicurezza*"; ii) la gestione, segnalazione e condivisione tra i Soggetti delle informazioni attinenti ai rischi per la cibersicurezza, nonché iii) la creazione di un comitato interistituzionale per la cibersicurezza (art. 1). Il successivo art. 3 contiene una serie di definizioni tra cui spicca quella di Soggetti dell'Unione.

Per quanto riguarda l'obiettivo sub i), il Regolamento prevede che ogni Soggetto dell'Unione istituisca un "*quadro interno di gestione, di governance e di controllo dei rischi*" cibernetici riguardante tutte le sue strumentazioni tecnologiche, anche se non connesse a internet, secondo un approccio multirischio. Tale quadro deve stabilire le politiche, i ruoli e le responsabilità dei soggetti coinvolti in materia di cibersicurezza. Al fine di assicurare la sua massima efficacia ed efficienza, il suddetto quadro deve essere riesaminato periodicamente e, comunque, almeno ogni quattro anni (art. 6). Inoltre, almeno ogni due anni, ciascuno Soggetto dell'Unione deve valutare la maturità dei propri strumenti di cibersicurezza (art. 7).

Per quanto riguarda l'obiettivo sub ii), l'art. 8 del Regolamento prevede che "*ogni soggetto dell'Unione adotta misure tecniche, operative e organizzative adeguate e proporzionate, sotto la vigilanza del livello di dirigenza più elevato, per gestire i rischi per la cibersicurezza individuati nell'ambito del quadro e per prevenire o ridurre al minimo l'impatto degli incidenti*". In particolare, l'art. 8, par. 2 specifica il contenuto delle suddette misure.

Tali misure di gestione del rischio compongono i piani per la cibersicurezza. Ai sensi dell'art. 9, un piano "*è volto ad aumentare la cibersicurezza complessiva del soggetto dell'Unione e contribuisce così al rafforzamento di un livello comune elevato di cibersicurezza all'interno dei soggetti dell'Unione*". Ogni Soggetto dell'Unione deve adottare senza ritardo, e comunque entro l'8 gennaio 2026, il proprio piano in cui occorre dedicare particolare attenzione agli incidenti significativi.

Per quanto riguarda l'obiettivo sub iii), l'art. 10 del Regolamento istituisce un comitato interistituzionale per la cibersicurezza (c.d. "**Interinstitutional Cybersecurity Board**" o "**IICB**") a cui è affidata l'attuazione degli obiettivi del Regolamento (art. 11). Tale organo deve creare un piano di gestione delle crisi informatiche che contenga gli elementi stabiliti dall'art. 23, par. 1 del Regolamento. Al fine di perseguire i propri compiti, l'IICB può chiedere informazioni e documenti ai Soggetti dell'Unione e laddove ravvisi che questi non rispettino il Regolamento, tra l'altro, può: i) trasmettere al Soggetto un parere motivato "*sulle carenze osservate nell'attuazione del ... regolamento*"; ii) fornire indirizzi al Soggetto dell'Unione "*affinché il suo quadro, le sue misure di gestione del rischio di cibersicurezza, il suo piano di cibersicurezza e le sue relazioni si conformino al presente regolamento entro un termine specificato*"; iii) emanare un avvertimento invitando il Soggetto a rimediare alle violazioni riscontrate entro un termine prestabilito e, laddove questo non provveda,

ISSN 2239-8570

inviargli una "*notifica motivata*"; iv) "*se del caso, informare la Corte dei conti … della presunta inosservanza*"; v) "*emanare una raccomandazione affinché tutti gli Stati membri e i soggetti dell'Unione attuino una sospensione temporanea dei flussi di dati verso il soggetto dell'Unione interessato*" (art. 12).

L'art. 13 è dedicato alla squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE (c.d. "**Computer Emergency Response Team for the EU institutions, bodies and agencies**" o "**CERT-UE**") a cui è affidato il compito di supportare i Soggetti dell'UE al fine di prevenire, rilevare e gestire gli incidenti informatici. Nello specifico l'art. 13, par. 6 dettaglia quali servizi possa prestare il CERT-UE. Quest'ultimo coopera con i suoi omologhi nazionali per assicurare l'attuazione del Regolamento. A tal fine, può adottare nei confronti dei Soggetti dell'UE: a) inviti descriventi le misure di sicurezza da adottare urgentemente; b) indirizzi e raccomandazioni che individuano i miglioramenti da apportare ai sistemi di gestione dei rischi e le modalità di valutazione degli stessi (art. 14).

L'art. 21, par. 1 stabilisce che un incidente sia significativo se:

- "*ha causato o è in grado di causare una grave perturbazione operativa per il funzionamento del soggetto dell'Unione interessato o perdite finanziarie per lo stesso*";
- "*ha interessato o è in grado di interessare altre persone fisiche o giuridiche causando considerevoli danni materiali o immateriali*".

In tal caso, ai sensi dell'art. 21, par. 2, i Soggetti dell'UE informano i loro omologhi nazionali e inviano:

- senza ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente, al CERT-UE un preallarme che può anche indicare se l'incidente si sospetta sia il frutto di atti illegittimi, possa avere rilevanza transfrontaliera o interessare diversi soggetti;
- senza ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente, una notifica al CERT-UE di aggiornamento delle informazioni già fornite che fornisca anche una valutazione iniziale dell'incidente, comprensiva della sua gravità e del suo impatto;
- una relazione finale sull'incidente che riepiloghi dettagliatamente l'incidente, la sua causa, l'impatto negativo, le misure di attenuazione, la rilevanza transfrontaliera ovvero se interessa diversi soggetti.

Al CERT-UE spetta il coordinamento tra i Soggetti dell'UE della gestione degli incidenti gravi.

L'art. 21, par. 5, infine, prevede che i Soggetti dell'UE informino, senza ritardo, gli utenti dei loro sistemi informatici interessati dell'incidente significativo, delle sue cause e delle misure di mitigazione adottate.

EMANUELE STABILE

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ%3AL_202302841

ISSN 2239-8570

2024/2(11)RA

11. Le ultime designazioni di VLOPs da parte della Commissione europea (per un totale di 24): Shein e Temu

Con decisioni emesse il 26 aprile e il 31 maggio 2024, la Commissione ha designato quali piattaforme *online* di dimensioni molto grandi ("**VLOPs**") i servizi di *fashion online retail* Shein e Temu, ai fini di quanto previsto dal regolamento (UE) 2022/2065 (Regolamento sui servizi digitali o *Digital Services Act* o "**DSA**"), (per la designazione del primo gruppo di VLOPs, v. in questa Rubrica la notizia n. 5 nel numero 2/2023 [2023/2(5)RA], e per la designazione di *Pornhub*, *Stripchat* e *XVideos* del 20 dicembre 2023, v. in questa Rubrica la notizia n. 12 nel numero 4/2023 [2023/4(12)RA]).

La designazione quali VLOPs di Shein e Temu è il risultato di indagini, portate avanti dalla Commissione, dalle quali è emerso che le due piattaforme *online* di *fashion retail* superano la soglia dei 45 milioni di utenti medi mensili nell'UE prevista all'art. 33, par. 1 del DSA.

Le due piattaforme dovranno ora impegnarsi a rispettare, in particolare, gli "*obblighi supplementari*" stabiliti dalla Sezione 5 del Capo III del DSA, in cui si prevede, tra l'altro, che:

- i fornitori di VLOPs "*individuano, analizzano e valutano con diligenza gli eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi*" (art. 34, par. 1 del DSA);
- una volta individuati i rischi sistemici, i "*fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi adottano misure di attenuazione ragionevoli, proporzionate ed efficaci* [di tali rischi], *prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali*" (art. 35, par. 1 del DSA);
- essi siano sottoposti "*a proprie spese e almeno una volta all'anno, a revisioni indipendenti volti a valutare la conformità: a) agli obblighi stabiliti al Capo III; b) agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 e dei protocolli di crisi di cui all'articolo 48*" (art. 37, par. 1 del DSA); tali revisioni devono essere effettuate da organizzazioni "*indipendenti e in assenza di conflitti di interessi*", "*dotate di comprovata esperienza nel settore della gestione dei rischi, di competenze e di capacità tecniche*" e di "*comprovata obiettività e deontologia professionale*" (art. 37, par. 3 del DSA). Ove la revisione risulti non positiva, i fornitori di VLOPs "*tengono debitamente conto delle raccomandazioni operative ad essi rivolte al fine di adottare le misure necessarie per attuarle*" (art. 37, par. 6 del DSA);
- i fornitori di VLOPs devono assicurare "*almeno un'opzione per ciascuno dei loro sistemi di raccomandazione, non basata sulla*

ISSN 2239-8570

profilazione come definita nell'articolo 4, punto 4), del regolamento (UE) 2016/679" (art. 38 del DSA);

- tali soggetti "*compilano e rendono accessibile al pubblico in una specifica sezione della loro interfaccia online, mediante uno strumento consultabile e affidabile che consente ricerche attraverso molteplici criteri e attraverso le interfacce di programmazione delle applicazioni, un registro contenente* [talune] *informazioni* [relative alla pubblicità effettuata], *per l'intero periodo durante il quale presentano pubblicità e fino a un anno dopo la data dell'ultima presentazione dell'annuncio pubblicitario sulle loro interfacce online*" (art. 39 del DSA);
- i fornitori di VLOPs "*forniscono al coordinatore dei servizi digitali del luogo di stabilimento o alla Commissione, su loro richiesta motivata ed entro un termine ragionevole specificato in detta richiesta, l'accesso ai dati necessari per monitorare e valutare la conformità al presente regolamento*", al fine di adottare eventuali provvedimenti a ciò finalizzati (art. 40, par. 1 del DSA);
- tali soggetti devono istituire "*una funzione di controllo della conformità indipendente dalle loro funzioni operative*" volta a: "*a) collaborare con il coordinatore dei servizi digitali del luogo di stabilimento e con la Commissione ai fini del presente regolamento; b) assicurare che tutti i rischi di cui all'articolo 34 siano identificati e adeguatamente segnalati e che siano adottate misure di attenuazione dei rischi ragionevoli, proporzionate ed efficaci a norma dell'articolo 35; c) organizzare e sovrintendere alle attività del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi relative alle revisioni indipendenti a norma dell'articolo 37; d) informare e consigliare i dirigenti e i dipendenti del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi in merito ai pertinenti obblighi a norma del presente regolamento; e) monitorare la conformità del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi agli obblighi derivanti dal presente regolamento; f) se del caso, monitorare la conformità del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 o dei protocolli di crisi di cui all'articolo 48*" (art. 41, par. 1 e 3 del DSA);
- la "*Commissione addebita ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi un contributo annuale per le attività di vigilanza al momento della loro designazione a norma dell'articolo 33*" (art. 43, par. 1 del DSA).

I nuovi VLOPs dovranno adeguarsi alle disposizioni poc'anzi illustrate entro 4 (quattro) mesi dalla notifica della decisione, al fine di garantire una moderazione dei contenuti più diligente, una migliore protezione dei minori

ISSN 2239-8570

e degli altri soggetti particolarmente vulnerabili, nonché una maggiore trasparenza dei servizi offerti sul *web*.

Con queste decisioni, la Commissione è così giunta a designare ben 24 VLOPs ai sensi del DSA.

RICCARDO ALFONSI

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2326
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3047

2024/2(12)RA

12. La risoluzione del Parlamento europeo del 12.12.2023 sulla progettazione dei servizi online che creano dipendenza e sulla tutela dei consumatori

Il 12 dicembre 2023, il Parlamento europeo (il "**Parlamento**") ha adottato una Risoluzione sulla progettazione di servizi *online* che creano dipendenza e sulla tutela dei consumatori nel mercato unico dell'Unione europea (la "**Risoluzione**").

La Risoluzione si fonda sul presupposto – ampiamente illustrato nei suoi Considerando – che "*determinate imprese* […] *utilizzano la progettazione e le funzionalità dei sistemi per sfruttare le vulnerabilità degli utenti e dei consumatori al fine di catturare la loro attenzione e aumentare la quantità di tempo che trascorrono sulle piattaforme digitali*" e, per tale via, "*massimizzare*" il "*denaro speso dagli utenti, la quantità di dati raccolti, nonché l'attività, le interazioni, la produzione di contenuti, lo sviluppo della rete e la condivisione di dati*" (Considerando A).

Secondo numerosi studi, tale "*progettazione manipolativa* […] *dei servizi online*" comporta "*rischi e danni legati al comportamento*" (Considerando A; ma v. anche Considerando C, D e F), soprattutto quando i servizi sono destinati ad essere utilizzati dai "*giovani tra i 16 e i 24 anni*", i quali passano molto tempo su *internet* e dinnanzi agli *smartphone* (Considerando C).

A ciò, il Parlamento aggiunge una considerazione di carattere generale, e cioè che la "*progettazione che crea dipendenza può avere un impatto negativo su tutti, non soltanto sugli individui che manifestano un uso problematico*": si pensi ai "*consumatori online che si trovano sempre più spesso a un sovraccarico di informazioni e a molteplici stimoli sensoriali*" che limitano le loro capacità cognitive (Considerando G). D'altronde, accade quotidianamente di imbattersi in "*interfacce di alcuni servizi digitali* [che] *sfruttano vulnerabilità psicologiche simili a quelle che portano alla dipendenza dal gioco d'azzardo*", con l'obiettivo di alimentare "*intenzionalmente le vulnerabilità dei consumatori*" (Considerando I) e, in particolare, "*i bisogni psicologici,* […] *i desideri dei consumatori* […] *e la perdita di autocontrollo*", dovuta "*a un'impennata di dopamina*" e a "*reazioni chimiche nel cervello*" (Considerando J).

ISSN 2239-8570

Tutto ciò si traduce in uno "***stato generale di vulnerabilità digitale***" (Considerando K) causato da "*pratiche che creano dipendenza*", tra cui rientrano – ad esempio – "*lo scorrimento infinito, il caricamento delle pagine* […], *la riproduzione automatica dei video incessante, i consigli personalizzati*" (Considerando L), "*taluni sistemi di raccomandazione*" (Considerando M) che difettano della necessaria trasparenza (Considerando N).

Il Parlamento europeo non dimentica che gli artt. 25, 27, 28 e 48 del regolamento (UE) 2022/2065 sui servizi digitali (il "**DSA**") prevedono il divieto di progettare interfacce *online* con caratteristiche ingannevoli o manipolative, obblighi di trasparenza e di scelta per i sistemi di raccomandazione e di profilazione, misure a protezione dei minori, nonché disposizioni contro i c.d. *dark patterns* (Considerando P). Tuttavia, le disposizioni del DSA "*non si applicano a tutti i servizi online, ma soltanto alle piattaforme online, escludendo pertanto servizi problematici e cruciali come i giochi online*" (Considerando P).

Ancora, con riguardo ai profili oggetto della Risoluzione occorrerà senz'altro tenere conto della "*legge sull'intelligenza artificiale*" ("**AI Act**"), la quale si pone l'obiettivo di "*vietare i sistemi di intelligenza artificiale che impiegano funzioni subliminali*"; essa, però, "*si limita ai sistemi che sono intenzionalmente manipolativi o che impiegano tecniche ingannevoli*" (Considerando P).

Alla luce di tutto ciò, il Parlamento europeo invita "*la Commissione a rivedere* […] *concetti e definizioni del diritto in materia di tutela dei consumatori, quali le definizioni di «consumatore», «consumatore vulnerabile» e «professionista», per proteggere i consumatori dai danni e rispondere alle sfide poste dall'era dei dati*" (punto 1; ma v. anche punto 5), dando in ogni caso "*una risposta normativa completa*" alla "*dipendenza digitale*" e alle "*tecnologie persuasive*" (punto 2), che non sono adeguatamente e sufficientemente trattate nella legislazione europea vigente (punto 4).

Tra queste risposte normative potrebbe esservi quella di "*vietare le pratiche più dannose*", inserendole nell'allegato I della direttiva sulle pratiche commerciali sleali (Direttiva 2005/29/CE), tenuto conto che – ad esempio – i c.d. *dark patterns* dovrebbero già reputarsi tali (e cioè, una pratica commerciale sleale) alla luce di quanto previsto dagli artt. 5 e seguenti della direttiva in parola (punto 6). Ciò, alla luce del fatto che le imprese hanno "*l'obbligo di sviluppare prodotti e servizi digitali etici, che siano privi di percorsi oscuri e di progettazione ingannevole o che crea dipendenza*", al fine di mantenere "*un'adeguata diligenza professionale*" (punto 8).

Sempre a proposito della Direttiva 2005/29/CE, il Parlamento poi: *(i)* invita "*la Commissione a prendere in considerazione l'inversione dell'onere della prova per le pratiche che, secondo quanto supposto o riscontrato dalla Commissione o dalle autorità nazionali, creano dipendenza*" (punto 8) (sui precedenti e più recenti studi della Commissione europea in materia, cfr.: la divulgazione del 30.1.2023 dei risultati dell'indagine a tappeto della Commissione europea e della rete CPC sulle pratiche di manipolazione

ISSN 2239-8570

online, su cui v., in questa Rubrica, notizia n. 10 nel numero 1/2023 [2023/1(10)RA]; nonché la comunicazione 2021/C 526/01 sugli orientamenti e sull'interpretazione della direttiva 2005/29/CE sulle pratiche commerciali scorrette); *(ii)* dichiara di reputare "*che la definizione di «decisione di natura commerciale» contenuta nella direttiva sulle pratiche commerciali sleali includa l'utilizzo continuo del servizio (ad esempio scorrere un feed), la visualizzazione di contenuti pubblicitari o fare click su un link*" (punto 8) (allo stesso modo nella predetta comunicazione 2021/C 526/01 della Commissione europea sugli orientamenti e sull'interpretazione della direttiva 2005/29/CE sulle pratiche commerciali scorrette, dove si legge: «*pratiche commerciali come quella di catturare l'attenzione del consumatore, che sfocia nell'adozione di decisioni di natura commerciale quali continuare a utilizzare il servizio (per es. scorrendo un* feed*), visualizzare un contenuto pubblicitario o cliccare su un* link» par. 4.2.7, p. 102).

Auspicando una "*progettazione etica dei servizi online*", il Parlamento chiede perciò "*che, nel suo riesame della vigente legislazione dell'UE in materia di progettazione che crea dipendenza, la Commissione proponga un diritto digitale a non essere disturbati*" (punto 10), anche attraverso la creazione di "*un elenco di buone pratiche in materia di funzioni di progettazione che non creino dipendenza o che non siano manipolative e che garantiscano agli utenti il pieno controllo e la possibilità di agire online in modo consapevole e informato, senza dover affrontare un sovraccarico di informazioni o essere influenzati a livello subconscio*" (punto 11).

RICCARDO ALFONSI

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_IT.html

2024/2(13)AN

13. Il report della task force dell'EDPB su ChatGPT del 23.5.2024

Il 23 maggio 2024 il Comitato europeo per la protezione dei dati (**EDPB**) - che riunisce le Autorità nazionali per la protezione dei dati personali dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati - ha pubblicato un report sui lavori svolti dalla *task force* relativa a ChatGPT (il **Report**).

Diverse Autorità nazionali di controllo (le **Autorità**) hanno intrapreso delle indagini su ChatGPT e sul rispetto da parte del sistema delle disposizioni del Regolamento (UE) 2016/679 (**GDPR**). Tuttavia, poiché OpenAI OpCp LLC (**OpenAI**) - titolare del trattamento dei dati del modello ChatGPT -non ha avuto una sede in Europa fino al 15 febbraio 2024, non è stato possibile applicare la procedura One-Stop-Shop (**OSS**), prevista dal medesimo GDPR. L'EDPB il 13 aprile 2023 ha quindi deciso di istituire una *task force* (**Chat GPT TF**) per promuovere la cooperazione e lo scambio di

ISSN 2239-8570

informazioni sulle eventuali azioni intraprese dalle Autorità relative al trattamento dei dati personali operato da ChatGPT, nonché il relativo coordinamento.

Nella riunione plenaria dell'EDPB del 16 gennaio 2024, è stato stabilito che ChatGPT TF dovesse in particolare:

(i) Facilitare lo scambio di informazioni tra le varie Autorità sulle attività svolte in relazione a ChatGPT;

(ii) Facilitare il coordinamento delle comunicazioni esterne da parte delle Autorità sulle suddette attività;

(iii) Identificare le principali questioni su cui l'adozione di un approccio comune tra le varie Autorità potesse rendersi necessario.

OpenAI ha successivamente aperto una sede nell'Unione Europea il 15 febbraio 2024, data a partire dalla quale si applica la procedura OSS. Le attività investigative svolte dalle diverse Autorità sino a quel momento continuano, tuttavia, ad essere coordinate dalla ChatGPT TF e il Report ne riassume i risultati.

Nell'introduzione, il Report evidenzia anzitutto come i titolari del trattamento dei dati nell'ambito dei *large language models* (**LLMs**) debbano garantire il pieno rispetto del GDPR, senza invocare ragioni di impossibilità tecnica quale esenzione dall'applicazione delle disposizioni normative. È evidente infatti che, per le caratteristiche di questi modelli, il tema della complessità tecnologica è quello più spinoso.

Il Report riporta le valutazioni effettuate in questo contesto, con riferimento a diverse condizioni previste dal GDPR:

(i) Liceità: rammentando che ciascun trattamento di dati personali deve essere basato su una delle condizioni previste dall'art. 6(1) e, in alcuni casi, art. 9(2) GDPR, il Report prende in considerazione le diverse fasi del trattamento dei dati personali:

a) Raccolta e preelaborazione dei dati e addestramento: in queste prime fasi i rischi per i diritti fondamentali e le libertà personali sembrano connessi soprattutto con il c.d. *web scraping*. Sotto questo profilo, OpenAI afferma di trattare i dati sulla base dell'art. 6 (1)(f) GDPR, che richiede il legittimo interesse del titolare, da bilanciare con i diritti e le libertà fondamentali dell'interessato, oltre all'obbligo di effettuare il trattamento nella misura minima, in relazione alla finalità del medesimo. In questo contesto è fondamentale l'adozione di misure di salvaguardia dei diritti degli interessati e -mentre le investigazioni sono ancora in corso- potrebbero essere adottate delle misure di natura tecnica, che definiscano criteri precisi e assicurino che determinate categorie di dati non siano raccolte o che determinate fonti (quali i profili pubblici di social media) siano esclusi dalla raccolta dati. Inoltre è essenziale che vengano adottate misure per cancellare o anonimizzare i dati personali che

ISSN 2239-8570

siano stati raccolti attraverso il *web scraping* prima della fase di addestramento

Con riferimento al trattamento delle categorie particolari di dati, perché il trattamento sia lecito, è necessaria la presenza di una delle eccezioni previste dall'art. 9(2) GDPR. In linea di principio, si potrebbe far riferimento all'art. 9(2)(e) GDPR (*i.e.* trattamento dei dati resi manifestamente pubblici dall'interessato). Non è, tuttavia, detto che la sola circostanza che i dati siano pubblici, significhi automaticamente che l'interessato abbia deliberatamente inteso renderli pubblici. Al fine di garantire la liceità del trattamento, occorrerebbe verificare, pertanto, la volontà dell'interessato sotto questo profilo.

Tenendo conto della tipologia di sistemi a cui appartiene ChatGPT, è evidente come non sia possibile effettuare questo esame caso per caso. Occorrerà, quindi, ricorrere alle misure di salvaguardia sopra menzionate con riferimento a tutti i dati sensibili. L'onere della prova dell'efficacia di tali misure incomberebbe su OpenAI quale titolare del trattamento.

b) Input (prompt), output e addestramento: tra i prompt devono essere ricompresi gli impulsi forniti dagli interessati che interagiscono con ChatGPT, così come i loro *feedback* alle risposte fornite dal sistema. OpenAI qualifica tutto questo come "contenuto" e dichiara espressamente di utilizzare tali informazioni per addestrare e migliorare il modello. In tale contesto l'art. 6 (1)(f) GDPR deve costituire la base legale del trattamento. Gli interessati, inoltre, dovranno essere chiaramente informati della circostanza che tale "contenuto" sarà utilizzato per l'addestramento del modello.

(i) Correttezza: il Report rileva come – in applicazione del principio di correttezza del trattamento di cui all'art. 5 (1)(a) GDPR- il titolare del trattamento non dovrà trasferire agli interessati la responsabilità dell'osservanza della normativa (ad esempio, attraverso condizioni generali che rendano gli interessati responsabili per i loro input nell'ambito delle interazioni con il LLM). Considerando che le interazioni degli interessati con ChatGPT costituiscono una parte importante degli input forniti al modello e possono essere condivise con chiunque lo utilizzi, OpenAI dovrà rimanere responsabile per l'osservanza del GDPR e non potrà eccepire, ad esempio, che l'input di determinati dati personali è proibito.

Le misure messe in atto da OpenAI per gestire questi aspetti sono ancora sotto esame.

(ii) Trasparenza e obblighi di informazione: nel caso di dati personali raccolti tramite *web scraping*, si dovrebbe, in linea di principio, applicare l'art. 14 GDPR con riferimento alle informazioni da fornire all'interessato. Considerando, tuttavia, l'importante quantità di dati raccolti e utilizzati, risulta praticamente impossibile fornire le informazioni richieste dalla norma. Si potrà, pertanto, applicare l'esenzione dell'art. 14 (5)

ISSN 2239-8570

(b) GDPR (*i.e.* impossibilità o sforzo sproporzionato nella trasmissione informazione agli interessati), ove tuttavia siano presenti le relative condizioni.

Diversamente, ove i dati personali siano raccolti attraverso l'interazione diretta con ChatGPT, si applicherà l'art. 13 GDPR.

(iii) Accuratezza: occorre distinguere tra dati di input e di output. I primi sono quelli raccolti tramite *web scraping*, nonché il "contenuto" fornito dagli interessati (es. i prompt). I dati di output comprendono quelli risultanti dalle interazioni con ChatGPT (es. i *feedback* forniti al modello).

Considerando che la finalità del trattamento non è quella di fornire informazioni corrette, ma l'addestramento di ChatGPT, l'attuale modello (considerata la natura probabilistica del sistema) può condurre a risultati "*biased"* o inventati. È pertanto fondamentale che – in linea con il principio di trasparenza di cui all'art. 5(1)(a) GDPR- siano fornite informazioni adeguate sul meccanismo di creazione di risultati probabilistici e sul limitato livello di affidabilità fornito dal titolare del trattamento, con indicazione espressa che il testo generato, per quanto sintatticamente corretto, potrebbe essere "*biased*" o inventato. Le misure attualmente poste in essere da OpenAI non appaiono sufficienti sotto il profilo dell'accuratezza.

(iv) Diritti degli interessati: OpenAI – nella sua *privacy policy* (versione europea)- fornisce un'informativa agli interessati sulle modalità di esercizio dei diritti garantiti dal GDPR. Alla luce della situazione particolarmente complessa in cui viene effettuato il trattamento dei dati e delle difficoltà oggettive di intervento da parte degli interessati, è obbligatorio che OpenAI continui a migliorare l'accesso di questi ultimo ai propri diritti, facilitandone l'esercizio. Ad esempio, attualmente viene suggerito agli utilizzatori del sistema di richiedere la cancellazione, anziché la rettifica dei dati, quando quest'ultima non è possibile per la complessità tecnica di ChatGPT.

Il richiamo alla complessità tecnica non è giustificato, tenendo conto che, in linea con l'art. 25 (1) GDPR, il titolare del trattamento deve, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, mettere in atto misure tecniche e organizzative adeguate a garantire i diritti degli interessati.

Il Report riporta in allegato il questionario utilizzato da diverse Autorità come base di partenza dei propri scambi con OpenAI. Si tratta di domande che, dopo un inquadramento generale del modello e delle modalità di trattamento dei dati realizzato, entrano più nello specifico in relazione alle diverse disposizioni del Regolamento, tenendo conto delle varie fasi del trattamento e delle misure adottate per assicurarne il rispetto.

Il quadro complessivo che emerge dal Report è quello di un'analisi che - sia pure preliminare rispetto alle attività ancora in corso da parte delle Autorità - evidenzia già diverse criticità relative al funzionamento di ChatGPT e alla difficoltà per la medesima di poter assicurare il rispetto delle prescrizioni del GDPR.

ISSN 2239-8570

ARIANNA NERI

https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

2024/2(14)BG

14. I Primi Orientamenti dell'EDPS del 3.6.2024 su IA generativa e dati personali per le istituzioni, gli organi, gli uffici e le agenzie dell'Unione europea.

Il 3 giugno 2024, il Garante europeo della protezione dei dati (**EDPS** o **Garante europeo**) ha pubblicato i "*First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*" (di seguito i **Primi Orientamenti** o il **Documento**), in qualità di autorità di controllo ai sensi del regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati (di seguito il **Regolamento** o **EUDPR**).

I Primi Orientamenti dichiaratamente forniscono indirizzi generali ed istruzioni pratiche, a supporto di istituzioni, organi e organismi dell'UE (singolarmente e collettivamente **IUE**) per la *compliance* ai requisiti di protezione dei dati previsti dall'EUDPR qualora le IUE utilizzino, a qualunque titolo, sistemi di intelligenza artificiale (**IA**) generativa.

Nelle premesse del Documento viene chiarito che essi non sono stati emessi dall'EDPS nell'esercizio delle prerogative conferitegli dall'AI Act (il Regolamento (UE) 2024/1689).

Viene inoltre chiarito che i Primi Orientamenti rappresentano solo il primo passo nella direzione di indicazioni sempre più specifiche in materia fornite da parte dell'EDPS, che terranno conto dell'evoluzione dei sistemi e delle tecnologie della IA generativa, del loro utilizzo da parte delle IUE e dei risultati delle attività di monitoraggio e sorveglianza del medesimo Garante europeo.

Se è vero che, in ragione dell'ambito di competenza dell'EDPS ai sensi dell'EUDPR, il Documento si rivolge direttamente alle istituzioni europee, tuttavia esso si presta a costituire un riferimento importante anche per le altre amministrazioni, nonché per gli operatori privati, rispetto all'implementazione di sistemi di IA generativa rispetto agli obblighi imposti dal Regolamento (UE) 679/2016 (**GDPR**), in un'ottica di *accountability*.

Proprio in un'ottica di *accountability*, è bene osservare che l'EDPS si è limitato nei Primi Orientamenti ad analizzare i principi e le potenzialità delle tecnologie e delle relative implementazioni, senza determinare specifiche misure di sicurezza volte a consentire l'implementazione dei sistemi di IA generativa. Tale adempimento, difatti, deve necessariamente essere rimesso all'*accountability* delle IUE in quanto titolari del trattamento,

ISSN 2239-8570

che potranno assumere decisioni autonomamente, ma suffragati dai Primi Orientamenti, in un'ottica basata sul rischio specifico dei trattamenti e dei sistemi di IA implementandi o implementati.

Il Documento analizza tredici tematiche fondamentali, secondo lo schema "domanda- risposta-principio-esempio", suddivise in altrettante sezioni:

(i) che cos'è l'IA generativa?
(ii) possono le IUE utilizzare l'IA generativa?
(iii) come si può verificare che l'uso di un sistema di IA generativa comporti il trattamento di dati personali?
(iv) qual è il ruolo dei responsabili della protezione dei dati personali (**DPOs**) nel processo di sviluppo o *deployment* dei sistemi di IA generativa?
(v) qualora un'IUE volesse sviluppare o implementare sistemi di IA generativa, quando dovrebbe effettuare una valutazione d'impatto sulla protezione dei dati (**DPIA**)?
(vi) quando è lecito il trattamento dei dati personali nelle fasi di progettazione, sviluppo e validazione di sistemi di IA generativa?
(vii) come si può garantire il principio della minimizzazione dei dati quando si utilizzano sistemi di IA generativa?
(viii) i sistemi di IA generativa rispettano il principio di accuratezza dei dati?
(ix) come informare le persone sul trattamento dei dati personali quando le IUE utilizzano sistemi di IA generativa?
(x) come gestire le decisioni automatizzate ai sensi dell'articolo 24 del Regolamento?
(xi) come si può assicurare un trattamento equo ed evitare *bias* quando si utilizzano sistemi di IA generativa?
(xii) come si può assicurare l'esercizio dei diritti individuali quando si utilizzano sistemi di IA generativa?
(xiii) come si può assicurare la sicurezza dei dati quando si utilizzano sistemi di IA generativa?

Infine, la quattordicesima sezione del Documento riporta una serie di link ad altri documenti contenenti indicazioni utili per l'approfondimento dei temi trattati.

In estrema sintesi, i Primi Orientamenti, dopo aver definito le espressioni «IA generativa» «*foundation model*» e «*large language model*» (**LLM**) (espressioni che non si trovano definite nell'AI Act), sostengono con favore il possibile utilizzo da parte delle IUE di sistemi di IA generativa nei servizi pubblici, a condizione che vengano soddisfatti i requisiti legali imposti dalla disciplina sui dati personali ed assicurato il rispetto dei diritti fondamentali.

Le definizioni di IA generativa, *foundation model* e LLM contenute negli Orientamenti sono le seguenti [ns. traduzione dall'inglese]:

"La IA generativa è una sottospecie di IA che utilizza speciali modelli di *machine learning* progettati per produrre una vasta e generale varietà di output, capaci di una serie di compiti e applicazioni, come la generazione di testi, immagini o suoni. Concretamente, essa si avvale dell'uso dei c.d.

ISSN 2239-8570

foundation models, che servono da modelli di base per altri sistemi di IA generativa che saranno affinati attraverso di essi".

"Un *foundation model* serve come nucleo dell'architettura o base su cui vengono costruiti altri modelli più specializzati. Questi modelli sono addestrati sulla base di diversi ed estesi set di dati, inclusi quelli che contengono informazioni pubblicamente disponibili. Essi possono rappresentare strutture complesse come immagini, contenuti audio, video o di linguaggio e possono essere affinate per specifici compiti o applicazioni".

"I LLM sono un tipo specifico di *foundation model* addestrati su enormi quantità di dati di testo (da milioni a miliardi di parole) che possono generare rispste in linguaggio naturale a un'ampio spettro di inputs basati su modelli e relazioni tra parole e frasi. Questa vasta quantità di testo utilizzato per addestrare il modello può essere presa da Internet, libri, e altre fonti diponibili. Alcune applicazioni già in uso sono sistemi che generano codici [di programmazione per elaboratori elettronici], assistenti virtuali, strumenti di creazione di contenuti, motori di traduzione tra lingue, riconoscimento vocale automatico, sistemi di diagnosi mediche, strumenti di ricerca scientifica, etc." Viene inoltre operato un rinvio ad una pagina web esplicativa dei LLM preparata dall'EDPS.

La relazione tra IA generativa, *foundation model* e LLM è definita "gerarchica", nel senso che "la IA generativa è la categoria più ampia che contiene modelli progettati per creare contenuti. Un *foundation model*, come un LLM, agisce come l'architettura di base su cui modelli più specializzati sono costruiti. I modelli specializzati, costruiti sul *foundation model*, si offrono a specifici compiti o applicazioni, usando la conoscenza e le capacità dell'architettura di base del *foundation model*".

Nel Documento, l'EDPS sottolinea essere fondamentale che l'EUDPR venga applicato a tutte le attività di trattamento dei dati personali e che a tal fine è necessaria una chiara definizione delle responsabilità di tutte le parti coinvolte nel ciclo di vita del sistema di IA. Si specifica che il Regolamento si applica ad ogni fase dell'implementazione del sistema di IA che coinvolge il trattamento di dati personali, dalla raccolta e creazione di *dataset,* all'interazione dei soggetti con il sistema e alla generazione di contenuti. Il Documento aggiunge che meccanismi di monitoraggio e controllo regolari sono ritenuti essenziali per garantire il rispetto dei principi di protezione dei dati.

