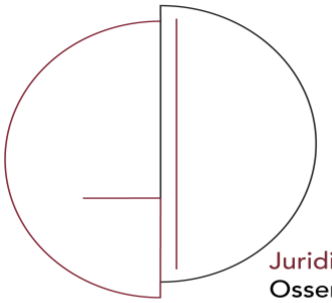

Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

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

1. **2024/4(1)STh** Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space) – **Shaira Thobani**

2. **2024/4(2)TDMCDV** Pubblicata in GU la direttiva (UE) 2024/2853 del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi ("nuova PLD") – **Tommaso De Mari Casareto dal Verme**

3. **2024/4(3)GM** Lo European Media Freedom Act (EMFA): regolamento (UE) 2024/1083 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media) – **Giuseppe Muto**

4. **2024/4(4)FBe** Pubblicata la CS3D: direttiva (UE) 2024/1760 sul dovere di diligenza delle imprese ai fini della sostenibilità (*Corporate Sustainability Due Diligence Directive*) – **Francesca Bertelli**

5. **2024/4(5)EMI** Il nuovo regolamento (UE) 2024/1781 sui requisiti di progettazione ecocompatibile per prodotti sostenibili (ESPR) – **Enzo Maria Incutti**

* 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

6. **2024/4(6)VR** Approvato il Cyber Resilience Act (CRA), sui requisiti di cibersicurezza dei prodotti connessi: regolamento (UE) 2024/2847– **Valentino Ravagnani**

7. **2024/4(7)MM** L'inizio di applicazione del regolamento (UE) 2023/988 relativo alla sicurezza generale dei prodotti (GPSR) – **Mario Mauro**

8. **2024/4(8)AS** Il regolamento (UE) 2024/903 che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile) – **Agostino Sola**

9. **2024/4(9)AA** Il regolamento (UE) 2024/1028 relativo alla raccolta e alla condivisione dei dati riguardanti i servizi di locazione di alloggi a breve termine – **Attilio Altieri**

10. **2024/4(10)VH** La sentenza della CGUE del 10.9.2024 nel caso Google Shopping (C – 48/22 P) e la conferma della condanna alla sanzione di 2,42 miliardi di euro – **Victor Hartl**

11. **2024/4(11)GD** La sentenza della CGUE del 19.9.2024 (causa C-264/23) sulle clausole di parità inserite negli accordi conclusi tra Booking.com e i prestatori di servizi alberghieri – **Giorgia Diotallevi**

12. **2024/4(12)MR** La sentenza della CGUE del 4.10.2024 nella causa C-621/22 sulla nozione di interesse legittimo come base per il trattamento di dati personali in ambito commerciale – **Matilde Ratti**

13. **2024/4(13)DI** Pratiche sleali e dati relativi alla salute: la sentenza della CGUE del 4.10.2024 nella causa C-21/23 Lindenapotheke (caso dei farmacisti tedeschi) – **Daniele Imbruglia**

14. **2024/4(14)RA** La sentenza della CGUE del 14.11.2024 nella causa C-646/22 sulla nozione di consumatore medio e sulle distorsioni cognitive – **Riccardo Alfonsi**

15. **2024/4(15)RDO** La sentenza della CGUE del 15.1.2024 nella causa C-33/22 sull'applicabilità del GDPR agli atti dei parlamenti nazionali e i regolamenti del Parlamento italiano in materia di "diritto all'oblio" – **Roberto D'Orazio**

16. **2024/4(16)MM-FN** La sentenza della Corte EDU del 5.11.2024 nel caso 25578/11 contro l'Italia sulla necessità di adire il Garante privacy in relazione al principio del previo esaurimento dei rimedi – **Mathilde Marè-Federico Nespega**

ISSN 2239-8570

17. **2024/4(17)MEU** La decisione del dicembre 2024 dell'EDPS di accertamento della violazione dell'EUDPR da parte della Commissione europea in relazione ad alcune pratiche di online microtargeting su utenti della piattaforma X a supporto di una pubblicità commissionata dalla Commissione europea – **Maria Elena Ursitti**