In proposito viene evidenziato che un ruolo cruciale nelle attività di monitoraggio e controllo deve essere esercitato dal DPO, figura centrale nell'assistere ed indirizzare le IUE nella *compliance* al Regolamento. Il DPO – si specifica nei Primi Orientamenti - deve essere in condizione di comprendere il ciclo di vita del sistema di intelligenza artificiale, garantire la trasparenza dei sistemi di IA, documentare i processi e promuovere la collaborazione tra le parti interessate, compresi i servizi legali e IT. I Primi Orientamenti suggeriscono la creazione di *task force ad hoc*, di cui faccia parte il DPO, ma che coinvolgano anche altre figure tecniche, al fine di massimizzare le competenze nel monitoraggio. Si sottolinea in proposito che i sistemi di IA introducono nuovi rischi per la sicurezza che devono essere gestiti con misure tecniche e organizzative adeguate, ed il

ISSN 2239-8570

monitoraggio continuo e il supporto tecnico specializzato sono essenziali per mitigare tali rischi.

Sempre a proposito dei sistemi di valutazione e monitoraggio, i Primi Orientamenti aggiungono che un ruolo fondamentale è svolto dal processo della DPIA. Il Documento specifica che la DPIA deve essere effettuata prima dell'inizio del trattamento algoritmico, e che essa è il principale strumento volto ad identificare e mitigare i potenziali rischi per i diritti e le libertà degli individui, per ciò idoneo a fornire un approccio strutturato alla gestione delle sfide relative alla protezione dei dati legate all'IA generativa.

Nella sezione 6, i Primi Orientamenti affrontano il tema della liceità del trattamento dei dati, in relazione alla determinazione della base giuridica più idonea su cui fondare i trattamenti algoritmici, e nelle sezioni 7 ed 8 affrontano le questioni specifiche inerenti all'applicazione dei principi di minimizzazione e accuratezza dei dati.

Gli ultimi approfondimenti dei Primi Orientamenti sono riservati alle maggiori criticità coinvolte nell'implementazione di sistemi di IA. Tra queste, il ruolo della trasparenza, di fondamentale importanza per poter informare gli interessati sulle modalità e le ragioni per le quali vengono trattati i loro dai personali. Nel Documento si riconosce che sistemi di IA generativa presentano sfide per l'esercizio dei diritti degli interessati; e si aggiunge che garantire la tracciabilità e una corretta gestione dei dati supporta l'esercizio efficace di questi diritti. Allo stesso modo, i Primi Orientamenti raccomandano alle IUE di implementare garanzie adeguate nei processi decisionali automatizzati, al fine di assicurare i diritti degli interessati, tra i quali emerge il diritto all'intervento umano e la possibilità di contestare le decisioni. Viene chiarito, in un'ottica orientata al rischio, che i sistemi automatizzati non dovrebbero essere utilizzati se sollevano preoccupazioni legali o etiche.

La minimizzazione dei *bias* e la garanzia di un output algoritmico equo sono altri due temi ai quali i Primi Orientamenti dedicano particolare attenzione. Il Documento sottolinea che sistemi di IA possono, anche inavvertitamente, perpetuare o amplificare i pregiudizi, portando a risultati ingiusti. In proposito, si sottolineano, giustamente, la necessità di un monitoraggio continuo e di strategie di mitigazione dei *bias* per sostenere gli standard etici e proteggere gli interessati dalle pratiche discriminatorie.

In conclusione, i Primi Orientamenti offrono un primo set di linee guida chiare e pratiche, intese ad aiutare le IUE a gestire la complessa relazione tra le tecnologie di IA, le norme sulla protezione dei dati e il più vasto complesso della tutela dei diritti fondamentali. L'EDPS vuole con ciò assicurare che le applicazioni dell'IA siano non solo *compliant*, ma anche eticamente sostenibili. In breve si vuole che il rispetto dei principi richiamati nel Documento, declinato dai soggetti nell'ambito della propria *accountability*, possa rendere l'uso dell'IA generativa consapevole e conforme alla legge, facilitando un futuro in cui l'innovazione tecnologica e la *privacy* si integrino armoniosamente, favorendo uno scenario di fiducia e progresso.

BEATRICE GALLUCCI

ISSN 2239-8570

https://www.edps.europa.eu/system/files/2024-06/24-06-03_genai_orientations_en.pdf

2024/2(15)VR

15. Il parere dell'EDPB n. 11/2024 del 24.5.2024 sull'uso delle tecnologie di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree per snellire il flusso dei passeggeri negli aeroporti.

Il 16.2.2024 l'Autorità di vigilanza francese (**Autorità**) ha chiesto al Comitato europeo per la protezione dei dati (**EDPB**) di emettere un parere sull'uso della tecnologia di riconoscimento facciale da parte degli operatori aeroportuali e delle compagnie aeree per l'autenticazione o l'identificazione biometrica dei passeggeri al fine di snellire il flusso negli aeroporti, ai controlli di sicurezza aeroportuali, alla consegna dei bagagli, all'imbarco e all'accesso alle sale d'attesa.

La richiesta muoveva essenzialmente dalla divergenza dei modelli in sperimentazione nei diversi aeroporti dell'Unione europea e dal conseguente rischio di diseguaglianze nel livello di tutela delle libertà fondamentali degli interessati.

Nello specifico, l'Autorità sottoponeva all'EDPB i quesiti che seguono.

In primo luogo, la compatibilità con gli artt. 5(1)(e) e (f), 25 e 32 del Regolamento UE n. 2016/679 (**GDPR**) dell'impiego della tecnologia descritta, nel caso di un sistema di memorizzazione in cui il modello biometrico di ciascun passeggero veniva memorizzato solo "nelle mani" dell'interessato, ad esempio sul suo dispositivo individuale, sotto il suo esclusivo controllo. In caso di risposta positiva, di poi, si richiedeva l'indicazione delle garanzie minime necessarie ai sensi degli artt. 25 e 32 GDPR.

In secondo luogo, la compatibilità con gli artt. 5(1)(e) e (f), 25 e 32 GDPR dell'impiego della tecnologia descritta nel caso di un sistema di archiviazione in cui il modello biometrico di ciascun passeggero veniva memorizzato in un *database* centralizzato all'interno dell'aeroporto, sotto il controllo dell'operatore aeroportuale, in forma criptata. Tale secondo quesito era a sua volta articolato in due sotto-quesiti, a seconda che le chiavi di accesso (necessarie alla decrittazione) fossero: nella disponibilità esclusiva dell'interessato (ad esempio, sul suo telefono cellulare); in possesso del gestore aeroportuale. In ambo i casi si domandava, in caso di risposta affermativa, l'indicazione delle garanzie minime adeguate ai sensi degli artt. 25 e 32 GDPR.

L'oggetto della richiesta, quindi, non comprendeva: il trattamento effettuato nell'ambito dei controlli di frontiera e di quelli effettuati dai negozi *duty-free*, poiché effettuato da titolari del trattamento diversi dagli operatori aeroportuali e dalle compagnie aeree; eventuali impieghi della tecnologia di riconoscimento facciale per scopi diversi da quelli illustrati o

ISSN 2239-8570

effettuato da parte di altri soggetti; il trattamento di dati personali di soggetti diversi dai passeggeri. Inoltre, il parere non concerneva – e, allo stesso tempo, non pregiudicava – un'analisi completa ed esaustiva della conformità al GDPR dei trattamenti operati nei singoli casi concreti.

Infine, esulava dai quesiti l'analisi della base giuridica applicabile; di conseguenza, non veniva esaminata la validità del consenso ai sensi degli artt. 6, 7 e 9 GDPR. Ad ogni modo, l'EDPB ha osservato, sul punto, quanto segue. In termini generali, i titolari del trattamento dovrebbero ottenere dalle persone che intendono utilizzare tali servizi un consenso esplicito, liberamente prestato, specifico, informato e revocabile in qualsiasi momento. È essenziale, inoltre, che le persone che non hanno acconsentito esplicitamente al riconoscimento facciale per lo scopo previsto non vengano scansionate dalle telecamere. In ogni caso, devono essere garantiti i principi sanciti dall'art. 5 GDPR in punto di necessità e proporzionalità.

All'analisi dei quesiti veniva anteposta un'illustrazione delle nozioni chiave.

Al riguardo, l'EDPB ha chiarito che un trattamento di dati quali le caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica può essere qualificato come avente a oggetto dati biometrici ai sensi dell'art. 4, n. 14 del GDPR solo allorché si dia una misurazione di tali caratteristiche. I dati biometrici sono, precisamente, il risultato di tali misurazioni. Il dato grezzo, quale, ad esempio, l'immagine del volto di un soggetto, rappresenta un campione biometrico; da esso è possibile estrarre una rappresentazione digitale ("*template*"), che consente o conferma l'identificazione unica della persona fisica. In genere, i processi finalizzati all'identificazione o all'autenticazione di un individuo tramite riconoscimento facciale consistono nel confronto tra un *template* biometrico in ingresso e gli oggetti memorizzati nel *database* di riferimento, per verificare una corrispondenza.

La tecnologia di riconoscimento facciale può svolgere due funzioni distinte: autenticazione e identificazione. L'autenticazione mira a confermare una richiesta biometrica attraverso un confronto che si esplica nella c.d. verifica 1 a 1. L'identificazione mira a ricercare in un *database* di registrazione biometrica gli identificatori attribuibili a un singolo individuo (c.d. identificazione 1-a-molti). In entrambi i casi, le tecniche di riconoscimento facciale si basano su una stima di stampo probabilistico e hanno a oggetto dati biometrici relativi a una persona fisica identificata o identificabile, integrando di conseguenza un trattamento di categorie particolari di dati personali ai sensi dell'art. 9 GDPR.

Ciò premesso, l'analisi delle questioni si snodava lungo quattro diversi scenari, come rappresentati nell'Allegato I della richiesta, da intendersi come esempi utilizzati a scopo illustrativo.

Il primo scenario prevedeva la memorizzazione del *template* biometrico registrato nelle mani del singolo utente, ad esempio sul suo dispositivo individuale, sotto il suo esclusivo controllo, al fine di autenticare il passeggero all'attraversamento dei suddetti punti di controllo aeroportuali. Più in dettaglio, l'iscrizione veniva effettuata dal gestore aeroportuale, sia da remoto tramite apposita applicazione sia presso i terminali aeroportuali, e consisteva nella registrazione e nella memorizzazione sul dispositivo del

ISSN 2239-8570

passeggero di un *template* biometrico e dei dati identificativi ("**ID**") necessari per il trattamento. La registrazione era eseguita solo una volta e per un periodo definito (ad esempio, la durata di validità del passaporto del passeggero). Né l'ID né i dati biometrici erano oggetto di conservazione terminata la registrazione.

In questo scenario, il *matching* era perfezionato nel contesto di un ambiente controllato, nel quale: i passeggeri venivano attivamente coinvolti; avevano un maggiore controllo sui loro dati, potendo interrompere il trattamento in qualsiasi momento con la cancellazione dei dati dal proprio dispositivo; la verifica passava attraverso appositi *pod*, di talché non erano estratti i dati biometrici di altri passeggeri che non avevano acconsentito al trattamento. Per tali ragioni, lo scenario presentava, a determinate condizioni, meno rischi rispetto all'uso di dati biometrici memorizzati in banche dati centralizzate.

Orbene, per quanto riguarda la compatibilità con l'art. 25 GDPR, e in particolare sul rispetto del requisito della minimizzazione, le misure in questione potevano considerarsi conformi al principio di necessità in relazione alla finalità perseguita (snellire il flusso dei passeggeri) a condizione che fosse dimostrata l'assenza di soluzioni alternative meno invasive in grado di raggiungere lo stesso obiettivo in modo altrettanto efficace.

Per quanto riguarda il principio di proporzionalità, si rilevava che l'intrusività del trattamento poteva essere controbilanciata dal coinvolgimento attivo dei passeggeri, in quanto il *template* biometrico era memorizzato esclusivamente nelle loro mani, sotto il loro esclusivo controllo, e i loro dati venivano cancellati poco dopo il completamento dell'abbinamento.

Per tali ragioni, l'EDPB ha concluso che il trattamento previsto nel primo scenario poteva considerarsi in linea di principio compatibile con gli artt. 5(1)(f), 25 e 32 GDPR, a condizione che venissero attuate garanzie adeguate. L'operatore doveva approntare almeno le seguenti salvaguardie, con l'intesa che il test di adeguatezza richiede un'analisi caso per caso e che occorreva garantire l'adozione di eventuali presìdi aggiuntivi, se necessari.

In primo luogo, si rendeva necessaria una valutazione d'impatto della protezione dei dati (DPIA), in linea con i requisiti *ex* art. 35 GDPR, ogniqualvolta era pianificato un trattamento dal rischio potenzialmente elevato. Per gestire i casi di falso negativo, era cruciale il contenimento del rischio di *bias* legati all'età, al genere e all'etnia attraverso il monitoraggio del funzionamento degli algoritmi in linea con le finalità della supervisione e dell'intervento umano. In generale, occorreva poi: garantire il massimo della trasparenza e assicurare il controllo da parte degli interessati nelle operazioni di trattamento; rispettare il principio di limitazione delle finalità; assicurare che non venissero catturate foto o video, anche se non registrate e non elaborate, di soggetti che non hanno acconsentito al riconoscimento facciale; consentire all'interessato di cancellare in qualsiasi momento il *template* biometrico; fornire soluzioni tecniche alternative a coloro che avessero rifiutato il consenso al riconoscimento.

ISSN 2239-8570

A livello organizzativo, oltre ai controlli di sicurezza di base sul dispositivo dell'utente, era opportuno: contenere la circolazione dei dati anche tra gli operatori partecipanti a vario titolo al trattamento, ove non strettamente necessario; definire una politica per la crittografia e la gestione delle chiavi; garantire la conformità agli artt. 44 ss. GDPR. Si rendevano inoltre necessari: un adeguato addestramento del personale; la predisposizione di procedimenti interni di valutazione delle misure tecniche e organizzative per garantire la sicurezza del trattamento. In ogni caso, doveva vietarsi l'accesso esterno ai dati identificativi e biometrici degli utenti.

Quanto alla sicurezza e alla gestione dei dati di controllo dell'identità degli utenti, l'EDPB richiedeva di: compartimentare i dati durante la trasmissione e l'archiviazione in almeno tre gruppi diversi (*e.g.* ID, dati biometrici e dettagli del volo); assicurare che essi venissero adeguatamente criptati tra la trasmissione e l'archiviazione; garantire procedure di cancellazione dei dati sicure ed eventualmente automatizzate, allo scadere di periodi di conservazione dei dati rigorosamente predeterminati; mantenere l'autenticità e l'integrità dei dati.

Il secondo scenario prevedeva la memorizzazione centralizzata, all'interno dell'aeroporto, di un *template* biometrico registrato in forma crittografata con una chiave che posta esclusivamente nelle mani del passeggero. La registrazione veniva effettuata una sola volta ed era valida per un determinato periodo (ad esempio, fino a un anno dopo l'ultimo volo e fino alla data di scadenza del passaporto). La procedura era controllata dall'operatore aeroportuale e consisteva nella generazione di dati ID e biometrici criptati, memorizzati in un *database* interno ai locali dell'aeroporto e senza che vi fosse interconnessione o interoperabilità tra i *database* centralizzati.

Con riguardo al principio di proporzionalità, l'intrusività del trattamento poteva essere controbilanciata dal coinvolgimento attivo del passeggero, che deteneva sotto il suo unico controllo la chiave/segreto dei suoi dati biometrici criptati.

In termini di sicurezza, i dati di ogni individuo venivano criptati con una chiave specifica conservata solo da quest'ultimo e posta sotto il suo esclusivo controllo. Inoltre, le informazioni necessarie per l'abbinamento (*i.e.* la chiave d'accesso) provenivano dall'utente stesso. Infine, il gestore aeroportuale predisponeva un secondo livello di crittografia con chiavi controllate dal gestore stesso.

Per assicurare la compatibilità con l'art. 5(1)(e) GDPR in questo scenario, ai titolari del trattamento si richiedeva di giustificare il rapporto di necessità tra il periodo di conservazione previsto e lo scopo da soddisfarsi nel caso completo.

La compatibilità con gli artt. 5(1)(f), e 32 GDPR poteva soddisfarsi a condizione che la chiave/segreto dell'individuo venisse conservata nel computer localizzato al posto di controllo e che solo l'indice del passeggero fosse inviato alla banca dati centrale per recuperare il *template* biometrico criptato. Con riferimento all'art. 25 GDPR, e in particolare per soddisfare il requisito della minimizzazione dei dati, occorreva garantire il rispetto del

ISSN 2239-8570

principio di necessità. Nello scenario in questione, il titolare del trattamento era tenuto dimostrare la mancanza di soluzioni alternative meno invasive idonee a soddisfare il medesimo obiettivo in modo altrettanto efficace.

In conclusione, il trattamento previsto nel secondo scenario poteva ritenersi in linea di principio compatibile con gli artt. 5(1)(e) e (f), 25 e 32 GDPR, a condizione che venissero prestate garanzie adeguate.

Nello specifico, in aggiunta alle considerazioni generali e alle indicazioni specifiche previste per lo Scenario I, si indicavano almeno i seguenti presìdi. Anzitutto, occorreva: assicurare che il passeggero avesse il controllo sui periodi di conservazione di tutti i suoi dati; limitare i periodi di conservazione a quanto necessario per lo scopo specifico, con possibilità degli interessati di stabilire il periodo di conservazione, anche più breve di quello predefinito; garantire all'interessato la possibilità di richiedere in qualsiasi momento la cancellazione di dati. A livello organizzativo, la gestione del server centrale doveva seguire regole di *governance* chiaramente definite e includere tutte le misure necessarie a garantirne la sicurezza. Sul piano tecnico, occorreva tenere traccia dei soggetti abilitati ad accedere ai dati personali, in particolare ai dati identificativi e biometrici, e delle avvenute consultazioni.

Per garantire la sicurezza – e, massimamente, proteggere il *database* centrale, anche da attacchi esterni – era necessario, tra l'altro, che: il *database* centrale, le unità di registrazione e le unità di abbinamento non fossero collegate a Internet; il funzionamento e la manutenzione di questi sistemi avvenissero localmente all'interno dei locali dell'aeroporto; fossero impiegate tecniche crittografiche all'avanguardia per proteggere gli scambi tra l'applicazione e il server centralizzato.

Il terzo scenario prevedeva la memorizzazione centralizzata di un modello biometrico registrato in forma criptata all'interno dell'aeroporto, sotto il controllo del gestore aeroportuale.

In questo caso i dati dei passeggeri erano oggetto di compartimentazione: i dati identificativi, il *template* biometrico registrato e le informazioni sul volo venivano memorizzati in tre diversi *database* e crittografati con chiavi diverse. I passeggeri dovevano registrarsi, per ogni volo, in un breve periodo prima della partenza (ad esempio, 48 ore). L'iscrizione poteva essere effettuata in remoto o presso i terminali aeroportuali, anche nella forma descritta nello Scenario 1. Nondimeno, in questo scenario i passeggeri venivano identificati secondo il confronto 1:N, dove N indicava il numero di passeggeri attesi in aeroporto in un arco di tempo di diversi giorni. Il periodo di conservazione era in genere di 48 ore e i dati venivano cancellati dopo il decollo.

Quanto ai potenziali rischi, poiché la memorizzazione dei dati identificativi e biometrici avveniva in un *database* centrale, se la riservatezza di quest'ultimo veniva compromessa, questo poteva comportare l'accesso all'intera serie di dati e provocare l'identificazione non autorizzata o illegale dei passeggeri in altri ambienti. Con riferimento al principio e ai requisiti di sicurezza (artt. 5(1)(f) e 32 GDPR), andava pertanto considerato che l'archiviazione di dati identificativi e biometrici in *database* centrali, anche se separati, può esporsi a rilevanti attacchi esterni e, potenzialmente,

ISSN 2239-8570

all'accesso illecito all'intero *set* di dati e a furti di identità su larga scala. Non solo. La violazione dei modelli di riconoscimento facciale e dell'ID associato poteva consentire l'identificazione non autorizzata o illegale degli interessati in altri ambienti. Il sistema di archiviazione centralizzata sotto il controllo del gestore aeroportuale, infine, sottraeva al passeggero il controllo dei propri dati.

A fronte di queste criticità, l'EDPB ha ritenuto che un risultato simile allo snellimento del flusso dei passeggeri negli aeroporti potesse essere raggiunto in modi diversi e meno invasivi. Di più. L'impatto negativo sui diritti e le libertà fondamentali degli interessati derivante da una violazione del *database* centralizzato doveva considerarsi maggiore del beneficio atteso da tale trattamento. Quest'ultimo, dunque, non soddisfaceva i principi di necessità e proporzionalità nel terzo scenario e non poteva ritenersi compatibile con l'art. 25 GDPR.

A differenza dei precedenti, infatti, nello Scenario 3 l'identificazione secondo il confronto 1:N comportava la ricerca nel *database* centrale e l'elaborazione di *template* biometrici su larga scala. Inoltre, le chiavi non erano tenute esclusivamente in mano dai passeggeri, con grave compromissione dell'autonomia dell'interessato, rimesso *in toto* alle scelte del titolare del trattamento.

Inoltre, ai fini degli artt. 5(1)(f) e 32 GDPR, le misure descritte con a questo scenario non sarebbero sufficienti a garantire un livello di sicurezza adeguato al rischio. In particolare, per quanto la limitazione della conservazione dei dati biometrici nel *database* centrale per un periodo di 48 ore poteva ridurre significativamente i rischi associati alle violazioni dei dati personali, il periodo di conservazione dei dati non era un fattore decisivo, di per sé, per la compatibilità complessiva di tale architettura, giacché esso poteva essere modificato dal titolare del trattamento.

Sulla scorta di queste considerazioni, l'EDPB ha concluso che il trattamento previsto nello Scenario 3 non poteva essere compatibile con gli artt. 5(1)(f), 25 e 32 del GDPR.

Infine, lo Scenario 4 prevedeva la memorizzazione centralizzata del *template* biometrico registrato in forma criptata sul *cloud*, sotto il controllo della compagnia aerea o del suo fornitore del relativo servizio.

In questo caso, i dati dei passeggeri erano crittografati e venivano decifrati all'atto del loro impiego (ad esempio, in occasione del *matching*); le chiavi d'accesso erano controllate dalla compagnia aerea o dal suo *cloud processor*. I dati biometrici dei passeggeri venivano utilizzati per l'identificazione dei passeggeri secondo il confronto 1:N.

Quanto ai rischi potenziali, poiché l'archiviazione dei dati identificativi e biometrici avveniva in un *database* centralizzato nel *cloud*, più soggetti avrebbero potuto attingervi: ad esempio, più operatori aeroportuali avrebbero potuto esaminare i risultati del *matching*. Non solo. Tale accesso avrebbe potuto estendersi a fornitori non appartenenti al SEE. Di poi, il fatto che i dati dei passeggeri venivano decriptati quando in uso e che le chiavi erano sotto il controllo della compagnia aerea o del *cloud processor* poteva aumentare la superficie di esposizione alla sicurezza. Poteva ancora osservarsi che: il carattere centralizzato del sistema di archiviazione

ISSN 2239-8570

sottraeva al passeggero il controllo dei propri dati; il periodo di conservazione, in questo scenario, poteva potenzialmente protrarsi fin quando il cliente restava titolare di un account con la compagnia aerea.

Valgono in questo caso le considerazioni già svolte con riferimento allo Scenario 3, accompagnate da qualche precisazione ulteriore. Si davano, anzitutto, maggiori rischi di trasferimento di dati personali verso paesi terzi, ponendosi maggiori difficoltà di raccordo con gli artt. 44 ss. GDPR.

Con specifico riferimento alla compatibilità con l'art. 25 GDPR, doveva osservarsi che i rischi derivanti dal confronto effettuato su larga scala erano acuiti rispetto allo scenario precedente, giacché nel criterio 1:N il secondo termine faceva riferimento al numero totale di clienti della compagnia aerea e non già solo al numero di passeggeri previsti in un arco di tempo di alcuni giorni.

Il trattamento previsto nello Scenario 4 non era dunque in grado di soddisfare il principio di necessità.

Per quanto riguarda il principio di proporzionalità, i rischi per i diritti degli interessati non sarebbero stati adeguatamente contenuti dalle garanzie previste, eccedendo il beneficio atteso dal trattamento, consistente solo in un leggero aumento della comodità e della velocità dei controlli.

Alla luce di queste considerazioni, l'EDPB ha ritento che il trattamento previsto nello Scenario 4 fosse: incompatibile con l'art. 25 del GDPR; non conforme agli artt. 5(1)(f), e 32 del GDPR; violativo dell'art. 5(1)(e) del GDPR in quanto privo di una ragione giustificativa sufficiente a supporto del periodo di conservazione previsto.

VALENTINO RAVAGNANI

Parere EDPB 11/2024

2024/2(16)FDA

16. La sentenza della CGUE del 14.3.2024 nella causa C-46/23 sul principio per cui le autorità di controllo degli Stati membri possono ordinare di cancellare anche d'ufficio i dati personali raccolti da qualunque amministrazione nazionale in violazione del GDPR

Con la sentenza C-46/23 del 14 marzo 2024 (la **Sentenza**) la Corte di giustizia dell'Unione europea (**CGUE**) ha enunciato l'importante principio giuridico per cui le autorità garanti della *privacy* degli Stati membri possono ordinare di cancellare, tanto su istanza di parte, quanto d'ufficio, i dati personali raccolti da qualunque amministrazione nazionale in violazione del regolamento UE 2016/679 (**GDPR**).

Nello specifico, i fatti di causa risalgono all'anno 2020, allorquando il comune ungherese di Újpest ha deciso di concedere un aiuto economico ad alcuni concittadini in difficoltà a causa delle restrizioni imposte dalla pandemia, chiedendo a tal fine all'amministrazione erariale e agli uffici dell'anagrafe nazionale di fornirgli i dati biografici e i riferimenti

ISSN 2239-8570

previdenziali dei possibili beneficiari per raccoglierli in una banca dati telematica.

Avvertito da una segnalazione il garante ungherese dei dati personali ha immediatamente avviato d'ufficio un'indagine e ha contestato all'amministrazione comunale di Újpest di aver divulgato un'ampia mole di dati riservati senza il previo consenso dei cittadini interessati e in violazione del GDPR; in conseguenza di ciò le ha ordinato di cancellare i dati trattati in maniera illecita e le ha inflitto una sanzione pecuniaria.

In risposta, il comune di Újpest ha impugnato il provvedimento avanti al tribunale amministrativo di Budapest e ha eccepito come il garante nazionale per i dati personali non avesse il potere di ordinare la cancellazione dei dati in "*assenza di una richiesta presentata dall'interessato*"; visto che tale diritto è "*concepito esclusivamente come un diritto dell'interessato*" dagli artt. 17 e 58 del GDPR (punto 18 della Sentenza).

È per questa ragione che il giudice amministrativo ungherese, dubitando della corretta interpretazione delle norme sovranazionali richiamate, ha deferito la questione alla CGUE, la quale, in prima battuta, ha precisato che la normativa di settore distingue due ipotesi: "*da un lato, la cancellazione dei dati su richiesta dell'interessato e, dall'altro, la cancellazione derivante dall'esistenza di un obbligo autonomo, gravante sul titolare del trattamento, e ciò indipendentemente da qualsiasi richiesta dell'interessato*" (punto 37 della Sentenza).

Nel secondo caso – in cui ricade la vicenda decisa dalla Sentenza – il GDPR assegna all'autorità nazionale di controllo "*poteri effettivi al fine di agire efficacemente contro le violazioni di tale regolamento e, in particolare, di porvi fine, anche nei casi in cui gli interessati non siano informati del trattamento dei loro dati personali, non ne siano a conoscenza o non abbiano, in ogni caso, chiesto la cancellazione di tali dati*" (punto 41 della Sentenza).

In simili occasioni, l'autorità nazionale può sempre "*adottare le misure appropriate al fine di porre rimedio alla violazione constatata, e ciò indipendentemente dall'esistenza di una previa richiesta presentata dall'interessato*" (punto 42 della Sentenza); un'eventuale interpretazione contraria "*significherebbe che il titolare del trattamento potrebbe, in assenza di una simile richiesta, conservare i dati personali in questione e continuare a trattarli illecitamente*" e "*nuocerebbe all'effettività della protezione prevista da tale regolamento, in quanto porterebbe a privare di protezione le persone inattive sebbene i loro dati personali siano stati trattati illecitamente*" (punto 45 della Sentenza).

Alla luce di ciò la CGUE ha concluso che "*l'autorità di controllo di uno Stato membro è legittimata, nell'esercizio del suo potere di adozione delle misure correttive previste da tali disposizioni, a ordinare al titolare del trattamento o al responsabile del trattamento di cancellare dati personali che sono stati trattati illecitamente, e ciò anche qualora l'interessato non abbia presentato a tal fine alcuna richiesta di esercitare i suoi diritti*"; inoltre il "*potere dell'autorità di controllo di uno Stato membro di ordinare la cancellazione di dati personali che sono stati trattati illecitamente può*

ISSN 2239-8570

riguardare sia dati raccolti presso l'interessato sia dati provenienti da un'altra fonte" (punto 54 della Sentenza).

FILIPPO D'ANGELO

https://curia.europa.eu/juris/documents.jsf?num=C-46/23

2024/2(17)GR

17. La sentenza della CGUE del 30.4.2024 nella causa C-470/21 su lotta alla contraffazione e tutela dei dati personali ai sensi della direttiva e-privacy

La Corte di giustizia dell'UE (**CGUE** o la **Corte**), nella sua composizione più autorevole, con sentenza del 30 aprile 2024, C-470/21, *La Quadratur du Net et al*., (di seguito anche solo la **Sentenza**) ha fornito risposta alla domanda pregiudiziale, sottopostagli dal *Conseil d'État* di Parigi, relativa all'interpretazione dell'art. 15(1) della direttiva 2002/58/CE sul trattamento di dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche (di seguito **direttiva e-privacy**) tenuto conto degli artt. 7, 8, 11 e 52(1) della Carta dei diritti fondamentali dell'Unione europea (**CDFUE**).

Ricordiamo che l'art. 15(1) direttiva e-privacy prevede che tutte le misure che gli Stati membri possono adottare ai sensi della medesima disposizione per limitare i diritti e gli obblighi previsti dalla direttiva e-privacy, tra cui per le finalità di contrasto di reati, devono in ogni caso essere conformi ai principi generali del diritto comunitario, e che i predetti articoli della CDFUE riguardano il rispetto della vita privata e della vita familiare (art. 7 CDFUE), la protezione dei dati personali (art. 8 CDFUE), la libertà di espressione e di informazione (art. 11 CDFUE) e la riserva di legge per ogni eventuale limitazione ai diritti garantiti dalla CDFUE nel rispetto del loro nucleo essenziale e del principio di proporzionalità (art. 52(1) CDFUE).

La vicenda giudiziaria che ha portato il *Conseil d'État* a sottoporre la domanda di pronuncia pregiudiziale alla CGUE vedeva contrapposti da un lato *La Quadrature du Net*, la *Fédération des fournisseurs d'accès à Internet associatifs*, *Franciliens.net* e *French Data Network* e, dall'altro lato, il *Premier ministre* e il *ministre de la Culture* della Repubblica francese. La questione controversa atteneva alla legittimità del *décret* n. 2010-236, del 5 marzo 2010, relativo al trattamento automatizzato di dati personali autorizzato dall'articolo L. 331-29 del codice della proprietà intellettuale rubricato "Sistema di gestione delle misure per la protezione delle opere su Internet" (come modificato dal *décret* n. 2017-924 del 6 maggio 2017, relativo alla gestione dei diritti d'autore e dei diritti connessi da parte di un organismo di gestione di diritti e recante modifica del codice della proprietà intellettuale).

ISSN 2239-8570

Precisamente il *Conseil d'État* ha sottoposto alla Corte di giustizia le seguenti tre questioni pregiudiziali:

(i) se, in linea di principio, i dati relativi all'identità civile corrispondenti a un indirizzo IP rientrino tra i dati di traffico o di ubicazione assoggettati ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente dotata di poteri vincolanti;

(ii) se al quesito sub (i) la Corte dovesse fornire risposta affermativa, tenendo conto della bassa sensibilità dei dati relativi all'identità civile degli utenti, si pone la questione di stabilire se la direttiva e-privacy, letta sulla scorta degli artt. 7, 8, 11 e 52(1) CDFUE, debba interpretarsi nel senso che essa osta ad una normativa nazionale che preveda la raccolta di tali dati relativi agli indirizzi IP degli utenti da parte di un'Autorità amministrativa, senza un controllo preventivo da parte di un giudice o di un'Autorità amministrativa indipendente con poteri vincolanti;

(iii) infine, qualora la Corte dovesse fornire risposta affermativa anche alla questione sub (ii), data la bassa sensibilità dei dati relativi all'identità civile, dato che solo questi dati possono essere raccolti al solo fine di prevenire violazioni di obblighi definiti in modo circostanziato, e dato che un controllo sistematico dell'accesso ai dati di ogni utente da parte di un giudice o di un'entità amministrativa terza con poteri vincolanti risulterebbe talmente gravoso da presentare il rischio di compromettere l'espletamento della missione di servizio pubblico affidata all'autorità amministrativa anch'essa indipendente che effettua tale raccolta, si pone la questione di stabilire se la direttiva e-privacy osti allo svolgimento di tale controllo con modalità appropriate, come un monitoraggio automatizzato, eventualmente sotto la supervisione di un servizio interno all'organismo, che offra garanzie di indipendenza e di imparzialità relativamente ai soggetti incaricati alla raccolta.

La Corte, anzitutto, ha ritenuto che le questioni ad essa sottoposte non possano essere trattate disgiuntamente risolvendosi tutte, sostanzialmente, nella domanda se l'art. 15(1) direttiva e-privacy, letto alla luce della CDFUE, debba essere interpretato nel senso che osta a una normativa nazionale che, al fine di identificare gli autori di una violazione dei diritti d'autore *online*, autorizza l'Autorità pubblica (incaricata della protezione dei diritti d'autore e connessi contro le violazioni commesse su Internet) ad accedere ai dati relativi all'identità civile, conservati dai fornitori di servizi di comunicazione elettronica, corrispondenti a indirizzi IP precedentemente raccolti da organismi degli aventi diritto, senza che tale accesso sia subordinato al requisito di un previo controllo da parte di un giudice o di un'Autorità amministrativa indipendente.

Così semplificata la questione, la CGUE ha stabilito che una Autorità pubblica nazionale responsabile della lotta ai reati di contraffazione online è legittimata accedere sulla base di un indirizzo IP ai dati di identificazione dei presunti colpevoli.

Più di preciso, secondo la Corte, l'articolo 15(1) direttiva e-privacy non impedisce ad una normativa nazionale di autorizzare un'Autorità preposta alla tutela del diritto d'autore ad accedere ai dati conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico incrociando i

ISSN 2239-8570

dati relativi all'identità civile con gli indirizzi IP, purché siano rispettate quattro condizioni desumibili dalla normativa vigente.

La prima è che tali dati siano conservati secondo modalità tecniche atte ad evitare che, mediante un'attività di profilazione basata sull'utilizzo combinato di diverse categorie di dati raccolti dai fornitori di servizi di comunicazione elettronica, possano trarsi informazioni sulla vita privata dei titolari dei rispettivi indirizzi IP. A tal fine secondo la Corte risulta opportuno, oltreché stabilire che i dati raccolti non possano essere conservati per un periodo superiore a quello strettamente necessario ad assicurare l'*enforcement* dei diritti d'autore e connessi, prevedere, ad esempio, l'obbligo di conservare separatamente le diverse categorie di dati personali raccolti (come i dati relativi all'identità civile, agli indirizzi IP, al traffico *online* e all'ubicazione) così impedendo *in limine* l'utilizzo incrociato prodromico all'attività di profilazione.