18. **2024/4(18)LC** La sanzione di quasi 800 milioni di euro irrogata a Meta dalla Commissione europea il 14.11.2024 per pratiche abusive relative a Facebook Marketplace – **Lucio Casalini**

19. **2024/4(19)TB** Il report del 9.10.2024 della Commissione europea al Parlamento e al Consiglio sulla prima revisione periodica circa il funzionamento della decisione di adeguatezza sullo EU-US Data Privacy Framework – **Timoteo Bucci**

20. **2024/4(20)TB** Il report del 4.11.2024 dell'EDPB sulla prima revisione periodica circa il funzionamento della decisione di adeguatezza sullo EU-US Data Privacy Framework – **Timoteo Bucci**

21. **2024/4(21)SB** Le Linee guida EDPB 2/2023 (versione 2.0) del 7.10.2024 sul campo tecnico di applicazione dell'art. 5(3) della direttiva e-Privacy – **Stefano Bartoli**

22. **2024/4(22)SB** Le Linee guida EDPB 1/2024 sottoposte a consultazione pubblica, sul trattamento dei dati personali basato sul legittimo interesse – **Stefano Bartoli**

23. **2024/4(23)BG** La dichiarazione dell'EDPB 5/2024 del 4.11.2024 sulle 42 raccomandazioni dell'High Level Expert Group istituito dalla Commissione Europea in materia di accesso ai dati personali per le attività di contrasto – **Beatrice Gallucci**

24. **2024/4(24)EB** Il parere EDPB 22/2024 del 7.10.2024 sugli obblighi dei titolari del trattamento di dati personali in conseguenza di incarichi affidati a responsabili e sub-responsabili ex art. 28 GDPR – **Emanuela Burgio**

25. **2024/4(25)CS** La dichiarazione EDPB 4/2024 del 7.10.2024 sulle modifiche alla proposta di regolamento che stabilisce ulteriori norme procedurali per l'applicazione del GDPR – **Carla Solinas**

26. **2024/4(26)SO** Il parere EDPB 28/2024 del 17.12.2024 su certi aspetti relativi al trattamento dei dati personali nel contesto dei modelli di IA – **Salvatore Orlando**

ISSN 2239-8570

27. **2024/4(27)DML** Il documento informativo del Garante privacy belga del dicembre 2024 in materia di sistemi d'intelligenza artificiale e GDPR – **Davide Maria Locatello**

28. **2024/4(28)FP** Il Final Report di ESMA del 17.12.2024 contenente le Linee guida per la qualificazione delle cripto-attività come strumenti finanziari **–** **Federico Pistelli**

29. **2024/4(29)CAT** I risultati del G7 Privacy di Roma del 9-11 ottobre 2024: verso un futuro digitale a prova di privacy – **Carmine Andrea Trovato**

30. **2024/4(30)AB** Il rapporto dell'11 ottobre 2024 pubblicato durante il G7 dei Garanti privacy su anonimizzazione, pseudonimizzazione e deidentificazione – **Alessandro Bernes**

31. **2024/4(31)IG** La dichiarazione dell'11.10.2024 del G7 dei Garanti Privacy su IA e bambini **–** **Ilaria Garaci**

32. **2024/4(32)PG** Adottato l'11.10.2024 durante il G7 dei Garanti Privacy un documento di analisi comparativa tra il GDPR ed il sistema CBPR globale di trasferimento dei dati personali con riferimento al sistema delle certificazioni - **Paolo Guarda**

33. **2024/4(33)CS** Il documento *Promoting enforcement cooperation* del G7 dei Garanti Privacy dell'11.10.2024 – **Carla Solinas**

34. **2024/4(34)ST** Le Linee Guida in materia di intelligenza artificiale della Pontificia Commissione dello Stato di Città del Vaticano del 16.12.2024 – **Sara Tommasi**

35. **2024/4(35)LS** Lo studio del World Economic Forum sulla governance della IA generativa dell'ottobre 2024: la necessità di un quadro normativo a 360° – **Ludovica Sposini**

36. **2024/4(36)FP** Lo studio del Financial Stability Board del 14.11.2024 sulle implicazioni di stabilità finanziaria dell'intelligenza artificiale – **Federico Pistelli**