La seconda condizione è che l'accesso dell'Autorità pubblica a tali categorie di dati risulti finalisticamente orientato esclusivamente a identificare la persona sospettata di aver commesso una violazione *online*, e purché siano assicurate al presunto *infringer* le garanzie necessarie affinché l'accesso ai dati che lo riguardano non possa consentire di trarre informazioni sulla sua vita privata. Secondo i giudici di Lussemburgo occorre, quindi, imporre ai funzionari dell'Autorità preposta il divieto di divulgare (al di fuori delle comunicazioni necessarie allo scopo di assicurare l'*enforcement* dei diritti), in qualsiasi forma, informazioni sui contenuti *online* consultati dai titolari dei rispettivi indirizzi IP e, più in generale, di utilizzare tali indirizzi IP per qualsiasi scopo diverso da quello volto all'identificazione dei presunti *infringer*.

La terza condizione è che la possibilità, per il personale incaricato all'esame dei fatti all'interno dell'autorità pubblica preposta, di incrociare i dati con *file* contenenti informazioni che rivelano il titolo di opere protette la cui messa a disposizione *online* ha legittimato la raccolta di indirizzi IP da parte delle organizzazioni dei titolari dei diritti, nei casi di reiterazione della violazione dei diritti d'autore o connessi, a un controllo da parte di un'autorità giudiziaria o amministrativa indipendente, che non può essere completamente automatizzato e deve avvenire prima di qualsiasi utilizzo incrociato dei dati, posto che tale uso è in grado, in determinate circostanze, a consentire di trarre informazioni precise sulla vita privata della persona, il cui indirizzo IP è stato utilizzato per attività potenzialmente in grado di violare il diritto d'autore o connessi.

Infine, la quarta condizione, si sostanzia nel fatto che il sistema di trattamento dei dati utilizzato dall'autorità pubblica risulti soggetto a intervalli periodici a una revisione, da parte di un organismo indipendente terzo rispetto a tale autorità pubblica, diretta a verificare l'integrità del sistema, quindi, le garanzie poste a presidio del rischio di accesso abusivo a tali dati o l'utilizzo illecito degli stessi, nonché la sua efficacia e affidabilità nell'individuare potenziali comportamenti illeciti.

GIORGIO REMOTTI

ISSN 2239-8570

Sentenza CGUE causa C-470/21

2024/2(18)DPDM

18. La sanzione di oltre 1,8 miliardi di euro irrogata il 04.03.2024 dalla Commissione europea ad Apple per abuso di posizione dominante per le regole delle app di musica in *streaming* su App Store

Con comunicato stampa del 4 marzo 2024, la Commissione europea (la **Commissione**) ha annunciato la sanzione di oltre 1,8 miliardi di euro imposta in solido ad Apple Inc. and Apple Distribution International Limited (**Apple**) per abuso di posizione dominante nel mercato della distribuzione di app di *streaming* musicale agli utenti di iPhone e iPad attraverso l'App Store (caso AT.40437). La Commissione ha accertato che Apple ha imposto restrizioni agli sviluppatori di app, impedendo loro di informare gli utenti iOS riguardo a servizi di abbonamento musicale alternativi disponibili al di fuori dell'app, violando così le norme antitrust dell'UE.

La Commissione ha accertato la situazione per cui Apple è l'unico fornitore di un App Store tramite il quale gli sviluppatori possono distribuire le loro app agli utenti iOS nell'intero Spazio Economico Europeo. Apple, inoltre, stabilisce i termini e le condizioni che gli sviluppatori devono rispettare per essere presenti sull'App Store e raggiungere gli utenti iOS nel mercato di riferimento.

L'indagine della Commissione ha evidenziato che Apple vietava agli sviluppatori di app di *streaming* musicale sia di informare adeguatamente gli utenti iOS riguardo alla disponibilità di servizi di abbonamento musicale alternativi e più economici, distribuiti al di fuori dell'app, sia di fornire istruzioni su come abbonarsi a tali offerte. In particolare, le restrizioni imposte agli sviluppatori colpiscono non solo le informazioni inerenti ai prezzi degli abbonamenti disponibili su internet, ma anche la possibilità di includere link che conducano a siti web dove possono essere acquistati abbonamenti alternativi. La decisione della Commissione conclude che tali clausole, dette '*anti-steering*', costituiscono condizioni commerciali sleali, che violano l'articolo 102(a) del Trattato sul Funzionamento dell'Unione Europea (**TFUE**).

La Commissione ha ritenuto che condotta di Apple, durata quasi dieci anni, ha probabilmente portato molti utenti iOS a pagare prezzi significativamente più alti per gli abbonamenti di *streaming* musicale a causa delle elevate commissioni imposte da Apple agli sviluppatori, trasferite poi sui consumatori. Inoltre, le clausole *anti-steering* hanno degradato l'esperienza utente, costringendo gli utenti iOS a una ricerca complessa per trovare offerte alternative o portandoli a non abbonarsi a nessun servizio.

Per stabilire l'ammontare della sanzione, la Commissione ha tenuto conto della durata e della gravità della violazione, nonché del fatturato totale e

ISSN 2239-8570

della capitalizzazione di mercato di Apple. Ha tenuto conto altresì del fatto che Apple ha fornito informazioni inesatte nell'ambito della procedura amministrativa di accertamento.

Nel strutturare la sanzione, la Commissione ha deciso di aggiungere all'importo di base un'ulteriore somma forfettaria di 1,8 miliardi di euro per garantire che la sanzione complessiva inflitta ad Apple sia proporzionata, sufficientemente dissuasiva, e che lo sia anche per aziende di dimensioni simili. Tale sanzione forfettaria si è resa necessaria in questo caso perché una parte significativa del danno causato dalla violazione delle regole della concorrenza consiste in un danno non monetario, che non può essere adeguatamente risarcito secondo la metodologia basata sugli utili della società. La Commissione ha inoltre ordinato ad Apple di rimuovere le clausole *anti-steering* e di astenersi dal reiterare la violazione.

Le sanzioni inflitte alle imprese che violano le norme antitrust dell'UE sono versate nel bilancio generale dell'UE e contribuiscono quindi a finanziare l'UE e a ridurre l'onere per i contribuenti di ciascuno Stato membro. Nel comunicato stampa, la Commissione ricorda che qualsiasi persona o azienda colpita da un comportamento anticoncorrenziale come quello descritto può adire i tribunali degli Stati membri al fine di chiedere il risarcimento dei danni, posto che, nei procedimenti dinanzi ai tribunali nazionali, una decisione della Commissione costituisce una prova vincolante sia del fatto che il comportamento ha avuto luogo sia della sua contrarietà al diritto della concorrenza.

DOMENICO PIERS DE MARTINO

Comunicato stampa:
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161

Testo provvisorio del provvedimento:
https://ec.europa.eu/competition/antitrust/cases1/202419/AT_40437_10026012_3547_4.pdf

Pagina online del Registro pubblico dei procedimenti antitrust della Commissione per il caso AT.40437:
https://competition-cases.ec.europa.eu/search?search=AT.40437&sortField=relevance&sortOrder=DESC

2024/2(19)EMI

19. La comunicazione della Commissione ad Apple del 24.6.2024 di conclusioni preliminari sulla violazione del DMA ad opera delle regole dell'Apple Store e l'apertura di una nuova indagine per violazione del DMA ad opera dei nuovi obblighi posti da Apple a carico di terzi sviluppatori di app e app stores tra cui la nuova "Core Technology Fee"

ISSN 2239-8570

In data 24 giugno 2024, la Commissione europea (la "**Commissione**") ha comunicato, in via preliminare (attraverso l'invio di *preliminary findings*), che le regole dell'App store di Apple violano il Digital Markets Act (Regolamento (UE) 2022/1965) ("**DMA**"), in quanto impedirebbero agli sviluppatori di app di indirizzare liberamente i consumatori verso canali alternativi a per offerte e contenuti.

In aggiunta, la Commissione ha avviato un nuovo procedimento di non conformità (*non-compliance investigation)* nei confronti di Apple sulla base dei timori che i nuovi requisiti contrattuali per gli sviluppatori terzi di app e di app store non siano in grado di garantire l'effettivo rispetto degli obblighi di Apple ai sensi del DMA. In particolare, oggetto di approfondimento è il nuovo c.d. "*Core Technology Fee*" che sembrerebbe essere in contrasto con le regole europee in materia.

In virtù di quanto disposto dal DMA, infatti, gli sviluppatori che distribuiscono le loro applicazioni tramite l'App Store di Apple dovrebbero essere in grado, gratuitamente, di informare i loro clienti sulle possibilità di acquisto alternative e più economiche, indirizzandoli verso tali offerte, e di consentire loro di effettuare gli acquisti in tal modo.

Apple ha tre serie di condizioni contrattuali che regolano i rapporti con gli sviluppatori di app, comprese le regole di gestione dell'App Store. La Commissione ha però ritenuto che nessuna di queste regole contrattuali consente agli sviluppatori di orientare liberamente i propri clienti. A titolo esemplificativo, la Commissione ha rilevato che gli sviluppatori non possono fornire informazioni sui prezzi all'interno dell'app o comunicare in qualsiasi altro modo con i loro clienti per promuovere offerte disponibili su canali di distribuzione alternativi.

Inoltre, in base alla maggior parte delle condizioni commerciali disponibili per gli sviluppatori di app, Apple consente il c.d. pilotaggio solo tramite il processo c.d. "*link-out*", ossia gli sviluppatori di app hanno la possibilità di includere un link nella propria app di reindirizzamento ad una pagina web dove il cliente può concludere un contratto. Il processo di *link-out* è soggetto a diverse restrizioni imposte da Apple che impediscono agli sviluppatori di app di comunicare, promuovere offerte e concludere contratti attraverso il canale di distribuzione da loro prescelto.

La Commissione ritiene che, sebbene sia corretto prevedere un compenso per Apple per aver facilitato l'acquisizione iniziale di un nuovo cliente da parte degli sviluppatori tramite l'App Store, i compensi addebitati da Apple vadano ben oltre quanto strettamente necessario per la remunerazione di una simile attività. Ad esempio, si mette in evidenza che Apple addebita agli sviluppatori un compenso per ogni acquisto di beni o servizi digitali che l'utente effettua nei sette giorni successivi all'uscita dall'applicazione.

Come detto, la Commissione ha, inoltre, avviato una indagine di non conformità sui nuovi termini contrattuali di Apple per gli sviluppatori. Queste nuove regole prevedono in particolare la fornitura di app store alternativi o la possibilità di offrire una applicazione tramite un canale di distribuzione alternativo. Ad oggi, Apple ha mantenuto l'opzione di sottoscrivere le condizioni precedenti, che non consentono affatto canali di distribuzione alternativi, in contrasto, quindi, con il dettato del DMA.

ISSN 2239-8570

In particolare, la Commissione vuole verificare se questi nuovi requisiti contrattuali per gli sviluppatori terzi di app e di app store violino l'articolo 6(4) del DMA e in particolare i requisiti di necessità e proporzionalità ivi previsti.

L'indagine si sofferma, in particolar modo, sulla nuova "*Core Technology Fee*" di Apple, in base alla quale gli sviluppatori di app store e app di terzi devono pagare un importo di 0,50 euro per ogni app installata. La Commissione, quindi, si pone l'obiettivo di accertare che la struttura tariffaria imposta da Apple nell'ambito delle nuove condizioni commerciali sia effettivamente conforme al DMA.

In aggiunta, si vogliono indagare anche i vari step di *download* e di installazione dell'app dall'App Store di Apple. Nel dettaglio, è necessario verificare che i vari passaggi che un utente deve compiere per completare con successo il download e l'installazione di app store o di app alternative, nonché le varie schermate informative visualizzate dall'utente, siano conformi al DMA.

Infine, oggetto di ulteriore approfondimento sono i requisiti di ammissibilità per gli sviluppatori che riguardano la possibilità di offrire app store alternativi o di distribuire direttamente app dal web sugli iPhone. Questi requisiti, come l'"iscrizione in regola" all'*Apple Developer Program* che gli sviluppatori di app devono soddisfare per poter beneficiare della distribuzione alternativa prevista dal DMA, devono essere oggetto di specifica indagine di conformità al DMA.

In conclusione, sia i sopra riassunti *preliminary findings* sia l'apertura di un'indagine preliminare per i descritti ulteriori addebiti di non conformità al DMA, mettono in rilievo le criticità delle regole e delle condizioni contrattuali utilizzate da Apple nei rapporti con gli sviluppatori di app nell'ambito del proprio App Store.

Apple, nelle more della presente indagine, ha già avuto modo di replicare, sostenendo, in una propria nota ufficiale, la piena aderenza dei propri requisiti e termini contrattuali alle regole vigenti in Europa.

Dunque, si dovranno ora attendere gli esiti dell'indagine per accertare le asserite violazioni del DMA da parte dell'App Store di Apple.

ENZO MARIA INCUTTI

https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3433

2024/2(20)RA

20. La Commissione europea apre una indagine su Meta per la possibile violazione delle norme del DSA in relazione a fenomeni di 'dipendenza social' dei minori sulle piattaforme Facebook e Instagram

Il 16 maggio 2024 la Commissione europea (la "**Commissione**") ha aperto un'indagine nei confronti di Meta Platforms Ireland Ltd. ("**Meta**") –

ISSN 2239-8570

fornitore delle piattaforme *online* Facebook e Instagram – al fine di verificare se la società irlandese abbia violato quanto previsto dal regolamento (UE) 2022/2065 (Regolamento sui servizi digitali o *Digital Services Act* o "**DSA**"), in relazione alla protezione dei minori.

Facebook e Instagram sono state designate piattaforme *online* di dimensioni molto grandi ("**VLOPs**") il 25 aprile 2023 (v. in questa Rubrica notizia n. 5 nel numero 2/2023 [2023/2(5)RA]), poiché oltrepassano la soglia dei 45 milioni di utenti medi mensili nell'UE prevista all'art. 33(1) DSA. In qualità di VLOPs, a partire dall'agosto 2023 (e, cioè, quattro mesi dopo la loro designazione), il fornitore di tali piattaforme è tenuto al rispetto degli obblighi generali previsti dal Capo III del DSA, nonché di taluni "*obblighi supplementari*" previsti dalla Sezione 5 del Capo III del DSA.

In particolare, Meta è tenuta a rispettare, tanto con riguardo a Facebook quanto con riguardo a Instagram:

- l'art. 28 DSA, che prevede che i "*fornitori di piattaforme online accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio*";
- l'art. 34 DSA, secondo il quale i "*fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi individuano, analizzano e valutano con diligenza gli eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi*", effettuando una valutazione del rischio che comprenda anche: *(i)* "*eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, in particolare* […] *al rispetto dei diritti del minore sancito nell'articolo 24 della Carta* [i.e. la Carta dei diritti fondamentali dell'Unione europea]"; *(ii)* "*qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona*";
- l'art. 35 DSA, a mente del quale i "*fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi adottano misure di attenuazione ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati a norma dell'articolo 34, prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali*" e ciò, anche attraverso l'"*adozione di misure mirate per tutelare i diritti dei minori, compresi strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi*".

Sulla base della valutazione del rischio effettuata da Meta nel settembre 2023, la Commissione ha manifestato talune preoccupazioni circa il fatto che i sistemi adottati da Facebook e Instagram siano conformi a quanto previsto dai menzionati artt. 28, 34 e 38 del DSA, posto che essi parrebbero stimolare dipendenze comportamentali dei minori (come il c.d. *rabbit-hole*

ISSN 2239-8570

effect) e, al contempo, non garantirebbero un'idonea verifica dell'età degli utenti.

Per tale ragione, attraverso l'indagine avviata il 16 maggio 2024, la Commissione dovrà ora comprendere se la società irlandese stia effettivamente osservando gli obblighi previsti dal DSA, con particolare riguardo:

- alla valutazione e alla mitigazione del rischio che l'interfaccia di Facebook e Instagram sfruttino debolezze e inesperienze dei minori, così da causare una dipendenza comportamentale e ledere il diritto fondamentale al benessere fisico e mentale dei minori;
- alla implementazione di misure di mitigazione tali da prevenire l'accesso dei minori a contenuti non appropriati, anche attraverso meccanismi di verifica dell'età dell'utente;
- alla necessità di impiegare misure adeguate e proporzionate alla necessità di assicurare un elevato livello di *privacy*, sicurezza e salute dei minori.

RICCARDO ALFONSI

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664

2024/2(21)RG

21. Entrata in vigore la legge sul c.d. oblio oncologico (legge 7 dicembre 2023, n. 193)

Con la legge 7 dicembre 2023, n. 193, rubricata *Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche*, il legislatore ha introdotto nell'ordinamento il c.d. diritto all'oblio oncologico la cui definizione è contenuta nel secondo comma dell'art. 1: «*diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica, nei casi di cui alla presente legge*».

La legge, entrata in vigore il 2 gennaio 2024, consta di cinque articoli finalizzati ad introdurre misure volte ad assicurare che i soggetti, clinicamente guariti da patologie oncologiche, godano dei medesimi diritti del resto della popolazione non subendo discriminazione a causa della malattia pregressa. La *ratio* generale della legge è chiara sin dal primo inciso dell'art. 1 il quale, nel definire il perimetro applicativo, sancisce in *incipit*, l'intento di escludere forme di discriminazione pregiudizievole, introducendo per un verso disposizioni attuative di norme, nazionali ed europee, in materia di parità di trattamento e non discriminazione e dall'altro tipizzando un vero e proprio diritto all'oblio oncologico.

Il rango delle norme richiamate nel primo comma dell'art.1 a cui la legge 193/23 intende dare attuazione ed il loro contenuto eterogeneo mostrano l'intenzione del legislatore di "avvolgere" "l'individuo guarito" in una rete di protezione molto ampia che ne assicuri istanze legate alle prerogative

ISSN 2239-8570

fondamentali della persona (si veda il riferimento all'articolo 2 della Costituzione sul riconoscimento dei diritti inviolabili dell'uomo ed al successivo art. 3 sull'eguaglianza e pari dignità sociale) con riferimento al diritto alla salute (e qui ricorre il richiamo all'art. 32 della Costituzione, all'art. 35 della Carta dei diritti fondamentali dell'Unione europea - di seguito "**CDFUE**" - e al Piano europeo di lotta contro il cancro, di cui alla Comunicazione della Commissione europea COM(2D21) 44 final) al rispetto della vita privata e della vita familiare (art. 7 CDFUE e art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali) alla protezione dei dati personali (art. 8 CDFUE), alla non discriminazione (art. 21 CDFUE) e alla protezione dei consumatori (art. 38 CDFUE).

L'interesse per le principali dimensioni di realizzazione della persona è confermato dal combinato disposto delle norme che seguono, non a caso dedicate all'uso e consumo di servizi (art. 2), alla genitorialità (art. 3 in materia di adozione) all'accesso al mondo del lavoro (art. 4 in materia di procedure concorsuali e selettive).

Al centro della legge 193/2023 stanno le informazioni relative allo stato di salute della persona fisica concernenti patologie oncologiche da cui la stessa sia stata precedentemente affetta e il cui trattamento attivo si sia concluso, senza episodi di recidiva, da più di dieci anni o da più di cinque anni nel caso in cui la patologia sia insorta prima del compimento del ventunesimo anno di età.

L'art. 2 vieta l'acquisizione e in ogni caso l'utilizzazione di tali informazioni relative ad una persona fisica contraente ai fini della determinazione delle condizioni contrattuali di qualunque tipo contratto, anche esclusivamente tra privati.

L'art. 3 introduce una serie di modifiche alla legge 4 maggio 1983, n. 184, in materia di adozione, vietando l'acquisizione e l'utilizzazione delle medesime informazioni relative alle persone che intendono adottare.

L'art. 4 vieta di richiedere le stesse informazioni relative a candidati ai fini dell'accesso a procedure concorsuali e selettive, pubbliche e private, anche quando nel loro ambito sia previsto l'accertamento di requisiti psico-fisici o concernenti lo stato di salute dei candidati.

Per quanto attiene più in particolare, all'art. 2, il nuovo diritto a non dover fornire informazioni né essere oggetto di indagini sulla propria pregressa condizione patologica opera anche in riferimento all'accesso ai servizi bancari, finanziari, di investimento (di seguito più sinteticamente "creditizi" o "finanziari") e assicurativi, dove una simile esigenza di non discriminazione appare particolarmente avvertita.

Va rilevato in proposito come nel settore della contrattazione finanziaria e assicurativa, il diritto all'oblio oncologico sia destinato a relazionarsi strettamente con quello all'accessibilità ai diversi servizi, che non deve essere pregiudicata, viziata, influenzata o esclusa dalla storia clinica passata, del singolo contraente.

A dispetto della rubrica dell'articolo, la norma ha una portata generale posto che l'inciso "*nonché nell'ambito della stipulazione di ogni altro tipo di contratto, anche esclusivamente tra privati*" rende invocabile un diritto

ISSN 2239-8570

all'oblio oncologico ogni qualvolta si sia in presenza di un accordo negoziale (dunque non solo nei servizi richiamati nella rubrica dell'articolo e non solo nell'ambito di rapporti *business to consumer*).

Quale che sia il contesto negoziale specifico, l'art. 2 contempla due diverse ipotesi che segnano i confini di estensione temporale della normativa perché il legislatore fa riferimento sia a futuri contratti (parla a tal fine di "stipulazione") sia a rapporti già in essere in forza di precedenti pattuizioni che siano oggetto di "rinnovo" per i quali è vietato richiedere informazioni dotate di precise caratteristiche qualitative e quantitative. Nel primo senso il divieto opera solo se queste riguardino patologie oncologiche (si presume dunque che diverse patologie non siano soggette al medesimo divieto) e, nel secondo caso, a condizione che sia decorso un pre-individuato lasso temporale in assenza di recidiva.

Come detto, il requisito temporale viene individuato nel medesimo comma, in una durata decennale salvo il caso di patologia insorta entro il ventunesimo anno di età ove il periodo viene dimezzato. Si deve tener conto poi del Decreto 22 marzo 2024 del Ministero della Salute che (a ciò espressamente autorizzato dall'art. 5, co. 2 della legge 193/2023) integra la legge in commento, riportando un elenco di patologie per le quali è previsto un termine ridotto per il maturarsi del diritto all'oblio oncologico rispetto al limite decennale o quinquennale.

Dunque, in base al tipo di malattia oncologica, la durata del periodo utile ad escludere la richiesta di informazioni in merito, sarà quella dell'art. 2 della legge 193 ovvero quella del decreto richiamato. L'importanza della legge si coglie se si tiene conto del fatto che il fulcro dell'accessibilità al mercato dei servizi finanziari e del credito è indubbiamente rappresentato dal merito creditizio e dalla storia assicurativa e dal bisogno degli intermediari di acquisire informazioni che tuttavia possono risultare fonte di discriminazione laddove si utilizzino per escludere dal credito o dalla copertura il soggetto o per imporre condizioni più onerose o svantaggiose. L'imposizione quindi in capo all'intermediario dell'obbligo di non assumere informazioni rispetto alle eventuali patologie oncologiche, dalle quali il cliente (o potenziale cliente) sia guarito si traduce in una volontà di correggere fattori di discriminazione.

Quanto al divieto menzionato, il combinato disposto del primo e dell'ultimo capoverso del primo comma dell'art.2 ne dettaglia il contenuto: non è ammessa la richiesta di informazioni sulla pregressa malattia né al diretto interessato né per mezzo dell'assunzione da fonti diverse con un collegato ulteriore divieto di utilizzo di quelle già in possesso dell'operatore o dell'intermediario.

Tale previsione è integrata dal divieto del quarto comma dell'art.2 ove è altresì vietata la richiesta di effettuare visite mediche se orientate ad acquisire informazioni propedeutiche alla conclusione del contratto.

In questo quadro va altresì richiamato il quinto comma dell'art. 2 che prende in considerazione l'ipotesi in cui l'intermediario sia già in possesso delle informazioni: in tal caso, a fronte di una apposita comunicazione inviata dal cliente che accerta la sussistenza dei requisiti necessari ai fini dell'applicazione della legge in commento, è previsto un obbligo di

ISSN 2239-8570

cancellazione delle informazioni oncologiche già archiviate a cui provvedere entro trenta giorni dal ricevimento della suddetta certificazione.

Il legislatore dunque, nel terzo comma dell'art. 2, rende ancor più forte la protezione del cliente intervenendo sull'autonomia privata mediante l'espressa esclusione della possibilità di applicare limiti, costi e oneri aggiuntivi, o trattamenti diversi rispetto a quelli previsti per le generalità dei contraenti.

Con il secondo comma dell'art.2, le prescrizioni gravanti sugli operatori del mercato creditizio ed assicurativo hanno anche un contenuto positivo: si sancisce infatti un preciso obbligo informativo sul diritto all'oblio nei servizi bancari, finanziari ed assicurativi. Non si tratta di un generico obbligo poiché il legislatore si preoccupa di dettagliarne l'applicazione temporale, non solo usando la locuzione "in tutte le fasi di accesso ai servizi" ma avendo cura di richiamare espressamente fasi quali quelle delle trattive precontrattuali, della stipula e del rinnovo del contratto.

Richiede inoltre che le informazioni siano "adeguate" e rispettino precisi requisiti formali quali l'espressa menzione nei moduli e formulari utilizzati. Va rilevato altresì come la portata della previsione si inserisca a pieno titolo nell'ampio spettro di obblighi informativi a cui sono già tenuti gli intermediari in ambito creditizio ed assicurativo e che si ritiene, debbano essere integrate anche delle suddette informazioni. L'impatto di una loro eventuale violazione è del resto degna di nota se si considera il quadro di conseguenze disegnato dal sesto comma dell'art.2 ove si precisa come «*la violazione delle disposizioni di cui ai commi da 1 a 5 determina la nullità delle singole clausole contrattuali difformi rispetto ai principi di cui al comma 1 e di quelle a esse connesse e non comporta la nullità del contratto, che rimane valido ed efficace per il resto*».

Da notare come vengano equiparate tutte le ipotesi dell'art.2 per cui la sanzione della nullità opererà ogni qualvolta siano state assunte informazioni ovvero siano state trattate o non siano state cancellate informazioni già possedute o ancora non si sia provveduto all'onere informativo prescritto.

Si tratta evidentemente di una nullità a tutela della parte debole del rapporto che sembra così assumere un valore "di protezione".

Essa opera solo a favore della persona fisica per cui deve ritenersi che il sistema dell'art.2 fatto di divieti ed obblighi si applichi alla generalità dei contraenti laddove invece la nullità sarà invocabile nel solo caso del contraente persona fisica.

Essa sarà altresì rilevabile d'ufficio (in ogni stato e grado del procedimento) e ad inefficacia "parziale" così scongiurando l'invalidità dell'intero accordo contrattuale poiché destinata a colpire solo i profili che siano frutto di una delle violazioni richiamate purchè confluite in clausole "difformi" o "connesse".

Il richiamo anche al comma 2 dell'articolo, farebbe pensare ad una nullità invocabile anche nel caso in cui sia stato violato l'obbligo informativo a condizione che ciò abbia però comportato la presenza nel contratto di clausole contrarie alla normativa in esame.

ISSN 2239-8570

Quanto sopra salvo dettagli che il comma settimo, in chiusura dell'articolo, rimette al Comitato interministeriale per il credito e il risparmio e all'Istituto per la vigilanza sulle assicurazioni, in entrambi i casi sentito il Garante per la protezione dei dati personali.

Nelle more dell'adozione di questi provvedimenti, come precisato dall'art. 5, i contratti bancari, finanziari e assicurativi stipulati dopo la data di entrata in vigore della legge in commento, devono conformarsi ai principi ivi introdotti, a pena di nullità delle singole clausole contrattuali.

Merita da ultimo menzionare il quarto comma dell'art. 5 che stabilisce come competente per la vigilanza sull'applicazione della legge 193/23 sia il Garante per la protezione dei dati personali, previsione questa che rende necessario proporsi la questione del coordinamento di competenze tra Autorità evidentemente coinvolte dalla natura negoziale degli obblighi connessi al diritto all'oblio oncologico oltre che da prerogative di vigilanza espressamente previste dalla legge nei settori a cui si rivolge l'art. 2.

RAFFAELLA GRISAFI

Legge 193/2023:
https://www.gazzettaufficiale.it/eli/id/2023/12/18/23G00206/sg

Decreto 22 marzo 2024 del Ministero della Salute:
https://www.gazzettaufficiale.it/eli/id/2024/04/24/24A02057/SG

2024/2(22)CAT

22. La modifica dell'art. 110 del Codice privacy sul trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico (DL 19/2024) e il provvedimento n. 298 del 9 maggio 2024 del Garante privacy sulle regole deontologiche

L'art. 9(4) del regolamento (UE) 679/2016 (**GDPR**) prevede che gli Stati membri possano introdurre ulteriori disposizioni, rispetto a quelle previste dallo stesso GDPR, con riguardo al trattamento di dati genetici, biometrici o relativi alla salute.

In virtù di tale competenza, il legislatore italiano è intervenuto con il D.lgs 101/2018 introducendo l'art. 110 D.lgs. 30 giugno 2003, n. 196 (**Codice privacy**) al fine di disciplinare la ricerca medica, biomedica ed epidemiologica. Tale articolo, prima della recente modifica, manteneva come regola generale per "il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico" il requisito dell'ottenimento del consenso dell'interessato, ammettendo tuttavia deroghe a tale base giuridica laddove: (a) vi fosse una disposizione di legge o di regolamento a copertura del progetto di ricerca e fosse resa pubblica una valutazione d'impatto sulla protezione dei dati personali; o (b) informare gli interessati risultasse impossibile, comportasse uno sforzo

ISSN 2239-8570

sproporzionato o pregiudicasse gravemente la finalità di ricerca. In tale ultimo caso, oltre al parere del comitato etico, era necessario che il progetto di ricerca fosse sottoposto a preventiva consultazione presso il Garante per la protezione dei dati personali (il **Garante** o l'**Autorità**) ai sensi dell'art. 36 GDPR.

Proprio su quest'ultimo aspetto, che non poche criticità ha creato nello sviluppo dei progetti di ricerca, il legislatore italiano è intervenuto con l'art. 44, comma 1-bis della legge 29 aprile 2024, n. 56 di conversione in legge, con modificazioni, del decreto-legge 2 marzo 2024, n. 19 (il **DL 19/2024**). La disposizione introduce una modifica significativa, eliminando l'obbligo per i titolari del trattamento di consultare preliminarmente il Garante, in conformità all'art. 36 GDPR, quando il consenso degli interessati non può essere ottenuto per ragioni specifiche, come l'impossibilità di raggiungerli o l'eccessiva onerosità di tale operazione. Al contrario, i titolari dovranno rispettare le garanzie che l'Autorità è chiamata a definire ai sensi dell'art. 106(2)(d) Codice privacy, coinvolgendo gli operatori di settore.

Con il Provvedimento n. 298 del 9 maggio 2024, il Garante Privacy ha dunque individuato le prime garanzie da adottare per il trattamento dei dati personali a scopo di ricerca medica, biomedica e epidemiologica, riferiti a pazienti deceduti o non contattabili e ha, contestualmente, promosso l'avvio della procedura per l'adozione delle suddette regole deontologiche, invitando i soggetti pubblici e privati, che intendano partecipare ai lavori, a darne comunicazione e a fornire informazioni e documentazione entro 60 giorni.

Tali misure che il Garante definirà avranno come obbiettivo il rispetto del principio di minimizzazione dei dati, favorendo l'uso di tecniche come la pseudonimizzazione per ridurre al minimo i rischi per i diritti e le libertà degli interessati, senza compromettere gli obiettivi della ricerca.

Recentemente, è stato evidenziato da alcuni commentatori un potenziale conflitto tra la modifica citata e l'articolo 8 del disegno di legge governativo (DDL) che introduce disposizioni nazionali in materia di Intelligenza Artificiale (IA). Tuttavia, quest'ultima disposizione riguarda esclusivamente i trattamenti di dati per la ricerca e la sperimentazione scientifica nella creazione di sistemi di intelligenza artificiale nel settore sanitario, in quanto necessari per la realizzazione e l'uso di banche dati e modelli di base, dichiarandoli di rilevante interesse pubblico. Pertanto, l'articolo 8 non copre la ricerca medica in generale, escludendo almeno i progetti di sperimentazione clinica non finalizzati alla realizzazione di sistemi di IA.

Concludendo, la recente revisione normativa introdotta dal DL 19/2024, oltre a essere più in linea con il principio di accountability sancito dall'art. 5 GDPR, rappresenta un passo rilevante verso la semplificazione delle procedure nel campo della ricerca medica e risponde alla necessità di mantenere l'Italia competitiva a livello internazionale in tale settore, riducendo il peso degli adempimenti burocratici percepiti come ostacoli dagli operatori del settore.

CARMINE ANDREA TROVATO

ISSN 2239-8570

Codice privacy
Provvedimento Garante n. 298 del 9 maggio 2024
Comunicato stampa Garante

2024/2(23)MS

23. Promulgata la legge 28 giugno 2024, n. 90 *Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*

Il 2.7.2024 è stata pubblicata nella Gazzetta Ufficiale la legge 28.6.2024, n. 90 recante Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (innanzi la **Legge sulla cybersicurezza** o la **Legge**). La Legge, ponendosi nel solco del d.l. 14.6.2021 convertito nella legge 4.8.2021 n. 109 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale) contiene disposizioni che incidono su molte materie, comprese disposizioni di diritto e procedura penale. Qui di seguito riferiremo succintamente di una serie di misure poste dalla Legge alla pubblica amministrazione, volte a prevenire e contrastare il compimento di reati informatici che possano compromettere interessi nazionali strategici, nonché di un ampliamento di delega conferita dalla Legge al Governo nella materia della resilienza operativa digitale nel settore finanziario.

Innanzitutto la nozione di pubblica amministrazione (di seguito **PA**) utilizzata dalla Legge include le pubbliche amministrazioni centrali (vale a dire quelle incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge n. 196 del 2009 (Legge di contabilità e finanza pubblica), le regioni e le province autonome di Trento e di Bolzano, le città metropolitane, i comuni con popolazione superiore a 100.000 abitanti, i comuni capoluoghi di regione, le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti, le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane, le aziende sanitarie locali, le società *in house* dei predetti enti (qualora le stesse società siano fornitrici di servizi informatici, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, ovvero di servizi di gestione dei rifiuti).

A ciascuna delle predette PA la Legge sulla cybersicurezza chiede di adempiere ad un vero e proprio "**obbligo di resilienza**", consistente, per un verso, nella immediata ("senza ritardo e comunque entro il termine massimo di ventiquattro ore") segnalazione all'Agenzia per la cybersicurezza nazionale (di seguito **ACN**) di qualunque incidente indicato "nella tassonomia di cui all'articolo 1, comma 3 bis, del d.l. 21.9.2019, n.105, convertito, con modificazioni, dalla legge 18.11.2019, n. 133 (Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica), aventi

ISSN 2239-8570

impatto su reti, sistemi informativi e servizi informatici" (sulla determina dell'ACN del 3.1.2023 sulla tassonomia degli incidenti informatici da notificare v. in questa Rubrica la notizia n. 17 del numero 1/2023 [2023/1(17)ES]). Per altro verso, nella effettuazione "entro settantadue ore a decorrere dal medesimo momento" della notifica completa all'ACN "di tutti gli elementi informativi disponibili". L'accertamento del ritardo o dell'omissione (della predetta notifica) da parte dell'ACN potrà comportare l'invio, da parte di quest'ultima, "nei dodici mesi successivi" di ispezioni presso la PA rimasta inerte "anche al fine di verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi".

Ma non solo. Nel momento stesso in cui l'ACN avrà contezza del ritardo o dell'omissione della notifica, la stessa Agenzia comunicherà alla PA resasi inadempiente che la reiterazione dell'inosservanza, nell'arco di cinque anni, comporterà l'applicazione della sanzione amministrativa pecuniaria da euro 25.000 a euro 125.000 a carico della stessa PA.

Non tutte le PA, però, saranno tenute ad effettuare la predetta segnalazione all'ACN. Ne saranno infatti esentati: a) i soggetti di cui all'articolo 3, comma 1, lettere g) e i), del d.lgs. 18 5.2018, n. 65 (vale a dire taluni fornitori, pubblici o privati, di servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali, la cui fornitura dipenda dalla rete e dai sistemi informativi e i fornitori di servizi digitali), e quelli di cui all'articolo 1, comma 2-bis, del d.l. 21.9.2019, n. 105, convertito, con modificazioni, dalla legge 18.11.2019, n. 133 (enti e operatori, pubblici o privati, inclusi nel perimetro di sicurezza nazionale cibernetica); e b) gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4,6 e 7 della legge 3.8.2007, n. 124.

Quanto sinora detto attiene alla notifica di incidenti verificatisi sulla rete e sui sistemi informativi. Per il caso invece in cui sia l'ACN, nella propria attività di valutazione del rischio, a venire a conoscenza di circostanze o eventi potenzialmente lesivi della sicurezza della rete e dei sistemi informativi di una o più PA, la Legge sulla cybersicurezza prevede che la ACN possa segnalare alla PA interessata l'esistenza di *"specifiche vulnerabilità"*, con conseguente obbligo di quest'ultima di adottare gli interventi risolutivi "indicati dalla stessa Agenzia" senza ritardo e comunque "non oltre quindici giorni dalla comunicazione". In caso di inottemperanza all'adozione di detti interventi risolutivi si applicheranno le anzidette sanzioni previste per l'ipotesi di mancata, o ritardata, notifica di incidenti riguardanti reti, sistemi informativi e servizi informatici.

La Legge sulla cybersicurezza assegna all'ACN anche i compiti di raccolta, elaborazione e classificazione, dei dati relativi alle notifiche di incidenti ricevute, e prevede che tali dati siano resi pubblici mediante la relazione annuale del Presidente del Consiglio dei ministri al Parlamento in materia di cybersicurezza nazionale.

Il nucleo centrale delle modifiche introdotte dalla Legge sulla cybersicurezza in materia di *governance* è rappresentato dalla previsione

ISSN 2239-8570

dell'obbligo di ogni PA di dotarsi, ove non già presente, di una struttura per la cybersicurezza, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente. Tale struttura, che potrà essere individuata anche in quella dell'ufficio del responsabile per la transizione al digitale, dovrà provvedere: "a) allo sviluppo delle politiche e delle procedure di sicurezza delle informazioni; b) alla produzione e all'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico; c) alla produzione e all'aggiornamento di un documento che definisca i ruoli e l'organizzazione del sistema per la sicurezza delle informazioni dell'amministrazione; d) alla produzione e all'aggiornamento di un piano programmatico per la sicurezza di dati, sistemi e infrastrutture dell'amministrazione; e) alla pianificazione e all'attuazione di interventi di potenziamento delle capacità per la gestione dei rischi informatici, in coerenza con i piani di cui alle lettere b) e d); f) alla pianificazione e all'attuazione dell'adozione delle misure previste dalle linee guida per la cybersicurezza emanate dall'Agenzia per la cybersicurezza nazionale; g) al monitoraggio e alla valutazione continua delle minacce alla sicurezza e delle vulnerabilità dei sistemi per il loro pronto aggiornamento di sicurezza".

Presso ciascuna delle predette strutture opererà "il referente per la cybersicurezza" (è peraltro previsto che, qualora la singola pubblica amministrazione non disponga di personale dipendente fornito di tali requisiti, la stessa pubblica amministrazione possa conferire l'incarico di referente per la cybersicurezza a un dipendente di una pubblica amministrazione).

Come per gli obblighi di notifica e di adeguamento alle segnalazioni dell'ACN sopra indicati, anche per le predette misure di *governance* è previsto che le stesse non si applichino a) ai soggetti di cui all'articolo 3, comma 1, lettere g) e i), del d.lgs. 18.5.2018, n. 65 (vale a dire a taluni fornitori, pubblici o privati, di servizi essenziali per il mantenimento di attività sociali e/o economiche fondamentali, la cui fornitura dipenda dalla rete e dai sistemi informativi e i fornitori di servizi digitali), ed a quelli di cui all'articolo 1, comma 2-bis, del d.l. 21.9.2019, n. 105, convertito, con modificazioni, dalla legge 18.11.2019, n. 133 (enti e operatori, pubblici o privati, inclusi nel perimetro di sicurezza nazionale cibernetica); e b) agli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato e agli organismi di informazione per la sicurezza di cui agli articoli 4,6 e 7 della legge 3.8.2007, n. 124.

Altra novità saliente dettata dalla Legge sulla cybersicurezza è quella concernente il rafforzamento delle misure di sicurezza dei dati attraverso l'uso della crittografia. Viene infatti istituito il Centro nazionale di crittografia presso l'ACN e si attribuisce alle strutture preposte alle attività di cybersicurezza nelle PA la funzione di verificare che i programmi e le applicazioni informatiche e di comunicazione elettronica "rispettino le linee guida sulla crittografia nonché quelle sulla conservazione delle password adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e non comportino vulnerabilità note, atte a rendere disponibili e intelligibili a terzi i dati cifrati".

ISSN 2239-8570

In relazione al procedimento amministrativo sanzionatorio per l'accertamento e la contestazione delle violazioni in materia di cybersicurezza di competenza dell'ACN vengono inoltre anticipati termini e modalità della relativa disciplina che verrà adottata con regolamento "entro novanta giorni dalla data di entrata in vigore" della Legge sulla cybersicurezza.

Una serie di ulteriori disposizioni della Legge sulla cybersicurezza, sulle quali non ci soffermiamo, è dedicata al personale dell'ACN e degli organismi di informazione per la sicurezza, comprese disposizioni sull'incompatibilità.

La Legge introduce una nuova disciplina in riferimento ai contratti pubblici di beni e servizi informatici impiegati "in un contesto connesso alla tutela degli interessi nazionali strategici". Sul punto, la Legge sulla cybersicurezza demanda ad un successivo decreto del Presidente del Consiglio dei ministri l'individuazione - per specifiche categorie tecnologiche di beni e servizi informatici - degli elementi essenziali di cybersicurezza che "i soggetti di cui all'articolo 2, comma 2, del codice dell'amministrazione digitale, di cui al d.lgs. 7.3.2005, n. 82" dovranno tenere in considerazione "nelle attività di approvvigionamento di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici, nonché i casi in cui, per la tutela della sicurezza nazionale, dovranno essere previsti criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti all'Alleanza atlantica (NATO) o di Paesi terzi (che saranno individuati con l'adottando decreto del Presidente del Consiglio dei ministri, *ndr*) tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione".

Quanto agli "elementi essenziali di cybersicurezza" ne viene fornita la seguente nozione: "insieme di criteri e regole tecniche la conformità ai quali, da parte di beni e servizi informatici da acquisire, garantisce la confidenzialità, l'integrità e la disponibilità dei dati da trattare" in misura corrispondente alle anzidette esigenze di tutela.

Nello specifico le singole stazioni appaltanti: i) potranno esercitare "la facoltà di cui agli articoli 107, comma 2, e 108, comma 10, del codice dei contratti pubblici, di cui al decreto legislativo 31.3.2023, n. 36 (la facoltà di non aggiudicare l'appalto per le ipotesi ivi previste, *n.d.r.*), ove accertino che l'offerta non tenga in considerazione gli anzidetti elementi essenziali di cybersicurezza"; ii) terranno sempre in considerazione i predetti elementi essenziali di cybersicurezza nella valutazione dell'elemento qualitativo, ai fini dell'individuazione del miglior rapporto qualità/prezzo per l'aggiudicazione; iii) "nel caso in cui sia utilizzato il criterio del minor prezzo, ai sensi dell'articolo 108, comma 3, del codice di cui al d.lgs. n. 36 del 2023, inseriranno detti elementi di cybersicurezza tra i requisiti minimi dell'offerta; iv) "nel caso in cui sia utilizzato il criterio dell'offerta economicamente più vantaggiosa, ai sensi dell'articolo 108, comma 4, del codice di cui al d.lgs. n. 36 del 2023", nella valutazione dell'elemento

ISSN 2239-8570

qualitativo ai fini dell'individuazione del migliore rapporto qualità/prezzo, stabiliranno "un tetto massimo per il punteggio economico entro il limite del 10 per cento"; v) prevederanno "criteri di premialità per le proposte o per le offerte che contemplino l'uso di tecnologie di cybersicurezza italiane o di Paesi appartenenti all'Unione europea o di Paesi aderenti alla NATO o di Paesi terzi individuati (con l'adottando decreto del Presidente del Consiglio dei ministri, *ndr*) tra quelli che sono parte di accordi di collaborazione con l'Unione europea o con la NATO in materia di cybersicurezza, protezione delle informazioni classificate, ricerca e innovazione, al fine di tutelare la sicurezza nazionale e di conseguire l'autonomia tecnologica e strategica nell'ambito della cybersicurezza".

Dette novità in materia di contratti pubblici di beni e servizi informatici si applicheranno anche ai soggetti privati non compresi tra quelli di cui all'articolo 2, comma 2, del codice di cui al d.lgs. 7.3.2005, n. 82, e inseriti "nell'elencazione di cui all'articolo 1, comma 2-bis, del d.l. 21.9.2019, n. 105, convertito, con modificazioni, dalla legge 18.11.2019, n. 133" (soggetti privati comunque inclusi nel perimetro di sicurezza nazionale cibernetica).

Per quanto attiene alle modifiche concernenti **gli intermediari finanziari**, la Legge ha integrato la legge 21.2.2024 n. 15 (Legge di delegazione europea 2022-2023), e nello specifico il relativo art. 16, contenente la "delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/2554 (di seguito **DORA** da *Digital Operational Resilience Act*) relativo alla resilienza operativa digitale per il settore finanziario (sul DORA v. in questa Rubrica la notizia n. 3 del numero 4/2022 [2022/4(3)ES]). In particolare, in virtù di questa integrazione, al Governo viene altresì demandato il compito di "apportare alla disciplina applicabile agli intermediari finanziari iscritti nell'albo previsto dall'articolo 106 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, nonché alla società Poste italiane Spa per l'attività del Patrimonio Bancoposta, di cui al regolamento di cui al decreto del Presidente della Repubblica 14.3.2001, n. 144, le occorrenti modifiche e integrazioni, anche mediante la normativa secondaria di cui alla lettera d) del presente comma, per conseguire un livello elevato di resilienza operativa digitale e assicurare la stabilità del settore finanziario nel suo complesso, in particolare: 1) definendo presidi in materia di resilienza operativa digitale equivalenti a quelli stabiliti nel regolamento (UE) 2022/2554 [DORA] […]; 2) tenendo conto, nella definizione dei presidi di cui al numero 1), del principio di proporzionalità e delle attività svolte dagli intermediari finanziari e dal Patrimonio Bancoposta; 3) attribuendo alla Banca d'Italia l'esercizio dei poteri di vigilanza, di indagine e sanzionatori di cui alla lettera b) (dell'art. 16, comma 2 legge 21.2.2024 n. 15, *ndr*) nei confronti dei soggetti di cui alla presente lettera".

Nel Capo II della Legge, si trova una serie di disposizioni di **diritto penale**. Si tratta, tra le altre, delle disposizioni che prevedono aumenti di pena e introduzione di nuove circostanze aggravanti per il reato dell'accesso abusivo ad un sistema informatico o telematico di cui all'art. 615 ter c.p., l'abrogazione dell'art. 615 quinquies c.p. (Diffusione di apparecchiature,

ISSN 2239-8570

dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico), l'integrazione dell'ipotesi di procedibilità d'ufficio per il reato di cui all'art. 617 quater c.p. (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche) di cui al n. 2 del terzo comma (se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio) mediante il riferimento a chi eserciti "anche abusivamente, la professione di investigatore privato", l'introduzione di nuove ipotesi di circostanze attenuanti e di modifiche alla disciplina del reato di danneggiamento di informazioni, dati e programmi informatici "pubblici o di interesse pubblico" di cui all'art. 635 ter c.p., modifiche alla disciplina del reato di cui all'art. 635 quater c.p. (Danneggiamento di sistemi informatici o telematici), quanto alla circostanza aggravante del medesimo reato, la modifica dell'art. 635 quinquies c.p. (Danneggiamento di sistemi informatici o telematici di pubblico interesse).

Per quanto attiene alle **modifiche introdotte al codice di procedura penale** si segnala in particolare l'aggiunta del numero 7 ter al comma 2, lettera a), dell'art. 407 c.p.p., di modo che, con l'entrata in vigore della Legge sulla cybersicurezza le indagini preliminari potranno ora avere la durata massima di cui al citato comma 2 anche per i "delitti previsti dagli articoli 615-ter, 615-quater, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 635-quater.1 e 635-quinquies del codice penale, quando il fatto è commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico".

Relativamente alle funzioni di impulso esercitate dal procuratore nazionale antimafia nei confronti dei procuratori distrettuali ai sensi del comma 4 bis dell'art. 371 bis c.p.p. (introdotto dall'art. 2-bis, comma 3, lettera b) del d.l. 10.8.2023, n. 105, convertito con modificazioni dalla legge 9.10.2023, n. 137), la Legge sulla cybersicurezza interviene per renderne effettiva l'applicazione anche in relazione alla disciplina di cui al d.l. 15.1.1991, n. 8, convertito, con modificazioni, dalla legge 15.3.1991, n. 82 (Nuove norme in materia di sequestri di persona a scopo di estorsione e per la protezione dei testimoni di giustizia, nonché per la protezione e il trattamento sanzionatorio di coloro che collaborano con la giustizia), al d.l. 13.5.1991, n. 152, convertito, con modificazioni, dalla legge 12.7.1991, n. 203 (Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa), ed alla legge 11.1.2018 n. 6 (Disposizioni per la protezione dei testimoni di giustizia).

Si segnalano inoltre alcune **modifiche** introdotte dalla Legge sulla cybersicurezza **al d.lgs. 8.6.2001 n. 231** (**Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica**). In particolare viene aggravata la sanzione di cui al comma 1 dell'art. 24 bis (Delitti informatici e trattamento illecito di dati), che per l'ente responsabile dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater c.p. passa da duecento a settecento quote (anziché da cento a cinquecento quote).

ISSN 2239-8570

Infine la Legge interviene con alcune disposizioni relative al personale dell'ACN addetto al CSIRT, l'organo dell'ACN che si occupa di monitoraggio preventivo e risposta agli incidenti informatici (da *Computer Security Incident Response Team*), nonché con alcune modifiche alla normativa sull'organizzazione ed il funzionamento dell'Ispettorato generale presso il Ministero di grazia e giustizia in materia di sicurezza negli accessi alle banche dati.

MARCO SCALDAFERRI

Legge 28 giugno 2024, n. 90

2024/2(24)MVT

24. La designazione di AGCOM quale Coordinatore dei servizi digitali ai sensi del DSA (DL 123/2023)

Il 14 novembre 2023 è stata pubblicata nella Gazzetta Ufficiale della Repubblica Italiana la Legge 13 novembre 2023, n. 159 recante "*Conversione in legge con modificazioni del decreto-legge 15 settembre n. 123, recante misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale*" (di seguito il **DL 123/2023** anche solo il **Decreto**).

Nella disciplina del Capo IV del DL 123/2023, rubricato "*Disposizioni per la sicurezza dei minori in ambito digitale*" (su cui v. in questa Rubrica la notizia n. 9 nel numero 1/2024 [2024/1(9)SGh]), si trova anche l'art. 15, con il quale, al fine di garantire la vigilanza sull'attività dei fornitori di servizi intermediari operanti in ambito digitale e prevenire la diffusione di contenuti illegali *online*, è stata data attuazione all'art. 49 del regolamento (UE) 2022/2065 (di seguito anche **Digital Services Act** o **DSA**) (su cui v. in questa Rubrica notizia n. 1 del numero 4/2022 [2022/4(1)ST]).

L'art. 49 DSA impone agli Stati membri l'obbligo di designare "*una o più autorità competenti incaricate della vigilanza dei fornitori di servizi intermediari e dell'esecuzione del presente regolamento*". Con l'art. 15(1) DL 123/2023, lo Stato italiano ha designato l'Autorità per le garanzie nelle comunicazioni (**AGCOM**) quale Coordinatore dei Servizi Digitali, ai sensi dell'art. 49 DSA.

L'AGCOM, pertanto, è, in virtù di questa designazione, responsabile della vigilanza e dell'applicazione del *Digital Services Act* nel territorio italiano.

Il Coordinatore dei servizi digitali, ai sensi dell'art. 15(3) DL 123/2023, definisce con proprio provvedimento le condizioni, le procedure e le modalità operative per l'esercizio delle funzioni di cui è titolare, agendo in modo imparziale, trasparente e tempestivo. Il garantire l'effettività dei diritti e l'efficacia degli obblighi stabiliti dal *Digital Services Act* è un compito particolarmente importante, soprattutto quando è in gioco la protezione dei minori e il raggiungimento di obiettivi quali, per esempio, la prevenzione

ISSN 2239-8570

della diffusione di contenuti pornografici disponibili *online* e, in generale, di altri contenuti illegali o comunque vietati.

Nello svolgere l'attività di Coordinatore dei Servizi digitali, l'AGCOM si avvale della collaborazione dell'Autorità garante della concorrenza e del mercato (**AGCM**), del Garante per la protezione dei dati personali (il **Garante privacy**) e di ogni altra Autorità nazionale competente. Gli aspetti applicativi e procedimentali della reciproca collaborazione sono disciplinati attraverso dei protocolli di intesa stilati tra le Autorità medesime (art. 15(2) DL 123/2023).

Il potere sanzionatorio, per il caso di violazione delle prescrizioni del *Digital Services Act,* è conferito agli Stati Membri dall'art. 52 DSA. Pertanto, l'art. 15(4) DL 123/2023 ha apportato alcune modifiche alla legge istitutiva dell'AGCOM, la legge 31 luglio 1997, n. 249, tra le quali l'introduzione del comma 32 *bis* nell'art. 1 della medesima legge, in questo modo attribuendo all'AGCOM il potere di applicare sanzioni amministrative in conseguenza della violazione degli obblighi di cui agli articoli 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 26, 27, 28, 30 e 45 del *Digital Services Act.*

In particolare, il richiamo è alla violazione degli obblighi di contestare i contenuti illegali; ordini di fornire informazioni; obblighi in materia di dovere di diligenza per un ambiente *online* trasparente e sicuro; obblighi relativi al sistema di gestione dei reclami e alla risoluzione extragiudiziale delle controversie; obblighi di comunicazione trasparente per i fornitori di piattaforme *online*; obblighi relativi alla pubblicità sulle piattaforme *online*; alla trasparenza dei sistemi di raccomandazione; alla protezione *online* dei minori e alla tracciabilità degli operatori commerciali e codici di condotta.

Il Coordinatore dei Servizi digitali ha il potere di applicare, con proprio provvedimento e in conformità ai principi di proporzionalità, adeguatezza e rispetto del contraddittorio, sanzioni amministrative pecuniarie fino ad un massimo del 6% del fatturato annuo mondiale nell'esercizio finanziario precedente alla comunicazione di avvio del procedimento al prestatore di un servizio intermediario.

In caso di informazioni inesatte, incomplete o fuorvianti e di inosservanza, da parte dell'intermediario dei servizi digitali, dell'obbligo di sottoporsi a un'ispezione, all'Autorità per le garanzie nelle comunicazioni è riconosciuto il potere di applicare, in conformità al combinato disposto di cui agli articoli 51 e 52 DSA, una sanzione amministrativa pecuniaria fino ad un massimo dell'1% del fatturato mondiale realizzato nell'esercizio finanziario precedente.

L'importo massimo giornaliero delle penalità di mora che l'Autorità per le garanzie nelle comunicazioni può applicare è pari al 5% del fatturato giornaliero medio mondiale del fornitore di un servizio intermediario interessato, realizzato nell'esercizio finanziario precedente.

Le sanzioni sono applicate dalla stessa Autorità ai prestatori di servizi intermediari nell'esercizio dei poteri che le vengono conferiti dagli articoli 51 e 52 DSA.

Nell'applicazione della sanzione, l'AGCOM deve tener conto della gravità del fatto e delle conseguenze che ne sono derivate, nonché della

ISSN 2239-8570

durata e dell'eventuale reiterazione della violazione. È escluso il beneficio del pagamento in misura ridotta della sanzione ai sensi dell'art. 6 L. 24 novembre 1981, n. 689.

Per quanto attiene alle misure organizzative, l'art. 15(5) DL 123/2023 incrementa la pianta organica dell'AGCOM di 23 unità, specificando le relative qualifiche, determina gli oneri da ciò derivanti per i prossimi 10 anni, e prevede che a tali oneri si provvede mediante un contributo di importo pari allo 0,135 per mille del fatturato risultante dall'ultimo bilancio approvato dai prestatori dei servizi intermediari stabiliti in Italia, così come definiti dal DSA, e individuati dall'AGCOM con la collaborazione dell'Istituto nazionale di statistica e dell'Agenzia delle Entrate.

MARIA VITTORIA TRINCHERA

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2023;159

2024/2(25)FB

25. La sentenza n. 69/2024 della Corte Costituzionale sulla illegittimità costituzionale di una disposizione di una legge regionale in materia di sistemi di videosorveglianza in strutture di cura

La decisione in sintesi

Con la sentenza n. 69, decisa il 20.3.2024 e pubblicata in Gazzetta Ufficiale il 24.4.2024, la Corte costituzionale ha ribadito (come aveva già fatto originariamente con la sentenza n. 271 del 2005 e da ultimo con la sentenza n. 177 del 2020) che la protezione degli individui con riguardo al trattamento dei loro dati personali rientra nella materia dell'«ordinamento civile» di competenza esclusiva dello Stato, ai sensi dell'articolo 117, secondo comma, lettera *l)*, della Costituzione. La protezione dei dati personali è ricondotta a tale materia poiché essa riguarda il riconoscimento di una serie di diritti alle persone fisiche e giuridiche (*sic*) relativamente ai propri dati; ivi includendo tanto le norme sostanziali che disciplinano la raccolta e il trattamento dei dati personali, quanto i diritti, di cui sono regolate analiticamente caratteristiche, limiti, modalità di esercizio, garanzie, nonché le forme di tutela in sede amministrativa e giurisdizionale delle situazioni soggettive del settore.

Nel caso di specie, è stata dichiarata costituzionalmente illegittima la norma di cui all'art. 3 della legge regionale della Puglia n. 123 del 2023, che regola «l'installazione di sistemi di videosorveglianza e la tutela della privacy» nelle strutture socio-sanitarie e socio-assistenziali al fine di prevenire e contrastare condotte di maltrattamento o abuso, anche psicologico, nei confronti di anziani e persone con disabilità. L'invasione della competenza legislativa statale da parte della Regione si manifesta già con l'introduzione di nuove fonti, che nel tempo possono essere modificate e integrate dai legislatori competenti.

ISSN 2239-8570

La censura costituzionale è mossa anche con riferimento al primo comma dell'articolo 117 della Costituzione, quest'ultimo in relazione al Regolamento (UE) 679/2016 quale norma interposta, in quanto l'Unione europea, nell'esercizio della sua competenza in materia di protezione delle persone fisiche riguardo al trattamento e alla libera circolazione dei dati personali, stabilita dall'art. 16 del TFUE, ha ampiamente regolamentato la materia, lasciando peraltro agli Stati membri solo limitati spazi normativi.

La Consulta ha rilevato come la complessità e l'ampiezza dei profili implicati nel trattamento dei dati personali richiedano delicati bilanciamenti tra diritti di rango inviolabile. La disposizione regionale censurata, pertanto, viola i vincoli derivanti dall'Unione europea ed invade la competenza legislativa esclusiva dello Stato in materia di ordinamento civile, sovrapponendosi con previsioni autonome e un rinvio selettivo al delicato intreccio di fonti europee e statali che regolano la materia.

Il ricorso

La Presidenza del Consiglio dei ministri ha promosso il giudizio di legittimità costituzionale dell'articolo 3 della legge della Regione Puglia 15 giugno 2023, n. 13, recante «Disposizioni per prevenire e contrastare condotte di maltrattamento o di abuso, anche di natura psicologica, in danno di anziani e persone con disabilità e modifica alla legge regionale 9 agosto 2006, n. 26 (Interventi in materia sanitaria)», con riferimento all'articolo 117, secondo comma, lettera *l)*, della Costituzione, in quanto la contestata norma regionale:

- invade la materia dell'ordinamento civile con riguardo alla protezione dei dati personali, introducendo una disciplina di dettaglio attraverso disposizioni precise in merito a: l'installazione dei sistemi di videosorveglianza, che deve essere effettuata in modo tale da garantire la sicurezza dei dati trattati e proteggerli da accessi non autorizzati; la necessità di ottenere il consenso degli ospiti o dei loro tutori prima dell'attivazione degl'impianti; l'obbligo di segnalare adeguatamente la presenza dei sistemi di videosorveglianza a tutti i soggetti che accedono alle aree interessate; l'esecuzione delle registrazioni, che deve avvenire in modalità criptata; e la visione delle registrazioni, che è riservata esclusivamente all'autorità giudiziaria;

- menziona in modo generico e sporadico solo alcune delle norme nazionali e sovra-nazionali di riferimento (*i.e.* il decreto legislativo n. 101 del 2018 ed il regolamento (UE) 2016/679, il "GDPR"), ignorando invece tutti gli strumenti normativi rilevanti;

- richiama le succitate fonti superiori esclusivamente con riferimento alla fase d'installazione dei sistemi di videosorveglianza;

- evoca la mera necessità del consenso degli ospiti (o dei loro tutori), senza specificare le modalità con cui tale consenso debba essere prestato, né le caratteristiche che deve possedere, non specificando, inoltre, il limite temporale di conservazione delle videoriprese;

- ignora la posizione degli operatori delle RSA e le garanzie loro offerte, in particolare, dall'articolo 4 dello Statuto dei lavoratori (come modificato da due dei provvedimenti della riforma nota complessivamente come *Jobs Act*, ossia il Decreto legislativo 151/2015, e il Decreto legislativo 185/

ISSN 2239-8570

2016), che regola le condizioni per l'ammissibilità dei controlli a distanza sui lavoratori nei luoghi di lavoro.

La Regione sarebbe pertanto intervenuta in un ambito riservato al Legislatore statale, a cui soltanto compete il bilanciamento degl'interessi giuridici in gioco (come già fissato dalla Corte nella sentenza n. 271 del 2005), violando conseguentemente il principio di proporzionalità, col disporre il ricorso ad uno strumento di monitoraggio particolarmente invasivo senza dimostrarne la sua adeguatezza e necessità in concreto.

Il Governo, ad ulteriore dimostrazione della competenza esclusiva del Legislatore statale, richiama due recenti norme nazionali che dispongono l'installazione di sistemi di videosorveglianza presso le strutture di assistenza per gli anziani, ed in particolare l'articolo 5-*septies*, comma 2, del decreto-Legge 18 aprile 2019, n. 32 (recante «Disposizioni urgenti per il rilancio del settore dei contratti pubblici, per l'accelerazione degl'interventi infrastrutturali, di rigenerazione urbana e di ricostruzione a seguito di eventi sismici», convertito, con modificazioni, nella Legge 14 giugno 2019, n. 55), che prevede un fondo destinato a finanziare l'installazione dei sistemi di videosorveglianza a circuito chiuso presso le strutture di residenza e cura degli anziani, e l'articolo 4, comma 2, lettera *r*), della Legge 23 marzo 2023, n. 33 (recante «Deleghe al Governo in materia di politiche in favore delle persone anziane», esercitate, poi con l'articolo 31 del decreto legislativo 15 marzo 2024, n. 29, recante «Disposizioni in materia di politiche in favore delle persone anziane, in attuazione della delega di cui agli articoli 3, 4 e 5 della Legge 23 marzo 2023, n. 33»), che annovera la presenza di sistemi di videosorveglianza a circuito chiuso fra i criteri di accreditamento e autorizzazione di tali strutture.

Oltre che per l'invasione della potestà legislativa in materia di «ordinamento civile», il Presidente del Consiglio dei ministri, rappresentato dall'Avvocatura generale dello Stato, eccepisce la violazione della lettera *l)* del secondo comma dell'articolo 117 della Costituzione, anche con riferimento all'«ordinamento penale», poiché la disposizione impugnata si limiterebbe ad attribuire all'autorità giudiziaria la sola competenza per l'accesso alle videoregistrazioni, senza rinviare all'intero quadro normativo di riferimento, che include anche il decreto legislativo 18 maggio 2018, n. 51, attuativo della Direttiva (UE) 2016/680, la quale detta la disciplina della protezione dei dati personali nell'ambito dei trattamenti effettuati per finalità di *law enforcement* da parte di tutte le autorità competenti.

L'Avvocatura generale dello Stato, sulla base della considerazione secondo la quale la disciplina del trattamento e della protezione dei dati personali è regolata principalmente da fonti dell'Unione europea, lamenta, infine, anche la violazione del primo comma dell'articolo 117 della Costituzione, in relazione ai già menzionati Regolamento (UE) 679/2016 e Direttiva (UE) 2016/680.

La difesa e la decisione sulle eccezioni d'inammissibilità formale del ricorso

La Regione Puglia, costituendosi in giudizio, ha sollevato tre eccezioni formali preliminari d'inammissibilità del ricorso.

ISSN 2239-8570

Con la prima ha contestato l'assenza, nella delibera del Consiglio dei ministri, di riferimenti al primo comma dell'articolo 117 della Costituzione e quindi alla violazione di vincoli derivanti dall'ordinamento europeo, eccependo pertanto un'eccedenza della censura contenuta nel ricorso dell'Avvocatura rispetto alla volontà dell'organo politico rappresentato. La Corte ha ritenuto tale eccezione infondata, valutando evidente dalla piana lettura della delibera del Consiglio dei ministri la manifesta volontà dell'organo politico di censurare il contrasto con gli espressamente menzionati vincoli derivanti dalle disposizioni del GDPR.

Con la seconda eccezione, la Regione rileva il mancato riferimento a "norme interposte" con riguardo all'«ordinamento civile», di cui all'articolo 117, secondo comma, lettera *l)*, della Costituzione e preliminarmente un'inadeguata individuazione della specifica materia rientrante nell'alveo di tale competenza legislativa. La Corte, oltre ad evidenziare l'uso improprio della locuzione "norma interposta" nell'ambito di una competenza legislativa statale esclusiva, ha ritenuto di disattendere anche tale secondo motivo d'inammissibilità proposto dalla Puglia, in quanto numerose sono le disposizioni di rango primario, costituenti espressione di tale competenza nella materia della protezione dei dati personali, ad essere contenute ed agevolmente rintracciabili nel ricorso. Peraltro, attraverso il puntuale e reiterato richiamo alla sentenza n. 271 del 2005, il Governo ha di fatto manifestamente specificato in quali termini considera il contenuto della norma regionale debordante nella materia «ordinamento civile».

Da ultimo, sempre sotto il profilo dell'ammissibilità formale del ricorso, la difesa regionale adduce l'inconferenza di tutti parametri costituzionali evocati dalla Presidenza del Consiglio (articolo 117, comma primo e comma secondo, lettera *l)*), ritenendo che una norma relativa all'installazione di impianti di videosorveglianza afferirebbe piuttosto alla materia dell'«ordine pubblico e sicurezza», di cui all'articolo 117, secondo comma, lettera *h)* o, in subordine, alla «tutela della salute», materia, questa, attribuita alla competenza legislativa concorrente delle Regioni dal terzo comma dello stesso articolo 117 della Costituzione. Ciò ha dato modo alla Consulta, nel rigettare come infondata anche quest'ultima eccezione preliminare, di pronunciarsi incidentalmente e ribadire (cfr. precedenti sentenze n. 163 del 2023, n. 132 del 2021 e n. 286 del 2019) che l'eventuale inconferenza del parametro indicato dal ricorrente rispetto al contenuto sostanziale della doglianza costituisce motivo di non fondatezza della questione, attenendo pertanto l'eccezione al merito e non al rito.

Nel merito, poi, la Regione Puglia afferma la necessità della norma impugnata, nata da urgenti ragioni contingenti di prevenzione da casi di maltrattamento e abuso a danno di anziani e disabili nelle strutture socio-sanitarie o assistenziali, e l'infondatezza delle questioni sollevate dal Governo. In risposta all'addebito di contrasto con la disciplina a difesa dal controllo a distanza dei lavoratori, la Regione sostiene che l'obbligo d'installazione della videosorveglianza nelle RSA, introdotto dal contestato articolo 3 della legge regionale, giova a quegli operatori sociosanitari che svolgono il loro lavoro con impegno e correttezza e la cui reputazione e

ISSN 2239-8570

professionalità vengono danneggiate dalle azioni di colleghi irresponsabili non sorvegliati.

In aggiunta, viene rilevato come, ai sensi dell'articolo 4 della stessa legge regionale, l'installazione degl'impianti di videosorveglianza è posto quale requisito necessario per l'accreditamento delle strutture private presso il Servizio sanitario regionale, nonché per conseguire o mantenere l'autorizzazione all'esercizio delle attività di assistenza socio-sanitaria (in perfetta continuità con il decreto-Legge n. 32 del 2019, come convertito, e con la Legge di delega n. 33 del 2023, richiamati dalla Presidenza del Consiglio dei ministri, i quali mostrano infatti il favore del Legislatore nazionale per l'adozione di sistemi di videosorveglianza da parte delle RSA per le medesima finalità di tutela contemplate dalla legge regionale in disamina, che quindi ne replica, a livello infra-nazionale, le prescrizioni), ad ulteriore conferma dell'inconferenza della disposizione impugnata con l'ambito del trattamento dei dati personali e della sua riconducibilità, invece, alla materia della «tutela della salute».

La difesa regionale asserisce quindi la conformità dell'articolo 3 alle disposizioni del GDPR, del Codice privacy (pur non richiamato dalla norma oggetto di esame costituzionale) e del decreto legislativo n. 101 del 2018 per ciascun profilo oggetto d'impugnazione. Mentre, per quanto riguarda la mancata menzione del decreto legislativo n. 51 del 2018, attuativo della Direttiva (UE) 2016/680, la Regione sostiene che tale disciplina inerisca al trattamento dei dati personali da parte delle autorità competenti a fini penali, collocandosi quindi al di fuori del perimetro applicativo dell'articolo impugnato.

Il merito della sentenza

La Corte Costituzionale introduce la questione richiamando i suoi noti precedenti (*in primis* la sentenza n. 271 del 2005 ed in senso analogo, anche la sentenza n. 177 del 2020) e così confermando l'afferenza della protezione delle persone con riguardo al trattamento dei dati personali alla materia «ordinamento civile», sia per quanto concerne le norme sostanziali, che disciplinano le modalità di trattamento dei dati, sia per quanto riguarda le tutele giurisdizionali e amministrative delle relative situazioni soggettive, che insieme riconoscono infatti una serie di diritti analiticamente disciplinati alle persone fisiche "e giuridiche" (così la Corte, nonostante l'intervenuta novazione apportata dall' art. 40, secondo comma, del decreto-Legge n. 201 del 6 dicembre 2011, convertito con Legge n. 214 del 22 dicembre 2011, che ha limitato tassativamente detta tutela alle sole persone fisiche) relativamente ai propri dati.