37. **2024/4(37)AAM** Lo studio del Consiglio UE del settembre 2024 sulle tecnologie Brain Computer Interface (BCI) – **Anna Anita Mollo**

38. **2024/4(38)ES** I due studi della Banca d'Italia dell'ottobre 2024 su protezione del consumatore, neurofinance e neuroeconomics - **Emanuele Stabile**

ISSN 2239-8570

39. **2024/4(39)BP** Il D.Lgs. 144/2024 di adeguamento dell'ordinamento italiano al DGA: la disciplina sanzionatoria e la nomina di AgID come autorità competente per i servizi di intermediazione e altruismo dei dati, come organismo di assistenza degli enti pubblici che concedono o rifiutano il riutilizzo di dati, e come punto unico di contatto – **Beniamino Parenzo**

40. **2024/4(40)ES** Il D. Lgs. 134/2024 di attuazione della direttiva (UE) 2022/2257 relativa alla resilienza dei soggetti critici (direttiva CER) – **Emanuele Stabile**

41. **2024/4(41)MC** Le nuove disposizioni di diritto italiano sulla tutela del giocatore contro il gioco patologico e sull'impiego di sistemi di intelligenza artificiale in materia di riordino del settore dei giochi (D.Lgs. 41/2024) – **Michele Ciancimino**

42. **2024/4(42)GG** Chiusa la consultazione pubblica AGCOM su *Age Verification* – **Giorgio Giuliano**

43. **2024/4(43)VP** La consultazione pubblica di AGCOM sulla proposta di Codice di condotta per gli influencer elaborata dal Tavolo tecnico e su alcune proposta di modifica delle Linee guida degli influencer – **Vincenzo Pittelli**

44. **2024/4(44)EB** Il provvedimento n. 755 del 2.11.2024 del Garante privacy di chiusura dell'istruttoria e di irrogazione di sanzione di 15 milioni di euro nei confronti di Open AI per il servizio ChatGPT e la contestuale comunicazione all'autorità di controllo irlandese per l'accertamento di eventuali ulteriori violazioni del GDPR in conseguenza dello stabilimento di OpenAI in Irlanda – **Emanuela Burgio**

45. **2024/4(45)FRo** Approvato dal Garante Privacy il 17.10.2024 ed entrato in vigore il 28.11.2024 il "Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale" elaborato da Assosoftware – **Francesca Rotolo**

46. **2024/4(46)EG** La notifica da parte del Garante privacy di procedimenti correttivi e sanzionatori a 18 Regioni e alle Province autonome di Trento e Bolzano per violazioni della disciplina sul FSE 2.0 – **Elisa Grossi**

47. **2024/4(47)RMa-RoM** Il provvedimento del Garante privacy del 13.11.2024 contro Foodinho per trattamento illecito dei dati personali dei ciclofattorini (rider) ai sensi del GDPR – **Riccardo Maraga-Roberta Marciano**

ISSN 2239-8570

48. **2024/4(48)FG** Il provvedimento del Garante Privacy del 27.11.2024 nei confronti di GEDI per l'accordo con Open AI – **Francesco Grossi**

49. **2024/4(49)FDA** La sentenza del Tribunale di Torino, Sezione Lavoro del 20.9.2024, n. 2287 sul risarcimento del danno derivante dall'uso di algoritmi per la distribuzione delle supplenze nelle scuole superiori – **Filippo D'Angelo**

50. **2024/4(50)FS** La sentenza del Tribunale di Amburgo del 27.9.2024 nel caso Kneschke/LAION: la prima decisione europea sull'utilizzo di opere protette dal diritto d'autore per l'addestramento di sistemi di intelligenza artificiale – **Francesco Santonastaso**

51. **2024/4(51)FG** Il ricorso del 26.9.2024 contro la decisione dell'U.S. Copyright Office di negare la protezione del copyright all'opera Théâtre d'Opéra Spatial generata con l'uso del sistema di IA Midjourney- **Francesco Grossi**