Si ha invasione della competenza legislativa statale già solo con l'introduzione di nuove fonti per materie che, nel tempo, potrebbero venire modificate ed integrate dai Legislatori competenti (come già espresso, fra le più recenti, dalla sentenza n. 239 del 2022 e, nella specifica materia dell'«ordinamento civile», dalle sentenze n. 153 del 2021 e n. 234 del 2017).

La Consulta ricostruisce quindi la «complessa trama di fonti», l'«articolato plesso normativo», l'«imponente corpo normativo», la «fitta disciplina eurounitaria e statale» di una «complessa e delicata materia» –

ISSN 2239-8570

che risulta, al contrario, alquanto chiara, piana e lineare –, riconoscendone la fonte primaria nel diritto dell'Unione europea, la quale, esercitando la competenza derivantele dall'articolo 16 del TFUE, ha ampiamente regolamentato la disciplina della protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e della libera circolazione degli stessi, lasciando invero limitati spazi d'intervento alla normazione degli Stati membri.

Viene pertanto escluso possa essere prerogativa della Regione operare, a sua discrezione, una selezione di fonti e disposizioni, come accade nella disciplina esaminata. Per ciò solo, la Regione non soltanto si sovrappone alla legislazione nazionale e sovra-nazionale, esuberando dalle proprie competenze, ma compie anche una cernita arbitraria, il cui effetto precettivo è quello di rendere vincolanti unicamente le disposizioni espressamente richiamate dal legislatore regionale, ma non le altre pur rilevanti. Non è pertanto privo di valore come il censurando articolo 3 abbia, in tale contesto, individuato quali fonti delle quali tenere conto il decreto legislativo n. 101 del 2018, il GDPR e la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, escludendo invece il Codice in materia di protezione dei dati personali o "Codice privacy" (Decreto legislativo 196/2003) - oggetto proprio delle modifiche di cui al decreto legislativo n. 101 del 2018-, lo Statuto dei lavoratori (legge 20 maggio 1970, n. 300), la Direttiva (UE) 2016/680 ed il decreto legislativo n. 51 del 2018, che le dà attuazione a nazionale.

Proprio l'omesso riferimento al Codice, a detta della Corte – che così risponde ad una espressa questione sollevata dall'Avvocatura –, esclude il rinvio al suo articolo 114, il quale a Sua volta richiama l'articolo 4 dello Statuto dei lavoratori, che detta le condizioni dell'installazione di impianti audiovisivi dai quali possa derivare un controllo a distanza dell'attività dei lavoratori, vale a dire proprio una fattispecie ricompresa nell'azione normativa del Legislatore regionale.

Sostanzialmente, come già puntualizzato dalla sentenza n. 271 del 2005, la Corte costituzionale rinviene il contrasto con i vincoli derivanti dall'Unione europea (primo comma dell'articolo 117 della Costituzione) e con la competenza legislativa esclusiva dello Stato (secondo comma dell'articolo 117 della Costituzione) tanto nel caso di rinvii parziali, quanto allorché una specifica normativa individui soltanto una porzione limitata di fonti, trascurando tutte le altre, che pure integrano il plesso normativo di riferimento.

Scendendo poi nello specifico, la Consulta evidenzia come la videosorveglianza presso le strutture socio-sanitarie e socio-assistenziali tocchi due ambiti particolarmente delicati: da un lato, essa comporta un monitoraggio che include la raccolta e il trattamento di dati sensibili riguardanti persone anziane, malate o disabili, con inevitabili ricadute sulla riservatezza e la dignità dei medesimi individui vulnerabili; dall'altro lato, come anticipato, implica un controllo sull'attività lavorativa del personale operante all'interno delle strutture sottoposte a videosorveglianza (medici, infermieri, operatori socio-sanitari, personale amministrativo, addetti alle pulizie e altri, nonché di eventuali lavoratori esterni la cui attività si svolge,

ISSN 2239-8570

in tutto o in parte, presso le stesse strutture). In considerazione delle complessità e ampiezza dei profili così coinvolti nel trattamento dei dati personali e che richiedono delicati bilanciamenti tra diritti spesso di rango inviolabile, l'intervento della Regione da un lato viola i vincoli imposti dall'Unione europea e dall'altro ingerisce nella competenza legislativa esclusiva dello Stato, sovrapponendosi con proprie previsioni autonome e selettive al delicato intreccio di fonti statali ed europee.

La Corte ha pertanto ritenuto che una disciplina simile non possa essere legittimamente ricondotta – come invece ha sostenuto la difesa della Regione Puglia – all'esercizio della competenza legislativa regionale concorrente nella materia della «tutela della salute». Ciò potrebbe valere solo in riferimento all'articolo 4 della stessa legge regionale Puglia n. 13 del 2023, che prevede l'installazione degl'impianti di videosorveglianza come requisito essenziale per l'accreditamento o l'autorizzazione all'esercizio delle attività socio-sanitarie e socio-assistenziali (in modo conforme anche alle normative di livello statale già evocate, che hanno incluso i sistemi di videosorveglianza a circuito chiuso tra i criteri per l'accreditamento e l'autorizzazione delle strutture socio-sanitarie e socio-assistenziali per anziani ed hanno istituito un fondo per finanziarne l'installazione). Tanto è più vero che l'accoglimento delle questioni sollevate sull'articolo 3 non inciderà, nel dettame della Corte sull'onere d'installare impianti di videosorveglianza, previsto dall'articolo 4, purché l'installazione sia effettuata nel pieno rispetto di tutte le previsioni dettate dall'Unione europea e dal Legislatore statale, nel campo della videosorveglianza e del trattamento dei dati personali.

Al contrario, la competenza legislativa concorrente nella materia della «tutela della salute» non può affatto considerarsi pertinente rispetto all'articolo 3 della legge regionale in questione, poiché tale competenza autorizzerebbe la Regione a prevedere un obbligo d'installazione degl'impianti di videosorveglianza, rinviando semmai al necessario rispetto della normativa europea e nazionale in materia di videosorveglianza e trattamento dei dati personali, ma non le consente certamente di scegliere selettivamente le relative fonti e d'individuare autonomamente le norme rilevanti.

La Consulta, riprendendo un esplicito rilievo del ricorso, sottolinea inoltre come tutte le fonti richiamate delineano una regolamentazione della videosorveglianza articolata in diverse fasi: dalle condizioni che ne consentono l'installazione, agli strumenti e modalità di raccolta dei dati; dall'informativa preliminare, al consenso degl'interessati (la Corte, testualmente, li definisce "titolari"); dal successivo trattamento dei dati, all'accesso ai supporti contenenti tali dati e alla loro utilizzazione. I commi 1 e 4 del contestato articolo 3 della legge regionale, invece, che prevedono rispettivamente l'autonoma installazione delle telecamere da parte delle strutture private con mera comunicazione alle aziende sanitarie locali, e una semplice segnalazione dei sistemi di videosorveglianza a tutti gl'individui che accedono all'area, omettono di considerare l'insieme di norme che, a livello europeo e statale, oltre a richiedere generalmente il consenso di tutti i soggetti i cui dati vengono trattati, disciplinano in dettaglio: l'informativa; le

ISSN 2239-8570

modalità di raccolta del consenso e le sue caratteristiche; le speciali cautele richieste per i dati sensibili; le operazioni di trattamento dei dati successive alla raccolta, comprese la durata e le modalità della loro conservazione; la garanzia per gl'interessati (per ben due altre volte, la Corte li appella nuovamente "titolari") di poter accedere agli stessi e di opporsi alla loro la diffusione, nonché gli ulteriori diritti, riflesso delle specifiche situazioni giuridiche soggettive.

L'articolo 3 della legge regionale della Puglia n. 13 del 2023 è pertanto dichiarato dalla Consulta costituzionalmente illegittimo per contrasto con l'articolo 117, primo comma, della Costituzione, in relazione al Regolamento (UE) 2016/679 ed alla Direttiva (UE) 2016/680, e con l'articolo 117, secondo comma, lettera *l)*, della Costituzione, con riguardo alla materia «ordinamento civile».

È assorbita ogni ulteriore censura, *i.e.* quella relativa alla materia dell'«ordinamento penale» per quanto concerne l'ultronea attribuzione all'autorità giudiziaria della competenza all'accesso alle videoriprese da parte della legge regionale.

Un'ultima considerazione

La sentenza in commento, richiamata anche dal Presidente del Garante per la protezione dei dati personali, Prof. Stanzione, nella sua relazione annuale alle Camere del 3 luglio 2024, come si è visto, poco o nulla aggiunge di nuovo a quanto incisivamente asserito sin dalla sentenza n. 271 del 2005. Tuttavia, e in conclusione, può osservarsi come, dopo l'intervento del GDPR, debba intendersi superato il richiamo da essa operato, per il caso di specie, al provvedimento di carattere generale del Garante in materia di videosorveglianza, adottato l'ormai lontano 8 aprile 2010, e come sia invece attesa e ormai improrogabile un'iniziativa legislativa in materia

FILIBERTO BROZZETTI

Sentenza C. Cost. 69/2024

2024/2(26)ES

26. Approvato in via preliminare il decreto legislativo di adeguamento al MiCAR (regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività)

Il 24 giugno 2024, dopo un periodo di consultazione pubblica sul relativo schema, il Consiglio dei Ministri ha approvato in via preliminare il decreto legislativo (da ora anche il "**Decreto**") che adegua l'ordinamento italiano al reg. 2023/1114/UE del Parlamento europeo e del Consiglio (c.d. "**Markets in Crypto-Assets Regulation**", da ora anche il "**Regolamento**" o "**MiCAR**" su cui v. in questa Rubrica la notizia 1 nel numero 2023/2 [2023/2(1)AF]: http://www.personaemercato.it/wpcontent/uploads/2023/08/Osservatorio.pdf).

ISSN 2239-8570

Il Decreto, innanzitutto, fornisce alcune definizioni (art. 2).

Il combinato disposto degli artt. 3 e 4 stabilisce che, per quanto riguarda i *token* collegati ad attività o di moneta elettronica, la Banca d'Italia e la Consob (da ora anche le "**Autorità**") abbiano poteri di vigilanza e indagine specificati dal Decreto e dall'art. 94, par. 1 del Regolamento, senza che ciò pregiudichi le competenze già riservate a tali Autorità dal D. Lgs. 385/1993 (il "**Testo Unico Bancario**" o "**TUB**") e dal D.Lgs. 58/1998 (il "**Testo Unico della Finanza**" o "**TUF**"). Banca d'Italia e Consob possono procedere ad audizioni ed ispezioni, in tale ultimo caso previa autorizzazione della Procura della Repubblica. Per quanto riguarda le cripto-attività diverse dai *token* collegati ad attività o di moneta elettronica, inoltre, la Consob può anche procedere a perquisizioni e sequestri (art. 15). Alle suddette Autorità di vigilanza compete anche l'emanazione di provvedimenti attuativi del Decreto (art. 5). I menzionati poteri sono esercitabili nei confronti degli emittenti dei *token* e di terzi che hanno siglato accordi con gli emittenti per la gestione della riserva di attività di quest'ultimi.

La Banca d'Italia è competente a vietare o limitare la commercializzazione, distribuzione o vendita dei *token* di moneta elettronica. La Consob e la Banca d'Italia congiuntamente hanno le medesime competenze sui *token* collegati ad attività e su tutte le restanti cripto-attività (art. 8, commi 1 e 2). Il successivo comma 3 dell'art. 8 entra nel dettaglio delle competenze delle Autorità e specifica che la Consob "*è competente per quanto riguarda la tutela degli investitori e l'ordinato funzionamento e l'integrità dei mercati delle cripto-attività",* mentre la Banca d'Italia è *"competente per quanto riguarda la stabilità dell'insieme o di una parte del sistema finanziario*". Al fine di assicurare il raggiungimento di tali obiettivi di vigilanza, gli artt. 9 e 10 prevedono forme di collaborazione transfrontaliera tra Autorità di vigilanza.

L'art. 11 del Decreto prevede che la Banca d'Italia d'intesa con la Consob approvino i *white papers* per l'emissione, l'offerta al pubblico e la richiesta di ammissione alla negoziazione dei *token* collegati ad attività (a seconda dei casi c.d. "**Electronic Money Token**" o "**EMT**" e "**Asset Referenced Token**" o "**ART**") anche laddove per tali operazioni l'emittente abbia costituito un patrimonio destinato. Resta inteso che le Autorità di vigilanza possono anche revocare le suddette autorizzazioni.

Gli emittenti possono avere solo la forma giuridica della società per azioni, in accomandita per azioni o a responsabilità limitata e oltre ad emettere i *token* possono anche prestare servizi, attività connesse e strumentali in favori di altri emittenti (art. 11, comma 8).

L'art. 12, commi 2 e 3 specifica le competenze, già sancite a livello generale dagli artt. 3 e 4, della Banca d'Italia e della Consob in tema di vigilanza degli emittenti di *token* collegati ad attività. Gli esponenti aziendali e i partecipanti al capitale degli emittenti devono avere i requisiti previsti, rispettivamente, dagli art. 26 TUB e 13 TUF e 25 TUB (art. 12, commi 8 e 9).

In merito ai prestatori di servizi per le cripto-attività, l'art. 16 Decreto prevede che la Consob, sentita la Banca d'Italia, autorizzi lo svolgimento di

ISSN 2239-8570

tale attività e, ricorrendone i presupposti, possa anche revocare la suddetta autorizzazione. Alla Consob e alla Banca d'Italia spetta la vigilanza sui prestatori di servizi. Ancora una volta, il Decreto ribadisce che la Consob è competente riguardo "*alla trasparenza, alla correttezza dei comportamenti, all'ordinato svolgimento delle negoziazioni e alla tutela dei clienti*", mentre alla Banca d'Italia è affidato il controllo sul contenimento del rischio, la stabilità patrimoniale e la sana e prudente gestione delle società (artt. 17 e 18). Gli esponenti aziendali e i partecipanti al capitale dei prestatori di servizi devono avere i requisiti previsti, rispettivamente, dagli art. 26 TUB, nonché 14 e 16 TUF e 25 TUB (art. 17).

Il Decreto detta altresì alcune norme speciali per gli emittenti di *token* collegati ad attività. Nello specifico, al fine di salvaguardare gli investitori, l'art. 19 prevede che la riserva di cripto-attività di un emittente e i beni in cui esse siano investite costituiscano un patrimonio separato da quello dell'emittente e dalle altre riserve di attività. Sul patrimonio separato non sono ammesse azioni dei creditori dell'emittente e al depositario è vietata la compensazione (legale, giudiziale o convenzionale) dei propri crediti con quelli dell'emittente. I possessori di *token*, invece, posso soddisfarsi su tale patrimonio separato nel limite del valore del loro credito (art. 19, commi 3 e 4).

In merito alla crisi degli emittenti, l'art. 47 MiCAR prevede che un emittente di *token* collegati ad attività debba elaborare un piano di rimborso per consentire *"il soddisfacimento ordinato di ciascun token collegato ad attività, che deve essere attuato sulla base di una decisione dell'autorità competente secondo cui l'emittente non è in grado o rischia di non essere in grado di adempiere i propri obblighi, tra l'altro in caso di insolvenza o, se applicabile, di risoluzione o in caso di revoca dell'autorizzazione dell'emittente, fatto salvo l'avvio di una misura di prevenzione della crisi o di una misura di gestione della crisi*". Dal canto suo, il combinato disposto degli artt. 20 e 22 del Decreto richiama il citato art. 47 MiCAR e stabilisce che gli emittenti debbano dotarsi di un piano di rimborso. Laddove quest'ultimo sia attuato al di fuori di una procedura concorsuale, l'emittente dovrà nominare dei liquidatori e determinarne i poteri; la nomina deve essere iscritta nel Registro delle Imprese. I liquidatori devono avere adeguata professionalità, esperienza e godere di buona reputazione. Ovviamente, qualora si apra una procedura concorsuale, la liquidazione volontaria si chiude. L'art. 23 prevede che la Banca d'Italia, sentita la Consob e, se del caso, l'Autorità Bancaria Europea, possa disporre la rimozione dei componenti degli organi di amministrazione e controllo di un emittente di *token*, nonché l'apertura dell'amministrazione straordinaria (art. 24) e/o della liquidazione coatta amministrativa (art. 25) di quest'ultimo.

Sempre nell'ottica di tutelare gli investitori, gli artt. 26 - 29 del Decreto prevedono che la separazione patrimoniale, l'esclusione della compensazione, la disciplina in tema di liquidazione volontaria e crisi d'impresa valgano anche per i prestatori di servizi per le cripto-attività.

Gli artt. 31 ss. del Decreto prevedono:

- delle rilevanti sanzioni amministrative e penali nei confronti degli emittenti e dei prestatori di servizi laddove ricorrano alcune

ISSN 2239-8570

fattispecie come, ad esempio, abusivo esercizio dell'attività, mancata collaborazione con le Autorità di vigilanza, abuso di informazioni privilegiate e manipolazione del mercato, ecc.;
- modifiche alla normativa di settore già in vigore;
- un regime transitorio in favore dei soggetti che alla data di entrata in vigore del Decreto già svolgano le attività da esso regolate. In particolare, le "*persone giuridiche che alla data del 27 dicembre 2024 risultino regolarmente iscritti nella sezione speciale del registro di cui all'articolo 17-bis, comma 1, del decreto legislativo 13 agosto 2010, n. 141, secondo quanto previsto dai commi 8-bis e 8-ter del medesimo articolo, che presentino istanza di autorizzazione … entro il 30 giugno 2025 possono continuare a prestare servizi relativi … fino al 30 dicembre 2025*";
- un'attività di monitoraggio per cui la Banca d'Italia e la Consob, entro due anni dall'entrata in vigore del Decreto, trasmettono un rapporto sull'applicazione della normativa al Comitato Fintech istituito presso il Ministero dell'Economia e delle Finanze.

Ai sensi dell'art. 48, infine, il Decreto entra in vigore il giorno successivo alla pubblicazione sulla Gazzetta Ufficiale, fatta eccezione per le norme relative alle cripto-attività diverse dai *token* collegati ad attività o di moneta elettronica, ai prestatori di servizi e alla prevenzione e divieto degli abusi di mercato relativi alle cripto-attività di cui al Regolamento che entreranno in vigore il 30 dicembre 2024.

EMANUELE STABILE

https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-87/26099

Schema di decreto sottoposto a consultazione pubblica

Decreto approvato in via preliminare

2024/2(27)FG

27. Pubblicato il 15.5.2024 il regolamento AGCOM sull'equo compenso di autori, artisti, interpreti ed esecutori e sulla gestione dei diritti connessi da parte degli OGC e delle EGI

Il 15 maggio 2024, l'Autorità per le Garanzie nelle Comunicazioni (**AGCOM** o l'**Autorità**) ha pubblicato la Delibera n. 95/24/CONS approvando il "Regolamento sugli obblighi di informazione e di adeguamento contrattuale degli autori e degli artisti interpreti o esecutori, nonché sulla rappresentatività degli organismi di gestione collettiva, in attuazione degli articoli 18-*bis*, 46-*bis*, 80, 84, 110-*ter*, 110-*quater*, 110-*quinquies*, 110-*sexies*, 180-*ter* della Legge sul Diritto d'Autore [**LdA**]" (il

ISSN 2239-8570

Regolamento). Il Regolamento costituisce l'Allegato A alla Delibera n. 95/24/CONS.

Dopo la chiusura della consultazione pubblica, avviata da AGCOM con la Delibera n. 44/23/CONS per raccogliere osservazioni e informazioni sullo schema di Regolamento, è stato necessario circa un anno per l'adozione del provvedimento in esame, che è entrato in vigore trenta giorni dopo la sua pubblicazione, i.e. il 16 giugno 2024.

Il Regolamento rappresenta l'ultima fase dell'implementazione in Italia della direttiva europea sul diritto d'autore e sui diritti connessi nel mercato unico digitale (Direttiva (UE) 2019/790, di seguito **Direttiva CDSM**) così come recepita dal d.lgs. 8 novembre 2021, n.177 (su cui v. in questa Rubrica la notizia n. 1 del numero 1/2022 [2022/1(1)EB]).

Il Capo terzo del Titolo IV della Direttiva CDSM ha come obiettivo quello di fornire una maggiore protezione a favore di autori, artisti, interpreti ed esecutori (**AIE**), che spesso si trovano in una posizione contrattuale svantaggiata sia nella fase di negoziazione sia in quella di esecuzione dei contratti di cessione o licenza dei diritti d'autore e dei diritti connessi. Questo obiettivo viene perseguito cercando di bilanciare i diversi interessi in gioco, inclusi quelli degli utilizzatori.

La normativa che fa da sfondo al Regolamento è complessa e densa di contenuti: delinea essenzialmente, da un lato, il *modus operandi* per l'adeguamento contrattuale a favore di autori e AIE (art. 110-quinquies LDA) e i criteri di misurazione della rappresentatività degli organismi di gestione collettiva (**OGC**) per la stipula di licenze collettive estese (art. 180-ter LdA), dall'altro, affida alla stessa Autorità poteri di vigilanza (art. 110 quater LdA), poteri di assistenza per il raggiungimento di accordi contrattuali (art. 110-ter LdA) o di risoluzione di controversie (art. 110-sexies LdA, art. 18-bis LdA, art. 46-bis e art. 84 LdA).

Il meccanismo di adeguamento contrattuale (art. 6 del Regolamento) garantisce una remunerazione adeguata e proporzionata agli autori e AIE stabilendo che, se la remunerazione forfettaria inizialmente prevista si rivela sproporzionatamente bassa rispetto ai ricavi successivamente generati dallo sfruttamento delle opere, la remunerazione può essere rideterminata. Per valutare se la remunerazione possa essere considerata troppo bassa, saranno presi in considerazione i ricavi derivanti dallo sfruttamento dell'opera in qualsiasi forma, inclusi i ricavi del merchandising.

Qualora l'autore o l'AIE non percepisca una remunerazione forfettaria, tale adeguamento non sarà necessario, in quanto i contratti gli garantiscono di ricevere una remunerazione commisurata al successo dell'opera della quale hanno ceduto i diritti. Sono esclusi dall'ambito di applicazione dell'articolo i contratti conclusi direttamente da OGC/EGI.

Il criterio di misurazione della rappresentatività degli OGC (art. 8 del Regolamento) riguarda, invece, la concessione di licenze collettive estese relativamente ai diritti di cui agli articoli 18-*bis* (equa remunerazione per noleggio spettante ad autori), 46-*bis* (compenso adeguato e proporzionato per gli autori di opere cinematografiche e assimilate), 73, 73-*bis* (compenso per l'utilizzazione dei fonogrammi a mezzo della cinematografia, della diffusione radiofonica e televisiva, nelle pubbliche feste danzanti, nei

ISSN 2239-8570

pubblici esercizi e in occasione di qualsiasi altra pubblica utilizzazione dei fonogrammi stessi), 80 (equa remunerazione per noleggio spettante agli AIE) e 84 LdA (compenso adeguato e proporzionato per gli AIE che nell'opera cinematografica e assimilata sostengono una parte di notevole importanza artistica).

È previsto che i tre OGC più rappresentativi per ciascuna categoria di titolari dei diritti possano stipulare licenze collettive estese per la remunerazione dei diritti, anche a favore di soggetti non rappresentati da alcun OGC, cd. apolidi (Articoli 7 e 10 del Regolamento).

Ogni titolare dei diritti può decidere, tramite un meccanismo di opt-out, di escludere, in qualsiasi momento, le proprie opere dal suddetto meccanismo di licenza collettiva. L'efficacia dell'opt-out decorre a partire dalla data della prima ripartizione dei proventi presso gli aventi diritto mandanti o associati, successiva al ricevimento della relativa comunicazione.

AGCOM valuterà annualmente quali OGC sono responsabili della raccolta e della distribuzione della remunerazione agli autori e AIE, basandosi su specifici criteri di rappresentatività di cui all'Allegato B del Regolamento.

In sede di prima applicazione (i.e. 2024), per calcolare la rappresentatività degli OGC, si considererà, per ciascuna categoria di titolari dei diritti, la media annua dei compensi incassati per la tipologia di diritto rilevante negli ultimi tre anni di attività, come risultanti dai bilanci depositati e certificati dall'organo di revisione contabile.

Il criterio del fatturato non verrà utilizzato per gli anni successivi perché presenta criticità: pur essendo un criterio oggettivo, come osservato nella delibera 44/23/CONS, può creare un circolo vizioso. Le percentuali di rappresentatività influenzano il valore della licenza, che poi determina le percentuali dell'anno successivo, cristallizzando le quote di mercato degli organismi di gestione collettiva (OGC). Questo rende difficile per nuovi organismi accreditarsi e guadagnare quote di mercato.

Dal 2025, si considererà l'effettivo sfruttamento da parte degli utilizzatori delle opere e di conseguenza l'effettivo sfruttamento dei diritti degli autori e degli AIE. Nell'ambito delle tipologie di sfruttamento individuate da AGCOM, ciascun OGC comunicherà all'Autorità la propria rappresentatività per determinate tipologie di utilizzatori (i.e. Broadcasting TV, Broadcasting radio, VOD, Online licenze nazionali musica, Webradio, Radio in store, Proiezioni cinematografiche, Diritto di riproduzione meccanica, Pubblica esecuzione feste private).

Il calcolo verrà effettuato per ciascuna delle categorie di titolari dei diritti individuati ai sensi dell'Allegato B alla Delibera n. 95/24/CONS (Allegato tecnico).

Si evidenzia che nella delibera in esame (vd. premessa e osservazioni dell'AGCOM all'Art. 8), AGCOM rilevi come il criterio di calcolo della rappresentatività potrebbe avere una valenza più generale per determinare la rappresentatività degli organismi collettivi in particolare in funzione delle negoziazioni delle licenze. Tale interpretazione è suffragata dall'art. 180 LdA che stabilisce come nell'ambito delle attività di intermediazione per il

ISSN 2239-8570

diritto d'autore, la concessione delle licenze debba avvenire anche considerando la rappresentatività di ciascun OGC.

AGCOM si riserva di estendere il ragionamento della rappresentatività alle EGI qualora, alla luce della sentenza LEA c. JAMENDO SA (causa C-10/22 sentenza del 21 marzo 2024, analizzata nel precedente numero di Persona e Mercato 2024/1), l'ambito di applicazione dell'art. 180 LdA fosse ulteriormente esteso anche alle stesse EGI.

Ai sensi del Regolamento, gli utilizzatori pagheranno i proventi relativi agli apolidi pro-quota tra i tre OGC maggiormente rappresentativi.

Gli apolidi potranno richiedere alle OGC i pagamenti ad essi spettanti e i soldi raccolti verranno distribuiti dagli OGC facendo riferimento ai regolamenti di ripartizione.

Gli OGC conserveranno gli importi per tre anni, dopodiché gli importi non distribuiti verranno utilizzati per finanziare attività culturali, sociali ed educative (ai sensi dell'art. 19 del D.Lgs. 35/2017).

I poteri di vigilanza spettanti all'Autorità ai sensi dell'art. 110-quater LdA sono stati affidati ad AGCOM per garantire il rispetto degli obblighi di informazione e comunicazione in capo, da un lato, a licenziatari e cessionari e, dall'altro, organismi di gestione collettiva ed entità di gestione indipendente ("EGI")(art. 5 del Regolamento).

Infatti, i licenziatari, inclusi i sub-licenziatari, e i soggetti a cui sono stati ceduti i diritti patrimoniali devono fornire agli aventi diritto (anche tramite OGC/EGI) informazioni aggiornate e complete sullo sfruttamento delle loro opere e sulla remunerazione dovuta. Le informazioni devono essere fornite almeno ogni sei mesi, salvo accordi diversi purché non superiore a un anno. Le informazioni richieste riguardano l'identità dei soggetti coinvolti, le modalità di sfruttamento delle opere, i ricavi generati (ivi inclusi introiti pubblicitari e di merchandising) e la remunerazione dovuta secondo quanto stabilito negli accordi di concessione di licenza o trasferimento dei diritti. Trascorsi tre anni dalla conclusione dell'accordo di licenza o del contratto di cessione, è possibile richiedere le informazioni formulando una apposita richiesta al licenziatario/cessionario.

Le informazioni richieste riguardano l'identità dei soggetti coinvolti, le modalità di sfruttamento delle opere, i ricavi generati (ivi inclusi introiti pubblicitari e di merchandising) e la remunerazione dovuta secondo quanto stabilito negli accordi di concessione di licenza o trasferimento dei diritti

Obblighi di informazione competono anche agli stessi OGC e alle EGI che, sulla base di una richiesta adeguatamente giustificata da parte dei licenziatari/sublicenziatari o cessionari, sono obbligati a fornire dati elettronici sui soggetti che rappresentano, sulle opere che gestiscono, i diritti che rappresentano direttamente o sulla base di accordi di rappresentanza, e i territori oggetto di tali accordi.

AGCOM può in qualsiasi momento accertare la violazione degli obblighi di cui all'articolo 5 attraverso ispezioni, richieste di informazioni e documenti, nonché audizioni, applicando sanzioni sul fatturato (non solo italiano) realizzato nell'ultimo esercizio chiuso anteriormente a notifica della contestazione.

ISSN 2239-8570

Infine, il Regolamento affida ad AGCOM poteri di assistenza per il raggiungimento di accordi contrattuali per licenze di sfruttamento delle opere audiovisive su servizi di video on demand (art. 110-ter LdA) o di risoluzione di controversie per l'adeguamento contrattuale dei compensi e per la definizione dei compensi in assenza di un accordo tra le parti (art. 110-sexies LdA, art. 18-bis LdA, art. 46-bis e art. 84 LdA). Le procedure da seguire sono descritte in dettaglio nel Regolamento.

FRANCESCO GROSSI

Delibera N. 95/24/CONS
https://www.agcom.it/sites/default/files/migration/delibera/Delibera%2095-24-CONS.pdf

Regolamento:
https://www.agcom.it/sites/default/files/migration/attachment/Allegato%2015-5-2024.pdf

2024/2(28)EB

28. Il nuovo regolamento AGCOM del 5.12.2023 emanato in seguito all'adozione del Codice delle comunicazioni elettroniche, recante disposizioni a tutela degli utenti finali in materia di contratti relativi alla fornitura di servizi di comunicazioni elettroniche

Il 5 dicembre 2023, con delibera n. 307/23/CONS, l'Autorità per le garanzie nelle comunicazioni (di seguito "**AGCOM**" o l'"**Autorità**") ha approvato il nuovo Regolamento recante disposizioni a tutela degli utenti in materia di contratti relativi alla fornitura di servizi di comunicazioni elettroniche tra operatori di servizi di comunicazioni elettroniche e utenti finali (di seguito anche solo "**Regolamento**").

L'intervento dell'AGCOM, che ha portato all'abrogazione del vecchio regolamento di cui alla delibera n.519/15/CONS, del 25 settembre 2015, è dovuto all'entrata in vigore Decreto legislativo, 8 novembre 2021, n. 207 (di seguito il "**D.Lgs. 207/2021**") che ha dato attuazione alla Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 (di seguito la **"Direttiva**") istitutiva del «Codice europeo delle comunicazioni elettroniche» (di seguito il "**Codice europeo**") e che ha adottato il «Codice delle comunicazioni elettroniche» (di seguito il "**Codice**").

In esito ad una procedura di consultazione pubblica *ad hoc*, il Regolamento ha inteso offrire una riposta a diversi operatori del settore che avevano chiesto all'Autorità di avviare un confronto sulle modalità attraverso cui dare corretta interpretazione ed attuazione alla disciplina in materia di tutela degli utenti contenuta nel Codice.

Le profonde modifiche introdotte dal Codice avevano infatti determinato l'avvio, sin dal 2022, delle attività di revisione della regolamentazione a

ISSN 2239-8570

tutela degli utenti finali nell'ambito del riassetto della regolamentazione inerente alla qualità dei servizi e alla tutela degli utenti con disabilità (delibere AGCOM nn. 23/23/CONS, 156/23/CONS, 436/22/CONS, 36/23/CONS, 251/23/CONS).

Con tale ultimo intervento regolatorio, l'Autorità ha invece proceduto ad un riassetto della disciplina regolamentare avente ad oggetto i contratti utilizzati per la fornitura dei servizi di comunicazione elettronica agli utenti finali, al fine di tener conto delle novità introdotte dal D.Lgs. 207/2021.

In particolare, le novità hanno interessato i seguenti aspetti del rapporto contrattuale tra operatori e utenti finali:

i. ambito di applicazione soggettivo;
ii. informazioni contrattuali;
iii. durata del contratto e costi di recesso;
iv. cessazione del rapporto contrattuale;
v. modifica delle condizioni contrattuali;
vi. discrepanza delle prestazioni rispetto a quanto promesso nel contratto e diritto di recesso;
vii. migrazioni e portabilità;
viii. contratti con previsione di adeguamento all'indice dei prezzi al consumo

Rispetto al primo punto (*i.*), ossia **l'ambito di applicazione soggettivo** (art. 2 del Regolamento), il Regolamento si preoccupa di ridefinire la nozione di "utente finale". Difatti, in linea con il Considerando 259 della Direttiva, il Regolamento trova applicazione sia per i consumatori/persone fisiche, trattandosi di norme di maggior tutela, che per le microimprese, piccole imprese e organizzazioni senza scopo di lucro. Queste ultime entità, a differenza dei consumatori, possono tuttavia decidere di rinunciare al livello di tutela ivi stabilito, negoziando condizioni diverse con il fornitore. Perché la deroga possa avere un qualche effetto è necessario, tuttavia, che essa venga approvata espressamente dall'impresa o organizzazione in sede di stipula. Per le imprese più grandi, la stessa Direttiva (e dunque il Regolamento) chiarisce che queste, proprio in ragione della loro dimensione possano negoziare clausole diverse senza bisogno di deroga espressa.

Quanto sopra trova una facile spiegazione nella presunzione secondo cui le microimprese, piccole imprese e organizzazioni senza scopo di lucro abbiano una posizione contrattuale comparabile a quella dei consumatori e debbano godere del medesimo livello di tutela, salvo che non vi rinuncino espressamente.

Una seconda novità apportata dal Regolamento attiene alle (*ii.)* **informazioni contrattuali** (artt. 3 e 4 del Regolamento) che gli operatori dovranno fornire, il cui contenuto è stato ampliato dal Codice.

Gli operatori devono infatti adeguare i propri modelli contrattuali e adottare tutte le misure necessarie affinché gli utenti finali dispongano, prima della conclusione del contratto, delle informazioni elencate di seguito, che devono essere riportate in modo chiaro, dettagliato e comprensibile e fornite su un supporto durevole, in un formato accessibile per gli utenti finali con disabilità. Tra le informazioni obbligatorie, gli operatori devono includere:

ISSN 2239-8570

a) i livelli minimi di qualità del servizio;
b) le condizioni, compresi i contributi, per l'utilizzo delle apparecchiature terminali fornite;
c) i costi di attivazione del servizio, i costi ricorrenti o legati al consumo;
d) i dettagli del piano tariffario, come i tipi di servizi offerti e i volumi inclusi (es. Gbyte, minuti, messaggi);
e) le tariffe in vigore per numeri o servizi soggetti a particolari condizioni tariffarie nel rispetto del Piano nazionale di numerazione;
f) per i pacchetti di servizi e apparecchiature terminali, il prezzo dei singoli elementi del pacchetto, se commercializzati anche separatamente;
g) dettagli e condizioni sul servizio postvendita, manutenzione e assistenza ai clienti;
h) informazioni sulla presenza di clausole relative all'adeguamento del prezzo all'indice di inflazione, se applicate;
i) ogni utilizzo minimo o durata minima richiesti per beneficiare di condizioni promozionali;
j) informazioni sulle procedure di passaggio ad altro operatore;
k) informazioni sul diritto al rimborso dei crediti residui per servizi prepagati in caso di passaggio;
l) oneri per risoluzione anticipata dal contratto, incluse informazioni sul recupero dei costi del terminale;
m) termine entro il quale avverrà l'attivazione del servizio e modalità di corresponsione dell'indennizzo automatico se tale termine non viene rispettato;
n) i diritti dei consumatori applicabili qualora non sia raggiunto il livello di qualità del servizio previsto dal contratto;
o) in caso di pacchetti di servizi e terminali, le condizioni di rinnovo e di risoluzione del contratto, le condizioni di cessazione del pacchetto o dei suoi elementi;
p) informazioni dettagliate su prodotti e servizi per utenti finali con disabilità;
q) i mezzi con cui possono essere avviati i procedimenti di risoluzione delle controversie;
r) le informazioni previste dal regolamento UE sulla *Net Neutrality*.

Un'ulteriore novità in tema informativo, attiene all'obbligatorietà di fornitura agli utenti finali, da parte degli operatori, di una sintesi contrattuale, concisa e facilmente leggibile che individua i principali elementi del servizio, anche in caso di contatto telefonico. Tale obbligo è stato introdotto dall'articolo 98 *quater decies*, co.1 del D.Lgs. 207/2021, il quale stabilisce parimenti il contenuto minimo di tale sintesi contrattuale, che deve illustrare almeno le caratteristiche di ciascun servizio, i relativi prezzi una tantum e ricorrenti, la durata del contratto, il rinnovo e la risoluzione, le misure per i disabili e le informazioni (in sintesi) previste dal regolamento sulla *net neutrality*.

Rispetto alla (*iii.*) **durata del contratto** (art. 5 del Regolamento) i contratti non possono prevedere, di norma, un periodo di impegno iniziale

ISSN 2239-8570

superiore a 24 mesi. Dopo il ventiquattresimo mese dalla stipula, l'utente finale ha il diritto di recedere in qualsiasi momento con un preavviso di massimo un mese e senza incorrere in alcuna penale né costi di disattivazione, eccetto quelli addebitati per la ricezione del servizio durante il periodo di preavviso e gli eventuali costi da recuperare per l'apparecchiatura terminale (es. il modem fisico).

Ai fini dell'eventuale pagamento del valore dell'apparecchiatura terminale, gli operatori sono tenuti ad applicare ai propri clienti, in caso di recesso o di disdetta del contratto principale, di default il pagamento delle residue rate, salvo che sia l'utente a chiedere espressamente di pagare in un'unica soluzione il rimanente costo. Il periodo di rateizzazione del terminale, con il consenso del cliente, può essere superiore a 24 mesi.

Il medesimo principio è ribadito anche a proposito della (*iv.*) **cessazione del rapporto contrattuale** (art. 8 del Regolamento). Difatti, in caso di disdetta del contratto, esercitata a seguito del preavviso di proroga, l'operatore non può addebitare all'utente finale alcuna penale se non il corrispettivo per i costi relativi alla cessazione, i corrispettivi dovuti per i servizi erogati fino alla scadenza del primo vincolo contrattuale e gli eventuali costi da recuperare in relazione all'apparecchiatura terminale.

Il Codice ha inciso parimenti sulla disciplina della *(v.)* **modifica delle condizioni contrattuali** (art. 6 del Regolamento). In caso di modifiche delle condizioni contrattuali proposte dall'operatore, gli utenti finali hanno il diritto di recedere dal contratto o di cambiare operatore, senza incorrere in alcuna penale né costi di disattivazione, entro 60 giorni dalla relativa comunicazione dell'operatore, il quale deve dare un preavviso non inferiore a trenta giorni.

Le modifiche delle condizioni contrattuali proposte dall'operatore possono tuttavia consistere anche in variazioni che vanno esclusivamente a vantaggio dell'utente finale, di carattere puramente amministrativo e che non abbiano alcun effetto negativo sull'utente finale o siano imposte direttamente dal diritto dell'Unione o nazionale. Di conseguenza, il diritto di recesso può essere esercitato nel caso in cui il mutamento delle condizioni contrattuali sia sfavorevole all'utente finale.

Il diritto dell'utente finale di risolvere il contratto è escluso solo nel caso in cui il fornitore sia in grado di dimostrare che tutti i cambiamenti contrattuali sono a esclusivo beneficio dell'utente finale o sono meramente amministrativi e non hanno ripercussioni negative sull'utente finale. Resta pertanto in capo all'operatore l'onere di dimostrare che i cambiamenti siano effettivamente a beneficio dell'utente finale.

Le modifiche che l'operatore intende introdurre al contratto devono essere comunicate all'utente con un preavviso di trenta giorni ed il Codice estende a sessanta giorni il termine per esercitare il recesso qualora l'utente finale non intenda accettare le nuove condizioni. Le nuove condizioni troveranno applicazione non appena siano trascorsi i trenta giorni di preavviso senza che l'utente abbia esercitato il diritto di recesso.

Sul tema, le novità introdotte dal Regolamento attengono sia al termine entro cui esercitare il recesso (entro sessanta giorni dall'avvenuta comunicazione di modifica delle condizioni contrattuali), sia alla previsione

ISSN 2239-8570

di recesso che avvenga dopo il trentesimo giorno dalla comunicazione delle modifiche contrattuali. Difatti, l'articolo 6 del Regolamento precisa che il recesso completato nei primi trenta giorni dalla comunicazione di modifica delle condizioni contrattuali, non comporta effetti per il recedente, in tal caso si applicano, nei trenta giorni dalla comunicazione di modifica delle condizioni contrattuali, le vecchie condizioni contrattuali.

Contrariamente, il recesso completato oltre il termine di trenta giorni dalla comunicazione di modifica delle condizioni contrattuali comporta effetti per il recedente nella parte di preavviso che si estende oltre il trentesimo giorno. In tale ultimo caso, infatti, l'Autorità ritiene opportuno che si applichino al recedente le vecchie condizioni contrattuali nei primi 30 giorni e quelle modificate dal trentunesimo giorno fino al completamento del recesso.

Più favorevole per l'utente è parimenti il recesso in caso di *(vi.)* **discrepanza delle prestazioni rispetto a quanto promesso nel contratto e diritto di recesso** (art. 6-bis del Regolamento)**.**

Difatti, in caso di discrepanza significativa, continuativa o frequentemente ricorrente, rispetto agli effettivi valori delle velocità minime della connessione a Internet in download e upload, del ritardo massimo di trasmissione dati o del tasso massimo di perdita dei pacchetti e la prestazione indicata nel contratto, l'utente finale ha il diritto di recedere dal contratto senza incorrere in alcun costo, fatto salvo il diritto agli indennizzi previsti dal contratto o dalla regolamentazione di settore per i disservizi subiti.

Una delle questioni che assume rilievo in ambito regolamentare riguarda l'esercizio del diritto di recesso nel caso di contestuale passaggio ad altro operatore. Difatti il nuovo Regolamento ha prestato particolare attenzione alla normazione di (vi.) **migrazioni e portabilità** (art. 8-bis del Regolamento). Si è visto infatti come, sebbene ai sensi della vecchia regolamentazione erano stati definiti chiaramente i passaggi da osservare per i soggetti coinvolti nella procedura di migrazione (i.e. l'utente, il ricevente e il cedente), spesso tale procedura risultava viziata da una serie di anomalie, che hanno determinato la necessità di disciplinare meglio la fattispecie.

In particolare, ai sensi dell'articolo 8-bis del Regolamento, gli operatori devono fornire all'utente finale informazioni chiare sulle procedure di passaggio da un operatore a un altro, inclusa la portabilità del numero. Inoltre, deve essere indicato nel contratto il termine entro cui, a seguito della comunicazione dell'utente della volontà di recedere dal contratto e di passare ad altro operatore, si procede all'avvio della procedura tecnica di attivazione dei servizi di accesso a Internet e telefonico, e gli indennizzi in caso di ritardi nel passaggio. L'avvio della procedura di passaggio deve avvenire senza indugio.

L'operatore cedente è poi tenuto a continuare a prestare il servizio di accesso a Internet e telefonico alle stesse condizioni tecniche ed economiche finché l'operatore ricevente non attiva il suo servizio.

In ultimo, una delle novità più rilevanti introdotte dal Regolamento attiene alla possibilità di concludere (vii.) **contratti con previsione di**

ISSN 2239-8570

adeguamento all'indice dei prezzi al consumo. Il Regolamento approvato conferma che la proposta di modifica delle condizioni contrattuali al fine di prevedere un adeguamento periodico all'indice dei prezzi al consumo, in caso di contratti che non prevedono già tale meccanismo, può essere attuata solo dopo esplicita accettazione, in forma scritta, da parte dell'utente finale. In caso di mancata accettazione esplicita della modifica contrattuale da parte dell'utente, restano in vigore le condizioni contrattuali già previste.

L'indice di riferimento usato per adeguare i contratti è l'Indice Nazionale dei prezzi al consumo per le famiglie di operai e impiegati (FOI) senza tabacchi. Invece, i contratti che contengano già la previsione di adeguamento all'indice dei prezzi al consumo potranno essere basati sull'applicazione senza correttivi dell'indice ISTAT o con correttivi quali soglie minime di aumento, mark-up, o similari.

Qualora l'utente finale aderisca a contratti indicizzati con correttivi, al momento dell'incremento del canone legato all'indice dei prezzi al consumo, questi ha il diritto di recedere senza sostenere costi. In caso contrario, se il contratto non contempla correttivi rispetto all'indice ISTAT, il recesso comporta per l'utente i costi previsti.

In tali ultimi casi, però, il Regolamento stabilisce che: le condizioni contrattuali devono prevedere che l'operatore possa aumentare le tariffe proporzionalmente all'aumento dell'indice annuale dei prezzi al consumo e, altresì, ridurle in caso di diminuzione dell'indice; l'applicazione dell'adeguamento non può avvenire prima di 12 mesi dall'adesione contrattuale; se l'adeguamento supera il 5% del canone, l'utente può richiedere il passaggio a un'offerta analoga priva di tale meccanismo, senza costi aggiuntivi.

Le disposizioni si applicheranno a tutti i contratti, indipendentemente dalla data di stipula e le clausole di adeguamento già comunicate sono nulle senza il consenso esplicito dell'utente.

Il Regolamento impone misure di trasparenza, richiedendo che le comunicazioni contrattuali relative all'adeguamento all'inflazione siano chiare e comprensibili. Le informazioni sull'indicizzazione devono essere incluse nelle offerte commerciali, nei materiali pubblicitari ed evidenziate su tutti i canali di comunicazione. Inoltre, l'operatore deve fornire una tabella degli incrementi del canone per vari indici di inflazione e un tool di calcolo sul sito web.

Infine, qualsiasi clausola di indicizzazione deve essere chiaramente indicata nella sintesi contrattuale e accettata espressamente dal cliente.

EMANUELA BURGIO

Delibera n. 307/23/CONS

Regolamento

2024/2(29)VP

ISSN 2239-8570

29. Le Linee-guida dell'AGCOM del 10.1.2024 sul rispetto del TUSMA da parte degli influencer e l'istituzione di un apposito Tavolo tecnico

La crescente diffusione, anche nel panorama italiano, di contenuti pubblicati *online* da parte di soggetti reali o virtuali comunemente chiamati "*influencer"* o anche "*vlogger*", "*streamer*", "*creator*" e "*uploader*", ha spinto l'Autorità per le Garanzie nelle Comunicazioni (di seguito **AGCOM** o l' **Autorità**) ad avviare una pubblica consultazione, e, in esito ad essa, ad approvare delle linee guida con lo specifico intento - rispondente all'ambito delle proprie competenze - di valutare questo fenomeno alla luce del D.Lgs. n. 208 del 8 novembre 2021, il Testo Unico dei Servizi di Media Audiosivi (di seguito il **Testo Unico** o **TUSMA**).

L'analisi condotta dall'Autorità, pertanto, non è stata (né poteva essere, in ragione delle sue competenze), per così dire, "a tutto tondo", ma si è concentrata su quei tratti dell'attività dei soggetti comunemente indicati con quelle espressioni – e per comodità, convenzionalmente chiamati tutti con il termine "***influencer***" – che la rendono analoga o comunque assimilabile all'attività dei fornitori di servizi di media audiovisivi sottoposti in Italia alle disposizioni del TUSMA.

Per questo motivo, l'analisi condotta dall'AGCOM non ha riguardato profili dell'attività degli *influencer* specificamente e direttamente rilevanti ai fini dell'applicazione di altri plessi normativi presidiati da altre autorità, ad es. quei profili dell'*influencer marketing* direttamente rilevanti ai fini dell'applicazione della disciplina sulle pratiche commerciali scorrette (presidiata dall'Autorità garante per la concorrenza e il mercato, di seguito **AGCM**), applicata di recente dall'AGCM nel noto caso Balocco. Al contempo, il fenomeno del *marketing* degli *influencer* (l'*influencer marketing*) è stato indagato dall'AGCOM per i profili rilevanti per il TUSMA, posto che, come noto, il Testo Unico contiene una serie di importanti disposizioni sulla comunicazione commerciale e sul *product placement* (artt. 43, 46, 47 e 48 TUSMA), e l'AGCOM ha, di conseguenza, specifiche competenze per l'applicazione di queste disposizioni.

Fatte queste opportune premesse, qui di seguito esporremo in estrema sintesi i contenuti delle "*Linee-guida volte a garantire il rispetto delle disposizioni del Testo Unico da parte degli influencer*" adottate dall'AGCOM con Delibera 7/24/CONS del 10 gennaio 2024 (di seguito le **Linee guida** e la **Delibera**).

L'Autorità chiarisce innanzitutto che, ai fini delle Linee guida, gli *influencer* sono soggetti che "*svolgono un'attività analoga o comunque assimilabile a quella dei fornitori di servizi di media audiovisivi sotto la giurisdizione nazionale*" e che "*hanno il controllo sulla creazione, produzione o organizzazione"* di "*contenuti pubblicati online, tramite piattaforme per la condivisione di video e social media*".

Vengono poi elencati, ai fini della nozione rilevante ai fini delle Linee guida, alcuni requisiti che - sottolinea l'Autorità - devono essere posseduti cumulativamente.

ISSN 2239-8570

L'attenzione si focalizza *in primis* sul servizio offerto, il quale deve essere accessibile al grande pubblico, raggiungere "*un numero significativo di utenti*" sul territorio italiano, deve avere "*un impatto rilevante su una porzione significativa di pubblico*" e i contenuti devono essere diffusi tramite un servizio di piattaforma di condivisione di video o di *social media*.

Il servizio deve inoltre costituire attività economica ai sensi degli artt. 56 e 57 del Trattato sul funzionamento dell'Unione europea (**TFUE**) e deve essere "*caratterizzato da un legame stabile ed effettivo con l'economia italiana*".

Il principale scopo del servizio deve essere, su richiesta dell'utente, la fornitura di contenuti, creati o selezionati dall'*influencer*, i quali abbiano la finalità intrattenere o istruire gli utenti e di generare reddito in esecuzione di accordi commerciali diretti con produttori di beni e servizi oppure indirettamente tramite "*accordi di monetizzazione*" applicati dalla piattaforma o dal *social media* utilizzato.

Tra gli altri requisiti cumulativi che devono sussistere è inoltre previsto, come detto, il controllo effettivo sulla creazione, selezione o organizzazione dei contenuti, che comporta anche la "*responsabilità editoriale*" sui medesimi contenuti.

Infine, l'Autorità chiarisce che – affinché un soggetto possa essere considerato un *influencer* assoggettato alle Linee guida – il servizio deve essere offerto tramite l'utilizzo della lingua italiana o essere espressamente rivolto agli utenti che si trovano sul territorio italiano.

Tanto chiarito, l'AGCOM si pone il problema di distinguere, ai fini dell'individuazione delle disposizioni del TUSMA applicabili agli *influencer*, quei soggetti che svolgono attività "*amatoriale*" da quelli che svolgono attività "*professionale*".

In breve, nelle Linee guida la distinzione serve per dire che a tutti gli *influencer* si applicano le disposizioni degli artt. 41 e 42 TUSMA, mentre ai soli *influencer* professionali, si applicano "*almeno*" una serie di disposizioni ulteriori del TUSMA, elencate al punto 8 delle Linee guida.

La distinzione tra le due categorie di *influencer* si poggia, secondo l'AGCOM, sui "*principi e canoni di proporzionalità, differenziazione e adeguatezza*" che presidiano l'applicazione delle disposizioni del TUSMA. In sede di prima applicazione, e salvo successiva revisione di questi criteri, le Linee guida definisce *influencer* professionali quelli che, unitamente agli altri requisiti sopra elencati:

a. raggiungono un numero di iscritti – i c.d. *follower* – pari, in sede di prima applicazione, ad almeno un milione, risultanti dalla somma degli iscritti sulle piattaforme e dei *social media* sui quali operano;
b. abbiano pubblicato nell'anno precedente alla rilevazione almeno 24 contenuti;
c. abbiamo superato almeno su una piattaforma o social media un valore di *engagement rate* medio negli ultimi 6 mesi pari o superiore al 2%.

Le Linee guida proseguono dunque elencando le disposizioni del TUSMA che si applicano ai soli *influencer* professionali (punto 8 delle Linee guida):

ISSN 2239-8570

- l'art. 4(1) TUSMA, che prevede i «principi generali» del sistema dei servizi di media audiovisivi e della radiofonia, a garanzia degli utenti;
- l'art. 6(2)(a) TUSMA, che prevede il «principio generale» per il quale la disciplina in materia, per quanto applicabile agli influencer, garantisce «la presentazione veritiera dei fatti e degli avvenimenti, in modo tale da favorire la libera formazione delle opinioni»;
- l'art. 32 TUSMA, che contiene disposizioni a protezione del diritto d'autore;
- gli artt. 30, 37, 38 e 39 TUSMA, che contengono disposizioni a tutela dei diritti fondamentali della persona, dei minori e dei «valori dello sport», nonché le pertinenti delibere attuative adottate dall'Autorità;
- gli artt. 43, 46, 47 e 48 TUSMA, che contengono disposizioni in materia di comunicazioni commerciali.

Viene precisato che in caso di violazione delle disposizioni sopra richiamate, agli *influencer* professionali si applicano le sanzioni previste dall'art. 67 TUSMA, nonché la disposizione dell'art. 1, comma 31, della legge n.249/97.

Di conseguenza, e più nello specifico, gli *influencer* professionali devono, a pena dell'applicazione delle sopradette sanzioni, adottare tutte le misure necessarie affinché i loro contenuti:

a. non contengano alcuna istigazione o provocazione a commettere reati o apologia degli stessi.
b. garantiscano il pieno rispetto della dignità umana, essendo di conseguenza proibite espressioni che siano in qualche modo suscettibili di diffondere, incidere, propagandare, minimizzare o diffondere violenza, odio o discriminazione, tanto verso singoli quanto verso gruppi di persone;
c. non deresponsabilizzino l'autore né corresponsabilizzino le vittime di violenza, odio, discriminazione o di qualunque forma di vittimizzazione;
d. rispettino le norme del TUSMA in tema di tutela dei minori in modo che non siano pubblicati contenuti gravemente nocivi per lo sviluppo fisico, psichico o morale degli stessi, impegnandosi anche al rispetto delle specifiche delibere adottate in materia dall'AGCOM (delibere n. 52/13/CSP e n. 74/19/CONS). In proposito, le Linee guida richiedono anche che, all'atto del caricamento del contenuto, gli *influencer* professionali usino, ove disponibili, le funzionalità fornite dalla piattaforma per la condivisione di video per indicare che il contenuto contiene contenuti potenzialmente nocivi per i minori;
e. non prevedano il ricorso a tecniche subliminali (tanto in tema di creazione / condivisione di contenuti, quanto in tema di comunicazione);
f. rispettino il divieto di pubblicità occulta. In proposito, è interessante segnalare che, sotto l'impulso della consultazione pubblica, le Linee guida hanno inserito espressamente tra le linee di condotta da osservarsi da parte degli *influencer* professionali, il rispetto delle

ISSN 2239-8570

previsioni del regolamento elaborato dall'ente privato IAP (noto per la creazione del primo codice di autodisciplina pubblicitaria in Italia, nel 1966, ora giunto alla 70a edizione con il nome di Codice di Autodisciplina della Comunicazione Commerciale) il c.d. Regolamento *Digital Chart* sulla riconoscibilità della comunicazione commerciale diffusa attraverso Internet;

g. garantiscano il rispetto delle disposizioni in materia di tutela del diritto d'autore e della proprietà intellettuale;
h. garantiscano la presentazione veritiera di fatti ed avvenimenti.

Il Tavolo tecnico istituito con le Linee guida (v. Allegato B alla Delibera) avrà la funzione di definire ulteriormente le caratteristiche necessarie per l'individuazione degli influencer professionali e le disposizioni del TUSMA applicabili, nonché di assistere l'AGCOM per l'elaborazione di codici di condotta.

L'indirizzo formulato dall'Autorità è che l'approfondimento del Tavolo tecnico avvenga considerando la specificità dei settori di attività in cui gli *influencer* professionali operano. La distinzione tra *influencer* professionali e no, deve infatti tenere necessariamente conto della natura dell'attività in concreto svolta, del livello di competenza e della loro influenza nel rispettivo campo.

Nei prossimi mesi, gli effetti della prima fase di implementazione delle Linee guida ed i lavori del Tavolo Tecnico forniranno maggiori informazioni sugli scenari che prospetta l'applicazione del TUSMA agli *influencer*, nel senso inteso dall'AGCOM.

VINCENZO PITTELLI

Pagina web di AGCOM sulla delibera 7/24/CONS:
https://www.agcom.it/provvedimenti/delibera-7-24-cons

Delibera 7/24/CONS:
https://www.agcom.it/sites/default/files/migration/delibera/Delibera%207-24-CONS.pdf

Allegato A, Linee guida:
https://www.agcom.it/sites/default/files/migration/attachment/Allegato%2016-1-2024.pdf

Allegato B, Tavolo tecnico:
https://www.agcom.it/sites/default/files/migration/attachment/Allegato%2016-1-2024%201705401286701.pdf

2024/2(30)EG

30. Il nuovo documento di indirizzo del Garante privacy italiano del 6.6.2024 sulla gestione della posta elettronica dei lavoratori e sul trattamento dei metadati

ISSN 2239-8570

Con Provvedimento n. 364 del 6 giugno 2024 (di seguito il **Provvedimento**), il Garante per la Protezione dei Dati personali (di seguito il **Garante** o l'**Autorità**), è tornato sulla questione relativa alla conservazione dei metadati contenuti nella posta elettronica dei dipendenti, pubblicando la versione aggiornata del Documento di indirizzo denominato "*Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati*" (il **Documento di indirizzo**), la cui prima versione, adottata con Provvedimento n. 642 del 21 dicembre 2023, aveva creato molti dubbi ed era stata perciò seguita da un provvedimento di sospensione e dall'avvio di una consultazione pubblica (v. in questa Rubrica la notizia n. 10 del numero 1/2024 [2024/1(10)EG]). Le modifiche apportate al Documento di indirizzo attraverso il Provvedimento sono state dunque adottate in esito alla consultazione pubblica in risposta alle perplessità di chi reputava che la prima versione del Documento di indirizzo introducesse la necessità di un drastico cambiamento nelle policy di conservazione dei metadati delle e-mail dei dipendenti. Il Provvedimento, come chiarisce il Garante, ha l'obiettivo "*di apportare specifiche modifiche e integrazioni* […] *nella prospettiva di agevolare, altresì, la comprensione dell'ambito dei trattamenti presi in considerazione e delle indicazioni fornite al fine di promuovere la consapevolezza delle scelte tecniche e organizzative dei datori di lavoro, in qualità di titolari del trattamento* […]". Tuttavia, esso non mira ad introdurre "*nuovi adempimenti a carico dei titolari del trattamento, ma intende offrire una ricostruzione sistematica delle disposizioni applicabili in tale specifico ambito*". Il solo fine è quello di *"fornire ai datori di lavoro indicazioni in ordine alla possibilità di trattare tali informazioni per consentire il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali garanzie di sicurezza informatica, senza necessità di attivare la procedura di garanzia prevista dall'art. 4, comma 1, l. 20/5/1970, n. 300, espressamente richiamata dall'art. 114 del Codice* [il D.lgs. 196/2003: Codice privacy]".

In poche parole, il Provvedimento ha dichiaratamente mera natura "orientativa" e di indirizzo, non essendo prescrittivo e non discendendo da esso nuovi adempimenti o responsabilità a carico dei datori di lavoro.

Vediamo di seguito le novità.

Il concetto di "metadati"

In primo luogo, il Garante indica con maggiore precisione l'ambito di applicazione del Documento di indirizzo, tramite la definizione tecnica di "metadato". Nel Documento di indirizzo, come emendato dal Provvedimento, i metadati rappresentano quelle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = *Mail Transport Agent*) e dalle postazioni client (MUA = *Mail User Agent*). In sintesi, sono metadati ai fini del Provvedimento:

- indirizzi e-mail di mittente e destinatario;
- indirizzi IP dei server o dei client coinvolti;
- gli orari di invio, di ritrasmissione o di ricezione;
- la dimensione del messaggio;
- la presenza e la dimensione di eventuali allegati;

ISSN 2239-8570

- l'oggetto del messaggio spedito o ricevuto (in relazione al sistema di gestione del servizio di posta elettronica utilizzato).

Si tratta, dunque, di dati registrati automaticamente dai sistemi di posta elettronica, indipendentemente dalla "*percezione e dalla volontà*" dell'utente. Ad ogni modo – specifica il Garante - tali dati "*non vanno in alcun modo confusi con le informazioni contenute nei messaggi di posta elettronica nella loro "body-part" (corpo del messaggio) o anche in essi integrate* […] *a formare il cosiddetto envelope,* […] *Le informazioni contenute nell'envelope, ancorché corrispondenti a metadati registrati automaticamente nei log dei servizi di posta, sono inscindibili dal messaggio di cui fanno parte integrante e che rimane sotto l'esclusivo controllo dell'utente (sia esso il mittente o il destinatario dei messaggi)*". Pertanto, chiarisce il Garante, le indicazioni del Documento di indirizzo relative ai tempi di conservazione "*non riguardano i contenuti dei messaggi di posta elettronica […] che rimangono nella disponibilità dell'utente/lavoratore, all'interno della casella di posta elettronica attribuitagli*".

Le (nuove) tempistiche di conservazione dei metadati

Secondo l'Autorità, la raccolta e la conservazione dei metadati come sopra definiti, non richiede l'esperimento delle garanzie di cui all'art. 4 comma 1 dello Statuto dei Lavoratori (accordo sindacale o dell'autorizzazione pubblica) solo quando:

i. avviene per "*assicurare il funzionamento delle infrastrutture del sistema della posta elettronica*";
ii. avviene per un periodo limitato che non dovrebbe superare 21 giorni (estendendo così il precedente limite di 7 giorni).

In questi due casi la raccolta e la conservazione dei metadati è consentita poiché verosimilmente funzionale a consentire l'assolvimento degli obblighi che discendono dal contratto di lavoro e, in particolare, funzionale a garantire l'esecuzione della prestazione lavorativa ai sensi dell'art. 4, comma 2 Statuto dei Lavoratori (l. 20 maggio 1970, n. 300).

Secondo il Garante, il datore di lavoro/titolare può superare il limite di 21 giorni di conservazione dei metadati solo sulla base di una comprovata valutazione delle specifiche esigenze tecniche e aziendali che legittimano tale necessità. Ad ogni modo, si legge nel Provvedimento che "*spetta in ogni caso al titolare adottare tutte le misure tecniche ed organizzative per assicurare il rispetto del principio di limitazione della finalità, l'accessibilità selettiva da parte dei soli soggetti autorizzati e adeguatamente istruiti e la tracciatura degli accessi effettuati*".

Di contro, la generalizzata raccolta e conservazione dei log di posta elettronica per un lasso di tempo più esteso, può determinare un "indiretto controllo a distanza" dell'attività dei lavoratori, richiedendo perciò l'esperimento delle garanzie previste dall'art. 4, comma 1 dello Statuto dei Lavoratori. In effetti, aggiunge il Garante: "*la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, per un periodo di tempo esteso, in assenza di idonei presupposti giuridici, può comportare la possibilità per il datore di lavoro di acquisire, informazioni riferite alla sfera personale o alle opinioni dell'interessato e quindi non*

ISSN 2239-8570

rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".

Il rispetto dei principi di correttezza e trasparenza

Tra le misure che il titolare del trattamento/datore di lavoro deve adottare, vi è anche – specifica il Garante – l'aggiornamento delle informative rivolte ai dipendenti, poiché "*è essenziale che gli interessati siano resi pienamente consapevoli delle complessive caratteristiche del trattamento (specificando i tempi di conservazione dei dati, gli eventuali controlli, ecc.)".*

Il rapporto tra datore di lavoro e fornitori di servizi di posta elettronica

Il Provvedimento, infine, richiama l'attenzione dei fornitori dei servizi di posta elettronica sulla necessità di contribuire a far sì che i titolari del trattamento possano adempiere ai loro obblighi di protezione dei dati, "*contemperando le esigenze di commercializzazione su larga scala dei propri prodotti con la conformità degli stessi ai principi del Regolamento, anche nella prospettiva di migliorare il prodotto offerto, sotto il profilo della sua maggiore conformità al Regolamento*". L'Autorità, dunque, rivolge ai fornitori un richiamo esortandoli ad una collaborazione attiva con i titolari, sebbene spetti sempre a questi ultimi "*verificare che i programmi e servizi informatici di gestione della posta elettronica in uso ai dipendenti - specialmente nel caso in cui si tratti di prodotti di mercato forniti in modalità cloud o as-a-service - consentano al cliente (datore di lavoro) di rispettare la disciplina di protezione dei dati nei termini indicati nel presente documento di indirizzo, anche con riguardo al periodo di conservazione dei metadati* ".

Conclusioni

Il Garante conclude esplicitando che i datori di lavoro pubblici e privati dovranno:

i. adottare le misure necessarie a conformare i propri trattamenti alla disciplina di protezione dati e a quella di settore;
ii. verificare che i programmi e i servizi informatici di gestione della posta elettronica consentano di rispettare la disciplina di protezione dei dati, anche con specifico riferimento al periodo di conservazione dei metadati;
iii. osservare le indicazioni sulle misure tecniche e organizzative evidenziate dal Comitato Europeo per la Protezione dei Dati nel documento denominato "*2022 Coordinated Enforcement Action Use of cloud-based services by the public sector*"
iv. garantire, in particolare, che i fornitori dei servizi cloud trattino i dati personali solo per conto dei rispettivi titolari e sulla base delle istruzioni da questi ricevute.

ELISA GROSSI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10026277

ISSN 2239-8570

2024/2(31)SB

31. La nota informativa del Garante privacy del 20.5.2024 sul web scraping

Il 20 maggio 2024, il Garante per la Protezione dei Dati Personali (il "**Garante**") ha pubblicato una nota informativa (la "**Nota**") sulle possibili azioni di contrasto al fenomeno del web scraping, tecnica impiegata dagli sviluppatori di sistemi di intelligenza artificiale generativa per alimentare e addestrare gli algoritmi alla base degli stessi sistemi di IA.

La Nota giunge al termine della relativa indagine conoscitiva avviata dal Garante il 21 dicembre 2023 e, sebbene non formalmente vincolante, costituisce una prima importante posizione del Garante su una tematica così attuale e allo stesso tempo sensibile. È doveroso evidenziare che la Nota non tratta della conformità della tecnica del web scraping alla normativa privacy, piuttosto, come detto, si sofferma sulle possibili tecniche di contrasto al web scraping, in particolare su quelle attuabili da parte dei gestori dei siti e delle piattaforme da cui i bot che attuano il web scraping raccolgono i dati impiegati per addestrare gli algoritmi di IA.

È noto, infatti, che i sistemi di IA generativa – specialmente quelli basati sui modelli linguistici di grandi dimensioni (LLM – Large Language Models) – per riuscire a produrre contenuti (i c.d. output che vengono creati dopo che il sistema ha ricevuto un prompt) devono ricorrere all'elaborazione massiva di dati. Gli algoritmi alla base dei sistemi di IA generativa si nutrono di dati senza i quali non potrebbero creare contenuti e adattarsi ed imparare.

La necessità di addestrare il sistema di IA con quantità ingenti di dati porta gli sviluppatori di sistemi di IA generativa a costituire grandi dataset; i dataset, a loro volta, vengono alimentati da appositi software (i c.d. bot) impiegati per scandagliare il web e raccogliere in modo sistematico, continuativo, indiscriminato e massivo (da qui, web scraping) dati, anche di natura personale, pubblicamente presenti sui siti e sulle piattaforme di terze parti. Ciò genera, quindi, problemi circa la compatibilità della raccolta dei dati con le norme poste a tutela dei dati personali e, più in generale, con il Regolamento (UE) 2016/679 (c.d. GDPR).

Come ha ricordato il Presidente del Garante, Prof. Pasquale Stanzione, nel suo discorso introduttivo alla Relazione Annuale del Garante per il 2023, presentata a Roma il 3 luglio 2024 alla Camera dei Deputati: "*la disciplina di protezione dei dati regola (e continuerà a farlo anche dopo l'AI Act) il fulcro dell'intelligenza artificiale: il trattamento di dati personali funzionale a processi decisionali automatizzati e all'addestramento dell'algoritmo*".

La Nota, pur non affrontando direttamente il problema della compatibilità del web scraping con la normativa di cui al GDPR, fornisce alcune indicazioni circa gli strumenti che i gestori dei siti e delle piattaforme, *in quanto titolari del trattamento dei dati personali pubblicamente disponibili sui loro siti o sulle loro piattaforme*, possono

ISSN 2239-8570

implementare per bloccare o mitigare la raccolta massiva dei dati tramite il web scraping.

Le misure indicate dal Garante sono quattro, di cui tre di natura prettamente tecnica ed una di natura giuridico contrattuale.

Quanto alle misure di natura tecnica, il Garante suggerisce: **(i)** la creazione di aree riservate sul sito o sulla piattaforma, con l'avvertenza che tale misura andrebbe contemperata con il principio di minimizzazione dei dati, ex art. 5(1)(c) GDPR, per non onerare gli utenti dei siti e delle piattaforme di eccessivi oneri per la fruizione dei contenuti presenti sui siti e sulle piattaforme medesime; **(ii)** il monitoraggio del traffico di rete sia in entrata ai siti e alle piattaforme che in uscita dalle stesse, così da adottare, nel caso di flussi anomali, tecniche di *rate limiting* cioè tecniche che consentono di limitare il numero di richieste di accesso ad un sito o ad una piattaforme solo a determinati indirizzi IP; **(iii)** l'adozione di misure in grado di intervenire sui bot impedendone l'operatività di scraping, ciò che può realizzarsi ad es. tramite le c.d. CAPTCHA (le quali, imponendo un'azione eseguibile solo da un essere umano, impediscono l'operatività dei bot) o per mezzo di file robots.txt cioè file che consentono o impediscono ai bot scraper di accedere al sito o comunicano ai bot scraper quali pagine e contenuti del sito non indicizzare, con l'avvertenza, anche qui, che l'impiego dei file robots.text non impedisce realmente lo scraping in quanto: a) il bot scraper non accede ad un sito o ad una piattaforma e non ne indicizza i contenuti se a monte non è programmato per rispettare il divieto che incontra da parte dei file robots.txt; b) ci sono attività di web scraping che non vengono attuate per raccogliere dati per addestrare una IA, riuscendo così a bypassare il divieto posto dai file robots.txt.