52. **2024/4(52)GD** I rimedi comportamentali e strutturali proposti dal Dipartimento di Giustizia degli Stati Uniti ("Google must divest Chrome") e da Google a fronte della sentenza del 5.8.2024, con cui è stato dichiarato l'abuso di posizione dominante di Google nelle ricerche online e nella pubblicità degli annunci di testo – **Giorgia Diotallevi**

53. **2024/4(53)RRa** La legge dell'Australia che vieta ai minori di anni 16 l'utilizzo di alcune piattaforme di social media – **Rachele Ranieri**

54. **2024/4(54)VR** L'audizione di Meta al Senato australiano del 26.11.2024 e la sua ammissione di ricorrere allo *scraping* generalizzato dei dati degli utenti a fini di addestramento dei propri modelli di IA – **Valentino Ravagnani**

55. **2024/4(55)LC** L'iniziativa del governo dell'Australia di vietare il dynamic pricing come pratica commerciale scorretta – **Lucio Casalini**

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-2020-2023/

ISSN 2239-8570

2024/4(1)STh

1. Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space)

Il 21 gennaio 2025 il Consiglio ha emesso un comunicato stampa in cui annuncia l'adozione del Regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/EU e il regolamento (UE) 2024/2847, la cui proposta risale al 2022. Si tratta del primo intervento normativo su un settore specifico in attuazione di quanto previsto con riguardo agli spazi comuni europei dei dati dalla strategia europea per i dati del 2020 (comunicazione della Commissione, *Una strategia europea per i dati*, COM(2020) 66 final, 19 febbraio 2020, su cui v. in questa Rubrica la notizia n. 1 nel numero 2/2020 [2020/2(1)FR] e *Atlante* p. 13). Come affermato dalla Commissione, il proposito è quello di creare "spazi interoperabili comuni di dati a livello dell'UE in settori strategici", che "mirano a superare gli ostacoli giuridici e tecnici alla condivisione dei dati tra le organizzazioni, combinando gli strumenti e le infrastrutture necessari ed affrontando le questioni relative alla fiducia, ad esempio mediante norme comuni elaborate per gli spazi". Si tratta dunque, in tali ambiti, di "rendere disponibili pool di dati […], in combinazione con gli strumenti tecnici e le infrastrutture necessari per l'utilizzo e lo scambio di dati e con gli adeguati meccanismi di governance". I settori economici strategici e gli ambiti di interesse pubblici in cui creare spazi comuni di dati sono stati individuati in quelli (i) industriale manifatturiero,(ii) finanziario (sulla proposta di regolamento FIDA, v. in questa Rubrica la notizia n. 4 del numero 3/2023 [2023/3(4)BC] e *Atlante*, p. 374), (iii) dell'energia, (iv) del Green Deal, (v) della mobilità, (vi) dell'agricoltura,(vii) della pubblica amministrazione, (viii) delle competenze e, per l'appunto,(ix) sanitario.

In quest'ultimo campo lo scopo è duplice. Innanzitutto, nell'ottica del legislatore europeo la condivisione dei dati sanitari contribuirà ad una migliore libera circolazione degli stessi con riguardo alla fruizione delle cure sanitarie. Tramite lo sviluppo e la diffusione di cartelle cliniche elettroniche, gli interessati e i professionisti sanitari potranno infatti avere un accesso più agevole alle informazioni utili a erogare le prestazioni di cura, anche in uno Stato membro diverso da quello in cui il paziente risiede (rimediando così all'efficacia sinora limitata della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera). Il primo scopo è dunque quello di migliorare l'assistenza sanitaria tramite una crescente digitalizzazione dei dati relativi alla salute. La disponibilità di dati sanitari in formato digitale è tuttavia una

ISSN 2239-8570

risorsa preziosa le cui potenzialità il legislatore intende sbloccare anche al di fuori dell'assistenza sanitaria. A tal proposito interviene dunque la seconda finalità: quella di mettere a disposizione dei soggetti pubblici e privati che operano nell'UE un *pool* massivo di dati sanitari che possa essere utilizzato per finalità di ricerca e interesse pubblico. Il regolamento introduce dunque le norme necessarie a rendere possibile la condivisione dei dati per le diverse finalità ivi indicate: si stabiliscono le regole della circolazione dei dati entro lo spazio comune, differenziando tra uso "primario" e "secondario" dei dati, e si prevede la creazione delle infrastrutture essenziali affinché tale spazio possa realizzarsi.