Quanto alla misura di carattere giuridico, il Garante suggerisce di inserire nei termini di servizio dei siti o delle piattaforme una clausola concernente il divieto di web scraping. Qui il rimedio può assolvere ad una funzione di deterrenza del web scraping, ma probabilmente diventa maggiormente utile ex post, in sede di eventuale contenzioso per inadempimento contrattuale tra il gestore del sito o della piattaforma online e lo sviluppatore dell'IA generativa.

Infine, lo stesso Garante, da un lato, prende atto che nessuna delle misure suggerite è in grado di bloccare al 100% il web scraping, e, dall'altro lato, non manca però di ricordare che i gestori dei siti e delle piattaforme, in quanto titolari dei dati personali ivi pubblicati, devono comunque adoperarsi per valutare le misure più idonee da adottare sulla base del principio di accountability (artt. 5 e 25, GDPR) al fine di impedire l'utilizzazione, ritenuta non lecita, dei dati personali presenti sui loro siti o piattaforme. E sebbene la Nota non sia formalmente vincolante, di fatto, potrebbe essere considerata come vincolante proprio per il richiamo rivolto ai gestori dei siti o delle piattaforme di prendere in esame le misure più adeguate a prevenire o a mitigare il web scraping sulla base del loro obbligo di accountability. Secondo quanto illustrato dal Prof. Stanzione nel suo discorso introduttivo alla Relazione annuale 2023, sembrerebbe questo anche l'approccio del Garante: "*Particolare rilievo assume anche il provvedimento sul webscraping, recante alcune garanzie essenziali (e, per converso,*

ISSN 2239-8570

adempimenti a carico dei titolari) *per impedire che le nostre vite si traducano – come si è detto - in alimento per gli algoritmi*" (enfasi, nostra).

STEFANO BARTOLI

Nota informativa:
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10020316

Relazione annuale 2023 e discorso del Presidente del Garante:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10032023

2024/2(32)SB

32. Web scraping e analisi del rischio fiscale: il Parere del Garante privacy italiano dell'11.1.2024 sullo schema del decreto legislativo sul concordato fiscale

In tema di web scraping, già prima della Nota informativa del 20.5.2024 (sulla quale v. la notizia precedente in questa Rubrica), il Garante per la protezione dei dati personali aveva preso una posizione nell'ambito di un più ampio parere, reso l'11.1.2024 "*su uno schema di decreto legislativo recante disposizioni in materia di accertamento tributario e di concordato preventivo biennale*" (il "**Parere**").

Pur senza utilizzare l'espressione «web scraping», il Garante ha in quella sede rilevato alcune criticità connesse agli strumenti di cui il Governo avrebbe voluto dotare l'Agenzia delle entrate e la Guardia di finanza ai fini della c.d. analisi del rischio fiscale (cioè, l'analisi dei dati dei contribuenti e tesa a prevenire e contrastare l'evasione fiscale, la frode fiscale e l'abuso del diritto in materia tributaria, nonché a consentire un migliore svolgimento dei controlli preventivi e così a stimolare l'adempimento spontaneo dei contribuenti) e del concordato preventivo biennale riservato ai contribuenti di minori dimensioni. Il riferimento, qui, è in particolare all'art. 2 dell'allora schema di d.lgs. a mente del quale l'Amministrazione finanziaria, ai fini dell'analisi del rischio fiscale, si sarebbe potuta avvalere di sistemi di intelligenza artificiale, utilizzando, oltre ai dati conservati nelle proprie banche dati, anche dati pubblicamente disponibili (art. 2, commi 1 e 3, dello schema di d.lgs.), mentre la Guardia di finanza, nella propria attività di accertamento, avrebbe potuto ricorrere a non meglio specificate "tecniche di analisi avanzate" (art. 2, co. 8, dello schema di d.lgs.).

Nel Parere, il Garante ha indicato di espungere tali previsioni o perché di natura indeterminata (quanto alle tecniche avanzate) o perché l'elaborazione dei dati attraverso l'acquisizione di informazioni pubblicamente disponibili sarebbe stata priva dei necessari requisiti di affidabilità, anche tenendo conto delle diverse finalità che avevano dato origine alla loro raccolta.

ISSN 2239-8570

Nel Parere, si avverte la preoccupazione per l'uso di sistemi di IA che, sulla base di dati acquisiti in modo massivo ed indiscriminato e, quindi, non certi, avrebbe potuto dare luogo a risultati distorti.

L'attinenza delle osservazioni svolte nel Parere con la più ampia tematica del web scraping è stata segnalata dal Presidente del Garante per la protezione dei dati personali.

Come rilevato dal Prof. Stanzione nel suo discorso di presentazione della Relazione annuale per il 2023: "*I limiti del webscraping sono stati sottolineati anche rispetto alla riforma fiscale, nel cui ambito il ricorso all'intelligenza artificiale esige requisiti stringenti di affidabilità ed esattezza dei dati utilizzati per la profilazione del contribuente. Se addestrato su dati anche soltanto parzialmente inesatti, infatti, l'algoritmo restituirà risultati errati in proporzione geometrica, con bias che dalla base informativa si propagano lungo tutto l'arco della decisione algoritmica. Per questo, ad esempio, nel parere sul decreto legislativo, sul concordato preventivo, è stato richiesto di espungere un riferimento che avrebbe potuto legittimare analisi del rischio fiscale fondate anche sul webscraping*".

STEFANO BARTOLI

Parere sullo schema di d.lgs. per la riforma fiscale:
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978230

Relazione annuale 2023 e discorso del Presidente del Garante:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10032023

2024/2(33)GD

33. Il provvedimento AGCM contro Meta del 21.5.2024 per pratiche commerciali ingannevoli relative ad informazioni fornite ed omesse agli utenti dei servizi Instagram e Facebook (PS12566)

Con Provvedimento n.31214 del 21.5.2024, pubblicato il 5.6.2024 (*PS12566 - META-PROBLEMATICHE ACCOUNT INSTAGRAM E FACEBOOK*), l'Autorità Garante della Concorrenza e del Mercato (**AGCM** o l'**Autorità**) ha irrogato una sanzionato pari a 3,5 milioni di euro nei confronti di Meta Platforms Ireland Ltd. e della capogruppo Meta Platforms Inc. (**Meta** o la **Società**) per due pratiche commerciali ingannevoli.

La prima pratica consiste nell'omessa informativa in fase di attivazione e prima registrazione dell'account Instagram (**IG**) dell'attività di raccolta e utilizzo, per finalità commerciali, dei dati degli utenti, così da indurli ad assumere una decisione di natura commerciale che non avrebbero altrimenti preso (registrazione nella piattaforma IG per usufruire dell'omonimo servizio di social network).

ISSN 2239-8570

La seconda pratica riguarda, invece, gli utenti già registrati alle piattaforme Facebook (**FB**) e IG e consiste nell'omessa informativa circa le ragioni legate ad alcune interruzioni del servizio di FB e IG, limitando il contraddittorio sulle relative cause.

Con riferimento alla prima pratica, nella pagina web di registrazione a IG risultava di immediata evidenza il claim "***Iscriviti per vedere le foto e i video dei tuoi amici***", mentre in fondo alla schermata di registrazione era presente la dicitura generica "***scopri in che modo [...] usiamo e condividiamo i tuoi dati***" senza ulteriori indicazioni, unitamente ai link iperterstuali "***Condizioni"***, "***Informativa sulla privacy***" e "***Normativa sui cookie***". In questo modo per l'utente non era possibile comprendere sin dalla prima schermata l'uso dei dati per fini commerciali, che poteva ricavarsi solo cliccando su diversi link, con rinvii da una sezione all'altra del sito.

Nel corso dell'istruttoria, il 25 marzo 2024, Meta ha introdotto il disclaimer "***Noi finanziamo i nostri servizi usando i tuoi dati personali per mostrarti le inserzioni***", già presente nel processo di registrazione via *app*, anche nella pagina web di registrazione a IG. Cliccando su tale dicitura, l'utente viene reindirizzato direttamente alla sezione delle condizioni d'uso di IG relative alle modalità di finanziamento del servizio medesimo.

A seguito di questa modifica, l'AGCM ha ritenuto sanata l'omessa informativa, ma ha comunque sanzionato Meta per la pratica scorretta posta in essere dal 28 marzo 2023 fino al 25 marzo 2024.

Per la prima pratica l'AGCM ha irrogato a Meta una sanzione di 3 milioni di euro, anche in considerazione della "*circostanza aggravante"*, costituita dal fatto che Meta ha parzialmente reiterato la condotta già sanzionata dalla stessa Autorità nel 2018 (provv. n. 27432 del 29.11.2018, proc. PS11112, *Facebook-Condivisione Dati con Terzi* - parzialmente annullato da TAR Roma, I, sentenza n. 261/2020, e Cons. Stato, VI, sentenza n. 2631/2021).

In particolare, l'AGCM nel 2018 aveva ritenuto che Facebook (*i.e.*, le allora Facebook Inc. e Facebook Ireland Ltd., oggi Meta) mediante la piattaforma FB avesse ***(A)*** raccolto e trattato in modo fuorviante i dati dei consumatori/utenti, pubblicizzando i propri servizi come "gratuiti", senza informarli che i dati sarebbero stati utilizzati per finalità commerciali, ossia sarebbero stati oggetto di sfruttamento diretto mediante la loro commercializzazione; e/o ***(B)*** implementato un sistema *opt-out* attraverso cui i dati degli utenti sarebbero stati raccolti automaticamente e trasferiti a soggetti terzi per finalità di profilazione e commerciali. In quel caso, il TAR e il Consiglio di Stato avevano annullato parzialmente il provvedimento dell'AGCM, ritenendo assenti i presupposti della condotta *sub* B e confermando l'ingannevolezza della condotta *sub* A.

Con riferimento alla seconda pratica, secondo l'AGCM, in occasione della sospensione dei servizi di FB e IG, disposta da Meta a fronte di violazioni degli utenti della *policy* delle piattaforme, la Società avrebbe omesso: ***i)*** con riguardo alla piattaforma FB, di indicare le modalità (automatizzata o manuale) con cui veniva assunta la decisione di sospendere l'*account*, ossia di interrompere il servizio; ***ii)*** con riguardo a entrambi i

ISSN 2239-8570

social network (FB e IG), di fornire indicazioni circa la possibilità di contestare la decisione di sospensione l'*account*, oltre che con "ricorso interno" diretto a Meta, anche adendo un organo di risoluzione extragiudiziale delle controversie o ricorrendo a un giudice, nonché per aver previsto un termine breve (di 30 giorni) per contestare tramite "ricorso interno" la decisione di sospensione dell'*account*.

A partire dal mese di agosto 2023, Meta ha modificato il *set* informativo reso all'utente, sia di FB che di IG, in occasione dell'applicazione di misure restrittive dell'*account*. Pertanto, l'AGCM ha ritenuto sanata l'omessa informativa, ma ha comunque irrogato a Meta una sanzione di 500.000 euro per la seconda pratica scorretta, posta in essere dal 28 marzo 2023 fino al mese di agosto 2023.

L'Autorità aveva avviato l'istruttoria nei confronti di Meta anche per una terza condotta relativa alla presunta omessa assistenza agli utenti impossibilitati ad accedere ai propri *account*. Nel corso dell'istruttoria Meta ha dimostrato di fornire un'assistenza avanzata e adeguata a risolvere i problemi di accesso degli utenti ai propri *account*, ivi inclusi quelli compromessi da attacco *hacker*. Di conseguenza, l'AGCM ha ritenuto legittimo l'operato di Meta al riguardo.

Il provvedimento in questione, sulla scia della precedente casistica (caso *Facebook*, provv. n. 27432 del 29.11.2018, proc. PS11112, *Facebook-Condivisione Dati con Terzi*; caso *WhatsApp*, provv. dell'AGCM dell'11.5.2017, n. 26597, proc. n. PS10601, *Trasferimento Dati a Facebook*), dimostra come l'Autorità sia molto attenta, tra le altre cose, nel valutare condotte ritenute potenzialmente idonee ad ingannare i consumatori sulle modalità di utilizzo dei loro dati nell'ambito di piattaforme digitale.

GIORGIA DIOTALLEVI

https://www.agcm.it/dotcmsdoc/bollettini/2024/23-24.pdf

2024/2(34)VR

34. L'ordinanza della Cassazione 12967 del 13.5.2024 sul caso del sistema software di supervisione degli studenti 'Respondus' impiegato dall'Università Bocconi di Milano per le prove scritte di esame

Il 13 maggio 2024 la Sez. I della Corte di Cassazione, con l'ordinanza n. 12967, si è pronunciata sulla vicenda relativa all'impiego da parte dell'Università Bocconi di Milano del software *"Respondus"* per la supervisione degli studenti durante le prove scritte di esame effettuate da remoto.

Come già illustrato (v. in questa Rubrica notizia n. 8 del numero 4/2021 [2021/4(8)VR]), il trattamento effettuato a mezzo del menzionato sistema di c.d. *proctoring* veniva dichiarato illecito dal Garante per la protezione dei dati personali (di seguito **Garante privacy** o l'**Autorità**) con ordinanza

ISSN 2239-8570

adottata il 16 settembre 2021, ai sensi degli artt. 78 Regolamento UE n. 2016/679 (**GDPR**), 152 d.lgs. n. 196/2003 (**Codice privacy**) e 10 del d.lgs. n. 150/2011, per violazione gli artt. 5(1)(a), (c) ed (e), 6, 9, 13, 25, 35, 44 e 46 GDPR nonché 2-*sexies* Codice privacy.

L'Ateneo impugnava il suddetto provvedimento innanzi al Tribunale di Milano (di seguito anche solo il **Tribunale**). Quest'ultimo accoglieva parzialmente il ricorso: confermando l'ordinanza dell'Autorità limitatamente alla contestazione di cui agli artt. 5(1)(a) e 13 GDPR e all'applicazione dell'art. 58 GDPR; riducendo l'importo della sanzione irrogata e, per l'effetto, condannando il Garante privacy alle restituzioni.

Il *rationale* del giudice di merito può condensarsi nei due punti che seguono.

Doveva anzitutto escludersi l'applicazione al caso di specie dell'art. 9 GDPR, in quanto il trattamento effettuato a mezzo del sistema *Respondus* non poteva qualificarsi come avente a oggetto dati biometrici *«intesi a identificare in modo univoco una persona fisica»*. Precisamente, la mera acquisizione di una foto (o di una registrazione video) non configurerebbe un trattamento di dati biometrici bensì di dati comuni, implicando il primo la più complessa estrazione dalle foto o dai video di caratteristiche biologiche e la successiva derivazione da quest'ultime di un modello matematico del volto del soggetto, a fini di riconoscimento dello stesso. Tale finalità non era contemplata nel *software* in oggetto, poiché esso lasciava ogni eventuale valutazione al docente titolare dell'insegnamento. Pertanto, non risultava dimostrata la concreta attuazione della fase quattro (del confronto o del *match*), enucleata dalle Linee guida in materia di riconoscimento biometrico e firma grafometrica adottate dal Garante il 12 novembre 2014.

Inoltre, il Tribunale di Milano affermava che l'Accordo sottoscritto in data 18 agosto 2020 tra l'Università Bocconi e la società fornitrice *Respondus* fosse tale da impedire il "*trasferimento internazionale*" dei dati personali, essendovi allegate clausole tipo idonee a garantire agli interessati una tutela adeguata rispetto agli standard europei. Di poi, la "pseudonomizzazione", impiegata per denominare i dati acquisiti in relazione a ciascuna persona, veniva ritenuta misura di protezione adeguata.

Simmetricamente, il Garante privacy proponeva impugnazione rappresentando quanto segue.

Col **primo motivo di ricorso** si denunciava la violazione e falsa applicazione degli artt. 6 e 9(2)(g) GDPR e 2-*sexies*(2)(b) Codice privacy.

La Cassazione ha accolto il motivo, muovendo da una ricostruzione sistematica del regime giuridico sui dati biometrici, nei termini di seguito riassunti. Nel diritto dell'Unione europea i dati biometrici sono dati personali se impiegati per identificare in modo univoco una persona. Il trattamento di tali dati è regolato in tre plessi normativi: art. 4 n. 14 GDPR; art. 3 n. 13 direttiva (UE) 2016/680 (è la direttiva c.d. *law enforcement*, sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati);

ISSN 2239-8570

art. 3 n. 18 regolamento (UE) 2018/1725 (è il regolamento c.d. EUDPR, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati). Tali plessi normativi convergono nel definire i dati biometrici come *«i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».* Il regime giuridico del trattamento, tuttavia, varia in base alla finalità disciplinare specificamente perseguita. Ancora, il Considerando n. 51 del GDPR preclude un'automatica considerazione del trattamento di fotografie come trattamento di categorie particolari di dati personali, *«poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica».* Ove ciò accada, l'art. 9(1) GDPR vieta il trattamento dei dati biometrici intesi a identificare in modo univoco una persona fisica a meno che non si dia una delle basi giuridiche di cui al par. 2 del medesimo articolo: a rilevare, nel caso di specie, sono il consenso esplicito dell'interessato (art. 9(2)(a) GDPR) e, soprattutto, la necessità del trattamento per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9(2)(g) GDPR).

A livello domestico, l'art. 2-*sexies* Codice privacy conferma l'ammissibilità dei trattamenti delle categorie particolari di dati personali di cui all'articolo 9(1) GDPR, ove necessari per motivi di interesse pubblico rilevante ai sensi della lett. g) del paragrafo 2 del medesimo articolo, e specifica, al comma 2, che si considera rilevante – *inter alia* – l'interesse pubblico relativo a trattamenti effettuati da soggetti che operano istituzionalmente nella materia dell'istruzione e formazione in ambito scolastico, professionale, superiore o universitario.

In ogni caso, il trattamento dei dati biometrici dovrà essere proporzionato alla finalità perseguita (art. 9(2)(b) GDPR). Inoltre, esso dovrà soddisfare i principi di cui all'art. 5 del GDPR e le condizioni di liceità *ex* art. 6 del GDPR (cfr. CGUE, 16 gennaio 2019, *Deutsche Post*, C-496/17, EU-C/2019/26, punto 57 e giurisprudenza ivi citata), anche in linea col c.d. principio di "responsabilizzazione (art. 5, par. 2 GDPR).

Come anticipato, secondo il giudice di merito *Respondus* realizzava la mera acquisizione di una foto (o una registrazione video) e non integrava dunque un trattamento di dati biometrici, precisamente in quanto l'identificazione univoca dello studente persona fisica era effettuata dal docente esaminante il video finale e non derivava dai dati biometrici raccolti e trattati dal *software*.

Secondo i giudici di legittimità, tale conclusione era viziata da un errore di sussunzione.

Il *software Respondus* non si limita a videoregistrare la prova di esame, bensì acquisisce immagini dell'esaminando persona fisica e seleziona, mediante la realizzazione di video, lo scatto di istantanee a intervalli casuali e i momenti in cui rileva comportamenti insoliti. In altri termini, le istantanee selezionate vanno a comporre un video destinato al docente ai fini

ISSN 2239-8570

della valutazione finale della regolarità della prova e in esso sono contrassegnate le anomalie riscontrate. Pertanto, i dati estratti da *Respondus* non assolvono solo la funzione di documentare la seduta, ma si connotano per la contestuale elaborazione e selezione del materiale progressivamente raccolto. Tale complessiva attività integra un autonomo e articolato trattamento di dati e attiene anche alla conferma dell'identità della persona fisica esaminata (art. 4, n.14 GDPR).

Non solo. Come ricordato dallo stesso Tribunale, il ciclo di vita dei dati biometrici è stagliato in quattro fasi, secondo la Descrizione accreditata dal Garante privacy (Linee Guida in materia di riconoscimento biometrico e firma grafometrica, 12 novembre 2014): *a*) il rilevamento, tramite sensori specializzati (*e.g.* scanner per il rilevamento dell'impronta digitale) o dispositivi di uso generale (*e.g.* videocamera), di caratteristiche biometriche; *b*) l'acquisisce un campione biometrico (*e.g.* immagine del viso); *c*) l'estrazione dal campione biometrico di tratti (*e.g.* specifici punti del viso) idonei a costituire il modello biometrico, che sarà conservato in una banca dati; *d*) il confronto (*match*) tra il modello biometrico e le effettive caratteristiche dell'individuo ai fini della identificazione univoca della persona fisica.

Ebbene, la decisione di merito trascurava di considerare che nel procedimento attuato mediante il software *Respondus*, la quarta fase di confronto avveniva nel corso di tutta la ripresa, sulla scorta della elaborazione informatica dei dati di volta in volta acquisiti ed elaborati mediante la creazione di *flag* relativi ai comportamenti anomali, che potevano riguardare anche la conferma della corrispondenza identitaria della persona ripresa in video con quella dello studente da esaminare, già identificato dall'Università. Inoltre, l'affidamento al docente della valutazione conclusiva della prova di esame non esclude (né è incompatibile con) il trattamento automatizzato dei dati biometrici e non lo sottrae alla disciplina dettata dall'art. 9 GDPR.

Per tali ragioni, la Corte ha anzitutto fissato il seguente principio di diritto: *«In tema di trattamento dei dati personali, ai sensi dell'art. 9 del Reg (UE) 2016/679, ricorre un trattamento di dati biometrici, come definiti dall'art. 4, n. 14 del Regolamento 2016/679, quando i dati personali sono ottenuti mediante un trattamento tecnico automatizzato specifico, realizzato con un software che, sulla base di riprese e analisi delle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, le elabora, evidenziando comportamenti o elementi anomali, e che perviene a un esito conclusivo, costituito da una elaborato video/foto che consente (o che conferma) l'identificazione univoca della persona fisica, restando irrilevante la circostanza che l'esito finale del trattamento sia successivamente sottoposto alla verifica finale di una persona fisica».*

Col **secondo motivo** si denunciava la violazione e falsa applicazione: degli artt. 44, 45 e 46 GDPR; degli artt. 3, 4 e 5 delle clausole contrattuali allegate alla Decisione della Commissione Europea n. 2010/87/UE; dell'art. 1321 c.c. Non solo. Il ricorrente impugnava la sentenza impugnata anche con riferimento al trasferimento internazionale dei dati personali e per aver

ISSN 2239-8570

il Tribunale di Milano ritenuto essere misura "adeguata" la pseudonomizzazione.

In primis, com'è noto, la sentenza della CGUE del 16 luglio 2020 (causa C-311/18), c.d. *sentenza Schrems II* (su cui v. in questa Rubrica la notizia n. 1 del numero 3/2020 [2020/3(1)CR]) la quale ha dichiarato invalida la decisione della Commissione n. 2016/1250 sull'adeguatezza della protezione offerta dal c.d. *Privacy Shield* (scudo UE-USA) circa il trasferimento di dati personali verso gli Stati Uniti, giudicando, invece, valida la decisione n. 2010/87 relativa alle Clausole Contrattuali Tipo (SCC). A seguito di tale decisione, l'Università Bocconi e la società *Respondus* perfezionavano in data 18 agosto 2020 un accordo col quale recepivano le clausole contrattuali tipo dettate nella decisione della Commissione europea n. 87/2010.

Il Tribunale di Milano riteneva che l'accordo così riformulato fosse tale da impedire il "*trasferimento internazionale*" di dati personali, proprio perché ad esso erano allegate le clausole tipo di cui alla Decisione 2010/87/UE, alle quali si faceva rinvio *per relationem*.

La Corte ha rifiutato la descritta argomentazione. Segnatamente, le clausole 4, par. 1, lett. *c*) e 5, lett. *c*) delle clausole standard prevedono espressamente che le misure di sicurezza debbano essere *«indicate nell'appendice 2»*, che peraltro *«costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti»*, e che tali disposizioni hanno efficacia anche con riferimento all'"interessato", terzo rispetto al contratto. Sulla scorta di tali elementi, non può ammettersi la determinazione *per relationem* del contenuto delle clausole contrattuali recanti le misure di sicurezza tramite rinvio a un documento esterno al contratto stesso, per frontale violazione della *lex contractus*. Inoltre, l'accordo in esame – assistito dalle clausole contrattuali tipo per il trasferimento di dati personali a soggetti stabiliti in paesi terzi – non obbliga solo i contraenti tra loro ma regola anche i diritti del terzo beneficiario. Quest'ultimi potrebbero ricevere nocumento, ove gli obblighi in materia di sicurezza non fossero oggettivamente individuati o individuabili.

Sul punto, merita evidenziare che la citata sentenza della CGUE c.d. *Schrems II* ha altresì precisato che la salvaguardia fondata su clausole tipo deve offrire ai soggetti i cui dati personali sono trasferiti verso un paese terzo un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea ("**CDFUE**"). A tal fine, occorre ancora osservare che l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo adottate dalla Commissione qualora ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dagli artt. 45 e 46 GDPR e dalla CDFUE, non possa essere garantita con altri mezzi.

Ebbene, nel caso in esame la mancata esplicitazione delle misure di sicurezza nell'allegato 2, in difformità da quanto da questo previsto, in una

ISSN 2239-8570

alla complessità della modalità di accesso informatico alle misure di sicurezza e all'incertezza sul relativo contenuto integrano circostanze che avrebbero dovuto essere espressamente valutate dal Tribunale in ordine all'applicabilità dell'art. 58(2)(f) e (j) GDPR.

Resta assorbita all'esito del riesame la questione introdotta della pseudonomizzazione dei dati, atteso che la decisione sul punto risulta inficiata dalla erronea qualificazione dei dati trattati come dati personali comuni piuttosto che come dati biometrici.

VALENTINO RAVAGNANI

Cass. 12967/2024

2024/2(35)EG

35. Il provvedimento del Garante privacy italiano del 9.5.2024 nei confronti di Wikipedia a proposito del diritto all'oblio

Con Provvedimento n. 274 del 9 maggio 2024 (d'ora in poi, il **Provvedimento**), il Garante per la protezione dei dati personali (il **Garante**) ha statuito che il trattamento dei dati personali effettuato dalla nota enciclopedia online "Wikipedia" deve rispettare i principi del regolamento (UE) 2016/679 (**GDPR**) e che ai contenuti pubblicati sulla piattaforma devono applicarsi le norme sull'attività giornalistica e la manifestazione del pensiero.

Il Provvedimento è stato emesso a seguito del reclamo di un interessato che lamentava una violazione della normativa in materia di protezione dei dati personali, in relazione alla pubblicazione su Wikipedia della notizia di una propria vicenda giudiziaria (risalente al 2017 e conclusasi nel 2018) che lo aveva visto imputato per reati di violenza sessuale e di detenzione di materiale pedopornografico.

Nello specifico, l'interessato rappresentava, tra le altre circostanze, che:

i. la diffusione dei suoi dati (nome, cognome, età, nazionalità e ruolo ricoperto) era avvenuta "*in chiaro e senza alcuna autorizzazione e/o preavviso*" e che la narrazione dei fatti che lo riguardavano era stata spesso "*travisata*";
ii. la vicenda, particolarmente delicata, non rivestiva più un interesse pubblico "*avendo la collettività ormai preso conoscenza del fatto*" e la relativa permanenza on-line causava un perpetuo danno all'immagine dell'interessato, con ripercussioni sui suoi rapporti familiari e professionali.

In ragione di quanto sopra, il reclamante accusava Wikipedia della violazione dell'art. 137(3) del D.Lgs. 196/2003 (**Codice Privacy**) e degli artt. 5(1)(e) e 17 GDPR, rilevando che il diritto di cronaca avrebbe dovuto affievolirsi a favore del rispetto della propria identità personale, non più sussistendo un apprezzabile interesse sociale alla notizia. Pertanto,

ISSN 2239-8570

richiedeva la rimozione da Wikipedia del predetto articolo e, in subordine, l'adozione di specifiche misure tecniche utili alla deindicizzazione.

Wikimedia Foundation (d'ora in poi **Wikimedia** o la **Fondazione**), la no-profit americana ideatrice dell'enciclopedia on line, replicava nel corso del procedimento di non essere vincolata al rispetto del GDPR, sia perché la propria sede è ubicata al di fuori dell'Unione Europea, sia perché Wikipedia non offre un servizio ad utenti europei: l'enciclopedia sarebbe solo un "*host neutrale*" che "*ospita*" i contenuti inseriti dalla comunità di volontari.

Tenuto conto di tutto quanto sopra esposto, con il Provvedimento, il Garante ha statuito, in primo luogo, che nel caso di specie deve ritenersi pienamente applicabile il GDPR, posto che Wikipedia offre servizi di informazioni su una vasta pluralità di argomenti, indicizzandoli anche per il mercato europeo. Ne sarebbero una dimostrazione la costante attività di indirizzo e verifica degli standard quantitativi dei contenuti rivolti dalla Fondazione alla comunità e la creazione di versioni del sito dedicati agli utenti degli Stati dell'Unione europea. La disponibilità e consultabilità degli articoli enciclopedici da parte di chiunque, concretizza – secondo il Garante – l'offerta di un servizio anche agli interessati europei, ai sensi dell'art. 3(2)(a) GDPR, "*tenuto conto di quell'elemento di 'intenzionalità', pure evidenziato nelle Linee-guida 3/2018 dell'EDPB*". Nel Provvedimento, il Garante ricorda, inoltre, che Wikipedia è stata inserita dalla stessa Commissione europea nell'elenco delle grandi piattaforme on-line tenute al rispetto degli obblighi previsti dal Regolamento (UE) 2022/2065 sui servizi digitali (**DSA**) (v. in questa Rubrica la notizia n. 5 nel numero 2/2023 [2023/2(5)RA]).

Chiarito l'ambito di applicazione, il Garante ha respinto l'istanza di cancellazione promossa dal reclamante, poiché il trattamento dei dati personali in oggetto risultava essere stato effettuato, all'epoca della pubblicazione della notizia, "*nell'esercizio del diritto di libera manifestazione del pensiero e rispondente all'interesse del pubblico a conoscere le vicende riportate all'interno del relativo articolo*".

Allo stesso modo – sottolinea il Garante - è lecita anche la permanenza dell'articolo nell'archivio dell'enciclopedia on line, poiché gli archivi di siti e giornali, anche cartacei, rivestono una funzione primaria ai fini della ricostruzione storica degli eventi.

Di contro, l'Autorità ritiene non sussistenti specifiche ragioni di interesse pubblico che giustifichino una perdurante reperibilità online dell'articolo al di fuori dell'archivio del sito, trattandosi di vicenda giudiziaria conclusasi nel 2018. Per di più, il Garante ha ritenuto che la presenza online della pagina vanificherebbe il beneficio del limite legale della conoscibilità posto alle condanne inferiori ai due anni che non sono inserite nel casellario giudiziario (ex art. 24(1)(2) Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di casellario giudiziale europeo, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).

In forza di quanto sopra, il Garante ha accolto la richiesta di deindicizzazione dell'articolo dai motori di ricerca esterni al sito web di Wikipedia, ordinando a Wikimedia ai sensi dell'art. 58(2)(c) e (g) di

ISSN 2239-8570

adottare misure tecniche idonee ad inibire l'indicizzazione dell'articolo, reperibile attraverso il link indicato nell'atto introduttivo del procedimento, tramite motori di ricerca esterni al sito medesimo, quali ad esempio, come espressamente indicato dalla stessa Fondazione, l'applicazione del metatag "NOINDEX".

ELISA GROSSI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10022403

2024/2(36)VR

36. Il Garante privacy italiano apre un'istruttoria per il progetto di videosorveglianza con riconoscimento facciale nelle stazioni metro di Roma

Come comunicato in data 9 maggio 2024, il Garante per la protezione dei dati personali (**Garante privacy** o l'**Autorità**) ha inviato a Roma Capitale (di seguito l'**Amministrazione**) una richiesta di informazioni circa un progetto di videosorveglianza da installare nelle stazioni della metropolitana.

L'iniziativa dell'Autorità è stata assunta poiché, secondo alcune fonti di stampa, in vista del prossimo Giubileo, l'Amministrazione avrebbe previsto di installare telecamere con tecnologia di riconoscimento facciale, *«in grado di verificare azioni scomposte»* all'interno dei vagoni e sulle banchine compiute da soggetti resisi in passato protagonisti di *«atti non conformi»*.

All'Amministrazione è stato dato un termine di 15 giorni per rispondere alla richiesta di informazioni del Garante privacy, che comprende, *inter alia*, una descrizione tecnica delle funzionalità di riconoscimento facciale, la finalità e la base giuridica di tale trattamento di dati biometrici e una copia della valutazione d'impatto sulla protezione dei dati (DPIA).

Il Garante ha, infine, ricordato che fino alla fine del 2025 vige una moratoria sull'installazione di impianti di videosorveglianza con sistemi di riconoscimento facciale attraverso l'uso di dati biometrici, in luoghi pubblici o aperti al pubblico, da parte delle autorità pubbliche o di soggetti privati. Tale trattamento è consentito solo all'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali e alle autorità pubbliche a fini di prevenzione e repressione dei reati, in ogni caso previo parere favorevole del Garante stesso.

VALENTINO RAVAGNANI

Comunicato stampa del 9.5.2024

2024/2(37)DI

ISSN 2239-8570

37. Il rapporto dell'aprile 2024 del Comitato di esperti nominato dal Presidente della Repubblica francese per studiare gli effetti dell'esposizione dei minori agli schermi: «*À la recherche du temps perdu*»

Il 23 aprile 2024 è stato pubblicato il documento *Enfants et écrans*: «*À la recherche du temps perdu*» ("**rapporto**"). Il rapporto è stato redatto da una commissione composta da dieci esperti (accademici, imprenditori, ricercatori impegnati nell'educazione) ("**commissione**"), istituita lo scorso gennaio 2024 su indicazione dell'attuale Presidente della Repubblica francese, Emmanuel Macron. Durante i lavori di stesura del rapporto, durati poco più di tre mesi, la commissione ha ascoltato i rappresentanti di associazioni attive nel campo della scuola, di attivisti a difesa della privacy, di istituti di ricerca sull'educazione, nonché di piattaforme digitali e dei principali social network (*Google*, *Meta*, *Apple*, *Youtube*, *X-Twitter*, *TikTok*, etc.).

Il rapporto ha ad oggetto la valutazione degli effetti dell'esposizione di minori (bambini ed adolescenti) a schermi (smartphone, pc, tablet, etc.) e la formulazione di raccomandazioni in merito a tale utilizzo. Esso muove da due aspetti, indicati nel preambolo. Il primo attiene alle innegabili possibilità delle tecnologie digitali di sviluppare la capacità dei bambini, consentendo altresì un accesso alla conoscenza che prescinde dall'ambiente socio-economico in cui l'utente opera. Il secondo riguarda la constatazione che la medesima tecnologia, come tutto ciò che è prodotto dall'uomo, possa essere utilizzata per isolare, alienare e manipolare gli utenti (in questo caso, i minori). Tale rischio è particolarmente acuito dalla circostanza per cui l'utilizzo degli schermi da parte dei minori avviene spesso in assenza dei genitori o adulti e senza alcuna misura di sicurezza. La commissione è consapevole che vi sia un certo consenso scientifico circa gli effetti nocivi dell'esposizione agli schermi sulla salute fisica dei minori (assenza di sonno, obesità, problemi alla vista). Rispetto ad altri possibili effetti negativi (neurologici), se del caso connessi all'utilizzo di detti schermi da parte di altri in presenza di minori (tecnoferenza), la commissione ritiene che, in attesa di studi consolidati, sia comunque opportuno procedere a una regolazione, la quale è considerata particolarmente urgente rispetto all'esposizione dei minori a immagini pornografiche, di estrema violenza, etc. Pur in assenza di una condivisa nozione di "dipendenza da schermo", infatti, la commissione considera che gli schermi, e in particolare l'uso dei social network, possano essere fattori di rischio aggiuntivi quando esiste una vulnerabilità preesistente in un bambino o in un adolescente (depressione o ansia).

Rispetto a questo contesto di conoscenze e valutazioni, il rapporto propone l'adozione di una trentina di misure di vario contenuto. Secondo gli autori, esse vanno accettate in blocco, giacché tali misure aspirano a costituire un sistema.

Sul piano descrittivo, le diverse misure possono essere articolate attorno a sei distinti temi ("*axes*").

ISSN 2239-8570

Il primo attiene al contrasto dell'effetto di dipendenza generato da alcuni servizi digitali e formula proposte (obblighi e divieti) tese a restituire ai bambini e agli adolescenti la libertà e la possibilità di fare scelte reali. Nell'ambito di questo tema, la commissione critica in particolare la tendenza di alcuni videogiochi a trasformarsi in modelli di gioco d'azzardo, con microtransazioni e design ingannevoli. Il secondo tema affrontato nel rapporto coinvolge la supervisione dell'attività dei minori tramite gli schermi. In luogo del solo controllo dei genitori, che ha dei limiti fisiologici, la commissione propone di impiegare delle soluzioni tecnologiche che consentano di aumentare la protezione dei minori dai contenuti illegali, qualunque sia il punto di accesso digitale (cellulare, box, Wi-Fi, a casa, a scuola, ecc.).

Il terzo tema concerne la promozione di un accesso graduale dei minori agli schermi e al loro utilizzo. Tale obiettivo dovrebbe consentire l'acquisizione di una autonomia per l'utente minore, proteggendo soprattutto i più giovani da usi e pratiche inappropriate. In quest'ottica, la Commissione propone dei limiti di età "di riferimento", che potranno essere regolarmente rivalutati. In tal senso, si propone di rafforzare l'attuale raccomandazione di non esporre i bambini di età inferiore ai 3 anni agli schermi e di sconsigliarne l'uso fino ai 6 anni, o almeno che esso sia molto limitato, occasionale, con contenuti educativi e accompagnato da un adulto. Con il medesimo intento, la Commissione ritiene che non sia opportuno che i bambini abbiano un telefono cellulare prima degli 11 anni, quando iniziano la scuola secondaria; a partire dagli 11 anni, se hanno un telefono, si raccomanda di non usarlo per connettersi a Internet; a partire dai 13 anni, se hanno un telefono connesso, non dovrebbero usarlo per accedere ai social network o a contenuti illegali; a partire dai 15 anni (età presa a simbolo del maggiorenne digitale), l'accesso ai social network dovrebbe essere limitato a quelli con un design appropriato.

Il quarto filone riguarda la raccomandazione di misure volte a sostenere i bambini e gli adolescenti nel mondo digitale, e a formarli sia dentro che fuori la scuola. Questa formazione deve essere più legata alle problematiche specifiche dei bambini e degli adolescenti; deve essere accompagnata sul territorio dalla visibilità di adulti di riferimento in grado di rispondere alle domande dei bambini e degli adolescenti, anche se desiderano porle in un contesto più intimo della classe.

La penultima questione attiene agli adulti, intesi come coloro che lavorano con i bambini e gli adolescenti, a partire dai genitori, e che devono dare l'esempio, senza il quale sarà difficile per i minori comprendere l'importanza del tema. Tale obiettivo domanda la promozione di tempi e luoghi "disconnessi", con l'organizzazione di rituali e di sfide simboliche di disconnessione, e l'esigenza di garantire il rispetto della vita dei genitori in un'epoca in cui il telelavoro si è diffuso, rendendo sempre più labile il confine tra vita personale e professionale.

L'ultima questione affrontata dal rapporto attiene alla *governance* di tale processo di regolazione. La commissione ritiene infatti che sia necessario, tra le altre cose, l'istituzione di un osservatorio che raccolga e monitori i dati principali sugli schermi e sulla diversità dei loro usi e la costruzione di

ISSN 2239-8570

un sistema di finanziamento dell'azione pubblica, della ricerca e dell'associazionismo che si basi sul dialogo con gli stessi attori digitali. Tale sistema potrebbe essere finanziato, in base al principio "chi inquina paga", con i proventi delle multe, o i costi di supervisione attualmente destinati alle sole autorità europee.

Infine, la Commissione chiede una strategia di comunicazione su larga scala, che metta in evidenza le legittime aspettative per lo sviluppo dei bambini e degli adolescenti, che trovi la sua routine nei momenti chiave della vita dei minori, che si affermi nel panorama pubblico come altri temi di salute pubblica sono riusciti a fare.

DANIELE IMBRUGLIA

https://tinyurl.com/yahxmnv9

2024/2(38)AAM

38. La legge del 17.4.2024 dello Stato del Colorado sul trattamento dei dati neurali nel contesto dei dispostivi neurotecnologici destinati al mercato dei prodotti di consumo (*Colorado House Bill 24-1058*) e la conseguente modifica del Colorado Privacy Act

Il recente sviluppo di dispositivi tecnologici sempre più avanzati, spesso basati sull'intelligenza artificiale, che consentono di individuare e decodificare l'attività cerebrale, ha dato luogo ad un ampio dibattito a livello internazionale circa la corretta regolamentazione giuridica di tali dispositivi e dei dati che da questi possono essere ricavati.

Già da tempo, infatti, le c.d. neurotecnologie hanno invaso il mercato dei prodotti di consumo (es. fasce per il wellness come *Insight*), non essendo più impiegate unicamente nell'ambito della ricerca sanitaria e riabilitativa, in ospedali e laboratori. Ciò da un lato comporta una forte spinta verso l'innovazione tecnologica e la crescita economica; dall'altro implica rilevanti rischi in tema di raccolta, trattamento e diffusione incontrollata di dati neurali.

Questi ultimi, per la complessità dei dispositivi il cui utilizzo ne determina la registrazione e il successivo trattamento, non hanno ancora una ben definita natura giuridica, mancando nella quasi totalità degli ordinamenti giuridici, sia di *Common Law* che di *Civil Law*, una esplicita regolamentazione degli stessi.

Il Cile con la "Ley n. 21.383 *Modifica La Carta Fundamental, Para Establecer El Desarrollo Científico Y Tecnológico Al Servicio De Las Personas*", del 25 ottobre 2021, è stato il primo Paese al mondo ad intervenire con una modifica legislativa per tutelare la mente umana da uno sviluppo tecnologico in grado di incidere negativamente sull'integrità psicofisica delle persone, modificando il primo comma, ultima parte dell'art. 19 della Costituzione cilena (*Constitución política de la Republica de Chile*) che attualmente prevede espressamente la protezione dell'attività

ISSN 2239-8570

cerebrale e delle informazioni da essa derivanti (su cui v. in questa Rubrica la notizia n. 12 nel numero 3/2023, che riguarda anche la prima sentenza al mondo resa in Cile sui "neuro-diritti" [2023/3(12)AAM]).

Da ultimo, negli Stati Uniti e precisamente nello Stato del Colorando, il legislatore è intervenuto con una specifica legge che definisce la nozione di "*biological data*" e "*neural data*" nell'ambito della disciplina a tutela dei dati personali dei consumatori.

La *Colorado House Bill 24-1058*, approvata il 17 aprile 2024 e che è entrata in vigore il 7 agosto 2024, focalizza in particolare l'attenzione su quelle tecnologie che comportano la raccolta di enormi quantità di dati personali connessi alle funzioni fisiche e mentali del relativo utilizzatore. Le "neurotecnologie" sono definite in tale legge come quei dispositivi in grado di "*recording, interpreting, or altering the response of an individual's central or peripheral nervous system to its internal or external environment"*, ovvero che possono monitorare, decodificare e manipolare l'attività cerebrale del suo utilizzatore (*Section 1, point 2, lett. c*). Si precisa ancora come le neurotecnologie sviluppate come dispositivi medici (sia invasivi che non invasivi) hanno già una precisa regolamentazione anche dal punto di vista del trattamento dei dati personali (*Health data privacy law*). Tuttavia, la recente implementazione di dispositivi neurotecnologici non invasivi, generalmente considerati "*consumer products*", ha messo in evidenza che la loro immissione sul mercato avviene in assenza di ogni regolamentazione sul punto e, soprattutto, in assenza di precisi *standard* di *data protection*.

La tutela del trattamento dei dati personali, nello Stato del Colorado già a livello costituzionale trova adeguata tutela nell'articolo II, *section 7*, che disciplina la *privacy* come diritto fondamentale ed elemento essenziale a garanzia della libertà dei soggetti. Con specifico riferimento poi all'innovazione tecnologica e alla crescente quantità di dati personali che vengono processati mediante dispositivi tecnologici immessi sul mercato, nel mese di luglio 2021, il Governatore del Colorado aveva adottato il *Colorado Privacy Act* (**CPA**), entrato in vigore il 1° luglio 2023, come parte del "*Colorado Consumer Protection Act*". In tale ambito, il CPA interviene ponendosi come normativa di protezione della *privacy* con specifico riferimento ai consumatori nei loro rapporti con i "*controllers*" (*Controllers means a person that, alone or jointly with others, determines the purposes for and means of processing personal data*. *Art. 6-1-1303, point 7 CPA*). Si tratta, pertanto, di un ambito di applicazione della norma molto ben preciso e delimitato, relativo unicamente ai prodotti e servizi digitali di consumo. Il CPA stabilisce alcuni diritti che i consumatori possono esercitare in merito al trattamento dei loro dati personali, tra cui il diritto di accesso, rettifica, cancellazione e portabilità; i consumatori hanno poi il diritto di *opt-out*, con il quale possono porre fine ad un trattamento di dati personali che li riguarda cui hanno già acconsentito in caso di pubblicità mirata, trasferimento a terzi di dati personali e profilazione. Peraltro, nell'attesa di una legge federale in materia di *privacy*, ora in discussione al Congresso americano (*American Privacy Rights Act_ARPA*), nell'attuale mosaico delle leggi nazionali sul trattamento dei dati personali negli Stati Uniti, proprio il tipo di attività per

ISSN 2239-8570

la quale il consumatore può esercitare il suo diritto di *opt-out* costituisce la principale differenza tra le diverse normative statali, per altro verso tra loro moto simili. L'obiettivo preso in considerazione del legislatore con tale intervento normativo è quello di responsabilizzare le aziende, circa il corretto trattamento dei dati personali dei loro "*consumers*" ma, allo stesso tempo, favorire e non limitare il processo di innovazione tecnologica.

Pertanto, sebbene il CPA avesse già introdotto una specifica disciplina a tutela della *privacy* dei consumatori, prevedendo specifici diritti (sul trattamento dei dati personali, inclusi quelli relativi a funzioni fisiche e mentali), la *General Assembly* ha ritenuto necessario intervenire nuovamente sul punto.

Con la recente *Colorado House Bill 24-1058* si è così ampliata la nozione di "*sensitive data*" contenuta nel CPA, per includervi anche la definizione di "*biological data*" e di "*neural data*" (*Section 1, Article 4, lett. a and b Colorado House Bill 24-1058*).

In tal modo, vengono modificati gli articoli 24 lett. b e c del CPA per introdurre una regolamentazione dei dati trattati a seguito dell'utilizzo delle neurotecnologie che segue lo schema di "genus" e "species". Infatti, è espressamente detto che i dati biologici ricomprendono anche i dati neurali. I primi – *biological data* - si riferiscono ai dati ottenuti dall'analisi delle caratteristiche biologiche, generiche, biochimiche, fisiologiche o neurali di un soggetto, sia singolarmente considerati sia se combinati con altri dati ("*Biological data means data generated by the technological processing, measurement, or analysis of an individual's biological, genetic, biochemical, physiological, or neural properties, compositions, or activities or of an individual's body or bodily functions, which data is used or intended to be used, singly or in combination with other personal data, for identification purposes. Biological data includes neural data*". *Section 2, art. 6-1-1303, point 2.5 CPA*). Quindi anche i dati relativi all'attività cerebrale di un soggetto che sono inferiti da altri dati personali e non rilevati direttamente possono essere qualificati come dati biologici. I dati neurali, più nello specifico, sono definiti come le informazioni derivanti dalla misurazione dell'attività del sistema nervoso centrale o periferico e che derivano dall'utilizzo di un dispositivo tecnologico ("*Neural data means information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device*" *Section 2, art. 6-1-1303, point 16.7 CPA*). La *ratio* dell'integrazione del CPA viene individuata nell'esigenza di dare compiuta regolamentazione ad un tipo particolare di dato personale idoneo a rivelare informazioni relativamente alla salute, stati mentali, emozioni e funzioni cognitive idonee a identificare o a rendere identificabile un soggetto (lett. *e, f CPA*).

Inoltre, la considerazione che la persona che utilizza dispositivi neurotecnologici non sia sempre in grado di comprendere - sebbene adeguatamente informato e dopo aver prestato idoneo consenso - il contenuto e la quantità delle informazioni che sono dal dispositivo raccolte e processate (*lett. f CPA*), ha indotto il legislatore ad ampliare l'ambito applicativo del CPA. Non appare infatti possibile avere un pieno controllo

ISSN 2239-8570

della specifica informazione neurale che può o potrebbe (anche in futuro) essere decodificata dal dispositivo.

Tale intervento normativo offre lo spunto anche per qualche riflessione sull'ampio dibattito circa la qualificazione giuridica dei dati neurali nel contesto dell'Unione Europea e del Regolamento Europeo sul trattamento dei dati personali (GDPR).

In mancanza di un espresso riferimento ai dati neurali, infatti, nel dibattito dottrinale sul tema appare dubbia la corretta applicazione dell'art. 9 GDPR anche nelle ipotesi in cui, come quella oggetto della legge del Colorado, i dati sono ottenuti in relazione a dispositivi non medici, qualificabili come prodotti di consumo. Ciò pone in dubbio che i dati neurali possano qualificarsi come dati relativi alla salute. In altri termini, si sostiene che i dati neurali non siano necessariamente dati relativi alla salute, ovvero all'integrità psico – fisica dell'individuo, quando si riferiscono a stati mentali (es. pensiero, ricordo) o emozioni.

Invero, la lettura del CPA come modificato dal *Colorado House Bill 24-1058*, sembra aprire ad una possibile diversa riflessione, che è possibile anche sulla base del dato normativo europeo.

Il punto della questione attiene, da un lato, al tipo di informazione che il dato neurale è in grado di fornire rispetto all'utilizzatore; dall'altro, alla nozione stessa di salute dal punto di vista giuridico, cui l'art. 4, n. 15 GDPR si riferisce per definire una categoria particolare di dati personali.

Quanto al tipo di dato, infatti, se è vero (come precisato dal *punto 2, lett. d* della *Section I* della *Colorado House Bill 24-1058*) che i dati neurali esprimono informazioni ampie sul soggetto, non strettamente collegate ad uno stato patologico del soggetto (ad es. emozioni o altri stati mentali), dovremmo poter affermare che tutti i dati connessi al funzionamento del sistema nervoso centrale e periferico – quindi ben oltre le funzioni cerebrali strettamente intese – possano essere ricompresi entro la medesima categoria di dati relativi alla salute e ricevere una regolamentazione uniforme. Ciò anche quando i dati neurali sono il risultato di un procedimento di inferenza inversa e non sono trattati singolarmente ma "*in combination with other personal data*" (Section 2, 2.5. *Colorado House Bill 24-1058*). Ciò appare coerente con la nozione giuridica di salute, comprensiva di condizioni patologiche e non patologiche, ed espressiva di una situazione fisica e psichica del soggetto, ciò anche a prescindere da una necessaria qualificazione in termini di benessere o malessere dell'individuo. In altre parole, il fatto stesso che i dati neurali si riferiscano al funzionamento di un apparato biologico, rende gli stessi dati relativi alla salute della persona cui si riferiscono, sebbene non raccolti in contesti clinici e/o di sperimentazione medica e sebbene non indichino una condizione patologica della persona. Si pensi al caso delle emozioni o di un ricordo. Nel primo caso, il dato emozionale può certamente con maggiore immediatezza esprimere una condizione di benessere o malessere della persona. Diversamente, se ci riferisce ai dati che sono ricollegabili ad una attività cerebrale espressiva di un ricordo o di un qualsiasi altro pensiero della persona, questi potrebbero non fornire necessariamente una indicazione sulla condizione di malessere o benessere della persona. Eppure, gli stessi dati connessi al ricordo o al

ISSN 2239-8570

pensiero della persona, possono in tale prospettiva qualificarsi come dati relativi alla salute nella misura in cui gli stessi sono espressione del funzionamento di una funzione cerebrale e dagli stessi è possibile inferire le condizioni di salute di un soggetto. Sulla base di tale assunto, sarebbe allora possibile in via interpretativa e senza richiedere ulteriori interventi legislativi, fornire adeguata tutela al trattamento dei dati neurali (unitariamente intesi da un punto di vista giuridico) facendo espressa applicazione delle norme già esistenti nell'ambito di applicazione del GDPR. Pertanto, anche i dati neurali raccolti da neurotecnolgoie di consumo dovrebbero essere trattati alla luce delle indicazioni contenute nell'art. 9 GDPR, ciò in quanto dati neurali relativi in ogni caso alla salute dell'utilizzatore in quanto riferibili al suo sistema nervoso; peraltro, nella nozione di dato personale relativo alla salute vi è già un espresso riferimento alla salute mentale e non solo fisica del soggetto, che agevola la riconduzione dei dati neurali a tale categoria (art. 4, n. 15 GDPR). Si potrebbe al più discutere dell'opportunità di adeguamenti nelle singole legislazioni nazionali, per indicare le misure giuridiche ed organizzative più adeguate a garantire un trattamento dei dati neurali che sia conforme a superiori interessi di tutela della persona e dei suoi diritti fondamentali.

Tuttavia, ciò non deve incidere sulle categorie giuridiche fondamentali né può spingeresti fino al punto di richiedere l'introduzione di nuovi diritti.

Il dibattito internazionale sui c.d. *neurorights*, pertanto, potrebbe riferirsi unicamente a quegli ordinamenti giuridici che non abbiamo principi e valori solidi su cui poggiare un'impalcatura di diritti fondamentali già individuati ed espressamente tutelati.

In Paesi come il Cile, piuttosto che il Colorado, l'intervento del legislatore si è reso necessario per la mancanza di riferimenti normativi adeguati e idonei a ricomprendere anche le nuove fattispecie emergenti dallo sviluppo tecnologico.

Diversamente, nell'ambito di applicazione del GDPR, la disciplina designata dal legislatore europeo – che ha infatti rappresentato il modello cui molti ordinamenti si sono ispirati per introdurre adeguate discipline in tema di trattamento dei dati personali, sebbene in un contesto di valore e principi molto differenti da quelli europei – ha già posto le basi per una tutela adeguata anche delle situazioni giuridiche connesse all'utilizzo di dispostivi tecnologici relativi alle funzioni cerebrali.

Il compito di estendere la fattispecie astratta individuata dalla norma al mutato contesto sociale non può che spettare all'operatore del diritto che, attraverso una corretta interpretazione ed applicazione delle norme già esistenti, può ritrovare nelle maglie della legislazione già in atto adeguata tutela.

ANNA ANITA MOLLO

https://leg.colorado.gov/sites/default/files/2024a_1058_signed.pdf

2024/2(39)SM

ISSN 2239-8570

39. Il divieto di vendita di prodotti software Kaspersky da parte del Dipartimento del Commercio degli USA

Il 20 giugno 2024 il Dipartimento del Commercio degli Stati Uniti d'America ha annunciato una determinazione finale che vieta alle società del gruppo Kaspersky di fornire prodotti o servizi negli Stati Uniti. Secondo il relativo comunicato ufficiale, questa decisione è stata presa per proteggere la sicurezza nazionale da attacchi cibernetici e dall'influenza del Governo russo sulle attività o i prodotti delle società del gruppo Kaspersky. L'indagine condotta dal Bureau of Industry and Security (**BIS**) ha rivelato che le operazioni delle società del gruppo Kaspersky negli Stati Uniti rappresentano un rischio "insostenibile" per la sicurezza nazionale.

Le principali preoccupazioni, dichiarate a giustificazione del provvedimento includono:

- giurisdizione e controllo del governo russo, in quanto il gruppo Kaspersky è soggetto alle leggi russe e deve rispondere a richieste di informazioni da parte del governo russo, il che potrebbe portare alla compromissione di dati sensibili;
- accesso a informazioni sensibili, in quanto il software Kaspersky ha accesso amministrativo ai dati dei clienti, che potrebbero essere trasferiti in Russia e utilizzati per scopi malevoli;
- capacità di installare software dannosi, in quanto le società Kaspersky potrebbero installare software dannosi o negare aggiornamenti critici, lasciando i sistemi statunitensi vulnerabili;
- integrazione con prodotti di terzi, in quanto il software di Kaspersky è integrato con prodotti di terzi, con ciò aumentando il rischio di introduzione di codici dannosi nei sistemi critici.

Coloro che utilizzano il software Kaspersky sono stati invitati ad utilizzare nuovi servizi per eludere il rischio di violazione dei dati personali. Sebbene non siano previste penalità legali per chi continua a utilizzare i prodotti di Kaspersky, tali utenti sono stati avvertiti che, nel continuare a fare ciò, si assumono tutti i rischi associati alla sicurezza informatica. Per minimizzare i disagi, la determinazione permette a Kaspersky di continuare alcune operazioni negli Stati Uniti, inclusi aggiornamenti del software, fino al 29 settembre 2024. Questo periodo di transizione dovrebbe aiutare gli utenti a trovare soluzioni alternative adeguate.

Già nel 2017, il Dipartimento della Sicurezza Nazionale aveva emesso una direttiva che richiedeva alle agenzie federali di rimuovere i prodotti Kaspersky dai sistemi informativi federali. Inoltre, il National Defense Authorization Act del 2018 aveva vietato l'uso di Kaspersky da parte del governo federale, e nel marzo 2022 la Federal Communications Commission aveva aggiunto Kaspersky alla lista delle attrezzature e dei servizi che rappresentano una minaccia per la sicurezza nazionale.

SERENA MIRABELLO

ISSN 2239-8570

https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers

2024/2(40)ST

40. L'India e le *Linee guida per la prevenzione e la regolamentazione dei dark patterns* in vigore dal dicembre 2023

In India, l'Autorità centrale per la protezione dei consumatori ha emanato le *Linee guida per la prevenzione e la regolamentazione dei dark patterns* che sono in vigore da dicembre 2023.

Le Linee guida sono state elaborate dopo che il Dipartimento indiano per gli Affari dei Consumatori (DoCA), nel settembre 2023, ha pubblicato una bozza sottoposta a consultazione pubblica. Il Dipartimento ha assunto l'impegno di salvaguardare gli interessi dei consumatori e promuovere un mercato equo e trasparente, soprattutto nello spazio digitale sempre più invasivo e in espansione.

Dette Linee guida definiscono e vietano diversi tipi di dark *patterns* elencati nell'allegato I. Segnatamente, sono elencati 13 tipi di *dark pattern* nella versione definitiva del dicembre 2023 delle *Linee guida per la prevenzione e la regolamentazione dei dark patterns*, rispetto ai 10 identificati nella precedente bozza.

Il fine delle Linee guida indiane è identificare, regolamentare e monitorare le pratiche che tendono a manipolare o alterare le scelte dei consumatori.

I *dark patterns* sono definiti come qualsiasi pratica o modello di progettazione ingannevole che: utilizzi interazioni *user interface/user experience* (UI/UX) su qualsiasi piattaforma; siano progettati per fuorviare o ingannare gli utenti a fare qualcosa che originariamente non intendevano o volevano fare, sovvertendone o compromettendone il processo decisionale. Tali "*practices or deceptive design patterns*" sono considerati, dalle *Linee guida per la prevenzione e la regolamentazione dei dark patterns,* equivalenti alla pubblicità ingannevole o alla pratica commerciale sleale o alla violazione dei diritti dei consumatori.

Dette Linee guida si applicano a: "*(i)All platforms, systematically offering goods or services in India; (ii) Advertisers; (iii) Sellers. I dark patterns sono vietati e "No person, including any platform, shall engage in any dark pattern*".

I 13 modelli di *dark patterns* che sono stati ufficialmente banditi in India dai siti di e-commerce sono:

(1) ***"False Urgency"*** che si sostanzia nell'affermare o sottintendere falsamente il senso di urgenza o di scarsità di un prodotto o di un servizio in modo da indurre un utente a effettuare un acquisto immediato o a intraprendere un'azione immediata che possa portare a un acquisto. Esemplificative sono le pratiche che si sostanziano nel mostrare una falsa popolarità di un prodotto o servizio per manipolare la decisione dell'utente oppure affermare che le quantità di un particolare prodotto o servizio sono

ISSN 2239-8570

più limitate di quanto non siano in realtà. Le Linee guida indiane forniscono anche esemplificazioni pratiche e, tra queste, con riferimento alla "*False Urgency*" si specifica che la stessa può essere integrata dalla presentazione di dati falsi relativamente alla domanda elevata del prodotto o servizio in modo da creare falsamente una pressione temporale per l'acquisto. Si pensi a quando si legge che "sono rimaste solo 2 camere e 30 altre persone stanno guardando lo stesso annuncio, oppure ai casi in cui si descrive una vendita come "esclusiva" per un periodo di tempo limitato solo per un gruppo selezionato di utenti.

(2) Sono vietate dalle Linee guida anche le pratiche di ***"Basket sneaking"***, inteso come l'inclusione di elementi aggiuntivi quali prodotti, servizi, pagamenti in beneficenza o donazione al momento del *checkout* da una piattaforma, senza il consenso dell'utente, in modo tale che l'importo totale pagabile dall'utente sia superiore all'importo pagabile per il prodotto o il servizio scelto dall'utente. Anche in questi casi gli esempi non sono pochi e ricorrono con frequenza nel quotidiano. Si pensi all'aggiunta automatica al carrello di servizi accessori a pagamento, con una casella preselezionata o in altro modo, quando un consumatore acquista un prodotto o un servizio; all'ipotesi nella quale un utente acquista un singolo servizio di parrucchiere, ma durante il *check-out* viene aggiunto automaticamente un abbonamento al servizio di parrucchiere; all'aggiunta automatica di un'assicurazione di viaggio mentre un utente acquista un biglietto aereo.

(3) Un ulteriore possibile modello di *dark patterns* consiste nella pratica di cd. ***"Confirm shaming"*** ossia nell'utilizzare una frase, un video, un audio o qualsiasi altro mezzo per creare un senso di paura o di vergogna o di ridicolo o di colpa nella mente dell'utente, in modo da spingerlo ad agire in un determinato modo e da indurre l'utente all'acquisto di un prodotto o di un servizio dalla piattaforma o alla prosecuzione di un abbonamento a un servizio, principalmente allo scopo di ottenere guadagni commerciali. Gli esempi sono: l'utilizzo, da parte di una piattaforma per la prenotazione di biglietti aerei, della frase "rimarrò senza assicurazione", quando un utente non include l'assicurazione nel suo carrello, oppure la frase "la beneficenza è per i ricchi, non mi interessa", qualora un utente preferisca rinunciare a contribuire alla beneficenza.

(4) La quarta pratica vietata dell'elenco è quella della ***"Forced action"***, intesa come la costrizione dell'utente a compiere acquisti ulteriori o aggiungere servizi o condividere informazioni personali al fine di acquistare o sottoscrivere un abbonamento. Sono esemplificative di questo modello di *dark patterns* il proibire all'utente di continuare a utilizzare il prodotto o servizio per il corrispettivo originariamente pagato e contrattato, a meno che non effettui un *upgrade* per una tariffa o un canone più elevati; costringere un utente a iscriversi a una *newsletter* per poter acquistare un prodotto; imporre ad un utente di scaricare un'applicazione separata, non prevista o non correlata, per accedere a un servizio originariamente pubblicizzato su un'altra applicazione. Si legge espressamente nelle Linee *guida indiane per la prevenzione e la regolamentazione dei dark patterns* che un esempio può essere quando «a user downloads app, X, meant for listing houses for renting. Once the user downloads X, they are forced to download another

ISSN 2239-8570

app, Y, for hiring a painter. Without downloading Y, the user is unable to access any services on X». Ulteriori esemplificazioni di *"Forced action"* si hanno quando si pone in essere una condotta tesa a costringere un utente a condividere informazioni personali legate alla carta di credito, anche quando tali dati non sono necessari per l'acquisto oppure a costringere un utente a condividere i dettagli dei suoi contatti o dei suoi *social network* al fine di accedere a prodotti o servizi acquistati o destinati all'acquisto da parte dell'utente, oppure nel rendere difficile per i consumatori la comprensione e la modifica delle loro impostazioni sulla *privacy*, incoraggiandoli così a fornire più informazioni personali di quanto intendano.

(5) Ulteriore modello di *dark patterns* è la ***"Subscription trap"***. Con questa espressione si intende il processo di rendere impossibile o complessa e lunga la cancellazione di un abbonamento a pagamento; di nascondere l'opzione di cancellazione di un abbonamento oppure la pratica di costringere un utente a fornire i dati di pagamento o l'autorizzazione all'addebito automatico per usufruire di un abbonamento gratuito oppure di rendere le istruzioni relative alla cancellazione dell'abbonamento ambigue, latenti, confuse, macchinose

(6) Pratica vietata è anche quella che consiste nel ***"Interface interference"***, espressione con la quale si intende un elemento di *design* che manipola l'interfaccia utente in modo tale da evidenziare alcune informazioni specifiche e oscurare altre informazioni rilevanti per sviare l'utente.

(7) Ugualmente vietata dalle Linee guida indiane, in quanto integra un modello di *dark patterns*, è la pratica di ***"Bait and switch"***, che consiste in una strategia di *marketing* che si basa sull'attirare i consumatori pubblicizzando un particolare risultato, per poi offrire, in modo ingannevole, un risultato alternativo. Per esempio, si pubblicizza il proprio prodotto a un prezzo molto conveniente e allettante che attira clienti (*bait*). Poi, però, al posto del prodotto che il cliente cerca, si prova a vendergli qualcosa che è più costoso o di valore inferiore rispetto a quello inizialmente pubblicizzato (*switch*). Un altro caso di *"Bait and switch"* è quello che si verifica quando un prodotto non è disponibile, ma viene falsamente mostrato come disponibile per invogliare il consumatore a spostarlo nel carrello. Una volta che il consumatore lo sposta nel carrello, si scopre che il prodotto è "esaurito" e al suo posto viene proposto un prodotto di prezzo superiore.

(8) Incide sulle capacità decisionali del consumatore anche il ***"Drip pricing"*** che è una tecnica pubblicitaria che si caratterizza per la pratica di pubblicizzare solo una parte del prezzo di un prodotto e rivelare altri addebiti in un secondo momento mentre il cliente segue il processo di acquisto. Nello specifico, in India, in base alle *Linee guida per la prevenzione e la regolamentazione dei dark patterns* si verifica una pratica di *"drip pricing"* quando «(i) elements of prices are not revealed upfront or are revealed surreptitiously within the user experience; or (ii) revealing the price post-confirmation of purchase, i.e. charging an amount higher than the amount disclosed at the time of checkout; or (iii) a product or service is advertised as free without appropriate disclosure of the fact that the

ISSN 2239-8570

continuation of use requires in-app purchase; or (iv) a user is prevented from availing a service which is already paid for unless something additional is purchased». É esclusa la responsabilità di ogni *"marketplace e-commerce entity*" quando le fluttuazioni di prezzo sono attribuibili a terzi o dovute ad altri fattori fuori dal proprio controllo. Si una pratica di "*Drip pricing*" quando il consumatore sta prenotando un volo e la piattaforma *online* presenta un certo prezzo nella pagina di *check-out* ma, al momento del pagamento, addebita al consumatore un prezzo superiore, oppure un consumatore ha scaricato un'applicazione mobile per giocare gratis, tuttavia, dopo 7 giorni, l'applicazione richiede un pagamento per continuare a giocare e il fatto che la versione gratuita del gioco è disponibile solo per un periodo di tempo limitato non è stato comunicato al consumatore al momento del *download*.

(9) Tra i modelli di *dark patterns* si colloca anche la ***"Disguised advertisement"*** che consiste nel generare confusione tra gli utenti sul confine tra contenuto reale e pubblicità, facendo passare gli annunci pubblicitari come altri tipi di contenuti, quali contenuti generati dagli utenti o nuovi articoli o elementi dell'interfaccia *online* a cui gli utenti potrebbero essere interessati, aumentando così le probabilità che gli utenti facciano clic su di essi. Nello specifico dell'ordinamento indiano, la *"Disguised advertisement"* comprende anche la pubblicità ingannevole come definita dalle Linee guida del 2022: *"Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements*".

(10) Rientra tra i *dark pattern* anche il ***"Nagging"*** che consiste in una pratica per mezzo della quale un utente è disturbato e infastidito da interazioni ripetute e persistenti, sotto forma di richieste, informazioni, opzioni o interruzioni. Si pensi ai siti *web* che chiedono in continuazione all'utente di scaricare la loro applicazione oppure alle piattaforme che chiedono all'utente di fornire il proprio numero di telefono o altri dati personali per presunti scopi di sicurezza o alla richiesta costante di attivare o accettare notifiche o *cookie* senza possibilità di rifiutare.

(11) Ugualmente vietata è la pratica cd. di **"*Trick Question*"** ossia quella che si sostanzia in porre domande a trabocchetto per mezzo dell'uso deliberato di un linguaggio confuso o vago, doppie negazioni o altri trucchi simili, al fine di fuorviare o indirizzare l'utente verso una risposta o un'azione specifica. Un esempio ricorrente è quello relativo ai casi in cui alla risposta: "desidera rinunciare a ricevere aggiornamenti sulla nostra collezione e sugli sconti per sempre?" si dà la possibilità di scegliere la risposta utilizzando frasi come "sì, desidero ricevere gli aggiornamenti" e "non ora", invece dell'opzione "sì", così da indurre l'utente ad effettuare una scelta diversa da quella che voleva veramente.

(12) "*Saas (Software as a Service) billing*" è una pratica che consiste nella *fatturazione per il rinnovo automatico silenzioso degli abbonamenti senza preavviso. Si tratta, per esempio, di sfruttare* cicli di abbonamenti ricorrenti per ottenere denaro dagli utenti nel modo più surrettizio possibile, perché non viene data alcuna notifica all'utente quando la prova gratuita viene convertita in pagamento; sono effettuate transazioni ricorrenti

ISSN 2239-8570

silenziose con addebiti che non sono notificati agli utenti; si addebitano ai clienti funzioni e servizi che non utilizzano.

(13) Infine, per ***"Rogue Malwares"*** si intendono programmi ingannevoli che inducono gli utenti a pagare per falsi strumenti di rimozione dei *virus* e che, invece, installano un programma/codice dannoso che mette a rischio un sistema. Per esempio quando un sito *web/app* pirata promette al consumatore di fornire contenuti gratuiti (audio o audiovisivi o altri), ma in realtà conduce a un "*malware*" quando si accede al *link*; quando i consumatori accedono al contenuto su piattaforme pirata, ma continuano a ricevere *pop-up* con pubblicità che contengono "*malware*"; quando i consumatori sono invitati a cliccare su una pubblicità o sono automaticamente reindirizzati a una pubblicità, ma invece trovano i loro file personali bloccati, seguiti dalla richiesta di effettuare un pagamento per riottenere l'accesso.

L'India con l'emanazione delle Linee guida commentate ha dimostrato consapevolezza dell'urgenza di una valutazione approfondita dei *dark pattern* sotto il profilo giuridico.

Sebbene il Governo Indiano sia stato elogiato per l'intervento diretto a contrastare i *dark pattern*, non sono mancate critiche legate ad alcune incongruenze redazionali sul carattere indicativo, o meno, dell'elenco dell'allegato I delle Linee guida e al carattere troppo rigido della definizione di ogni *dark pattern*, dato che con la rapida evoluzione della tecnologia, è probabile che emergano nuove forme di *dark pattern* che rischiano di rimanere fuori dall'architettura disegnata.

SARA TOMMASI

https://consumeraffairs.nic.in/sites/default/files/The%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%2C%202023.pdf

ISSN 2239-8570