Come accennato, la prima finalità del legislatore è quella di migliorare l'assistenza sanitaria tramite un migliore accesso ai dati sanitari elettronici dei pazienti, sia da parte degli stessi interessati, sia da parte dei professionisti sanitari. Si tratta dell'uso primario dei dati, che consiste nel trattamento "per la prestazione di assistenza sanitaria al fine di valutare, mantenere, o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso" (art. 2, par. 2, lett. d). Per creare uno spazio comune di dati idoneo a tale utilizzo, il legislatore impone a chi presta assistenza sanitaria di registrare una serie di informazioni sanitarie (tra cui, ad esempio, i "profili sanitari sintetici dei pazienti", i risultati di laboratorio, gli esami diagnostici per immagini, art. 14) in una cartella clinica elettronica (art. 13), da intendersi come "una raccolta di dati sanitari elettronici relativi a una persona fisica e rilevati nell'ambito del sistema sanitario, il cui trattamento avviene ai fini dell'assistenza sanitaria" (art. 2, par. 2, lett. j). I dati in questione sono dunque, di *default*, inseriti nelle cartelle cliniche elettroniche, con la possibilità per gli Stati membri di prevedere un diritto di *opt-out* degli interessati, i quali non possono tuttavia in ogni caso impedire il trattamento necessario a proteggere gli interessi vitali dell'interessato stesso o di terzi (art. 10). Oltre a tale (eventuale) diritto di *opt-out*, gli interessati hanno diritto di (i) accedere (e di autorizzare un'altra persona ad accedere) ai dati sanitari elettronici che li riguardano (art. 3); (ii) rettificarli (art. 6); (iii) ottenerne la portabilità (art. 7); (iv) inserire essi stessi ulteriori informazioni nella propria cartella clinica elettronica, le quali devono tuttavia rimanere distinte da quelle inserite dai professionisti sanitari (art. 5); (v) limitare l'accesso ai propri dati a coloro che prestano assistenza sanitaria (art. 8); (vi) essere informati sugli accessi effettuati ai propri dati sanitari elettronici (art. 9). L'inserimento dei dati nella cartella clinica elettronica, salvo l'eventuale esercizio del diritto di *opt-out* o di limitazione dell'accesso, comporta il diritto dei professionisti sanitari di accedere ai dati ivi contenuti tramite servizi di accesso dedicati (artt. 11-12). Si noti che lo scambio dei dati sanitari elettronici per uso primario deve rimanere fuori dai circuiti di mercato: è infatti vietato qualunque corrispettivo per rendere disponibili, consentire l'accesso o condividere tali dati (art. 18).

Per rendere tecnicamente possibile la condivisione dei dati per uso primario, il legislatore prevede che la Commissione adotti le specifiche tecniche per un formato europeo comune di scambio delle cartelle cliniche

ISSN 2239-8570

elettroniche (art. 15) e che stabilisca una infrastruttura transfrontaliera (LaMiaSalute@UE o MyHealth@EU) che consenta lo scambio dei dati sanitari elettronici tramite i singoli punti di accesso nazionali (art. 23). Per il monitoraggio e lo sviluppo di soluzioni tecniche adeguate, si prevede che ciascuno Stato membro istituisca un'autorità di sanità digitale responsabile dell'attuazione e dell'applicazione delle norme sull'uso primario dei dati (art. 19) e dotata anche di funzioni paragiurisdizionali. Al fine di coordinare l'attività di tale autorità con quella dall'Autorità di controllo per la protezione dei dati personali, laddove il reclamo riguardi i diritti degli interessati con riguardo ai propri dati sanitari elettronici, di cui si è detto sopra, esso sarà trasmesso all'Autorità (art. 21).

Il secondo intento del legislatore è quella di rendere disponibili i dati sanitari elettronici per l'uso secondario, cioè per finalità (diverse da quelle per cui inizialmente i dati sono stati raccolti) (a) di interesse pubblico nell'ambito della sanità pubblica o della medicina del lavoro; (b) di sostegno a enti pubblici per attività di *policy making* nel settore sanitario o dell'assistenza; (c) di elaborazione di statistiche relative al settore sanitario o dell'assistenza; (d) di istruzione o insegnamento nel settore sanitario o dell'assistenza; (e) di ricerca scientifica nel settore sanitario o dell'assistenza; (f) di miglioramento e ottimizzazione delle prestazioni di assistenza (art. 53). Si noti che il legislatore (forse memore della nozione restrittiva di "ricerca scientifica" elaborata dal Comitato europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020) dà una definizione estremamente estesa delle finalità di ricerca relative al settore sanitario o dell'assistenza che giustificano l'uso secondario dei dati: la norma si riferisce infatti alla ricerca che contribuisce non solo alla salute pubblica, ma anche "alla valutazione delle tecnologie del settore sanitario o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali". Tra queste sono menzionate a titolo esemplificativo le attività di sviluppo e innovazione per prodotti o servizi e quelle di addestramento, prova e valutazione di algoritmi anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di intelligenza artificiale e applicazioni di sanità digitale (art. 53, par. 1, lett. e).

Se questi sono gli usi ammessi, il legislatore si preoccupa anche di indicare quelli vietati. I dati non possono essere utilizzati per (a) adottare decisioni pregiudizievoli per una persona fisica o per un gruppo di persone fisiche (tra cui, ad esempio, le decisioni relative a offerte di lavoro, all'offerta di beni e servizi, la determinazione delle condizioni assicurative o di mutuo e in ogni caso qualunque decisione discriminatoria sulla base dei dati sanitari); (b) attività pubblicitarie o di marketing; (c) lo sviluppo di beni o servizi che possano danneggiare le persone, la salute pubblica o la società in generale; (d) attività contrarie all'ordine pubblico (art. 54).

Per consentire la condivisione dei dati sanitari per uso secondario, il regolamento impone ai "titolari dei dati sanitari" come definiti nel medesimo regolamento ("*health data holders"* in inglese), che sono tutti i soggetti del settore sanitario o dell'assistenza (che comprendono non solo

ISSN 2239-8570

coloro che erogano prestazioni sanitarie, ma anche coloro che sviluppano beni o servizi per i settori sanitari e dell'assistenza, chi fa ricerca in tali ambiti e, in generale, tutti coloro che, per determinate finalità, trattano dati sanitari elettronici: art. 2, par. 2, lett. t) di mettere a disposizione i dati in loro possesso (art. 51), salvo alcune eccezioni previste per le persone fisiche e le microimprese che sarebbero altrimenti gravate eccessivamente da tale obbligo (art. 50). Il legislatore elenca le categorie di dati che devono essere messi a disposizione, tra cui, ad esempio, quelli provenienti dalle cartelle cliniche elettroniche, dalle applicazioni per il benessere, dai registri di mortalità, dagli studi clinici, dai registri di prodotti e dispositivi medici, dalle biobanche, dai risultati di questionari e ricerche in ambito sanitario (art. 51). Laddove si tratti di dati coperti da diritti di proprietà intellettuale o da segreti commerciali, dovranno essere predisposte misure adeguate per tutelare tali diritti e, se questo non è possibile, la condivisione potrà essere negata (art. 52).

Per quanto riguarda il processo di condivisione tra titolari (che forniscono i dati) e "utenti dei dati sanitari" (che chiedono l'accesso, "*health data users*" in inglese), come definiti nel regolamento, si prevede che esso si svolga tramite l'intermediazione di organismi pubblici (gli "organismi responsabili dell'accesso ai dati sanitari", istituiti da ciascuno Stato membro, art. 55), i quali ricevono le richieste di accesso, decidono se accoglierle o meno e, in caso di accoglimento, forniscono un ambiente di trattamento sicuro in cui gli utenti possono accedere ai dati. Più nel dettaglio, chi intende utilizzare i dati per una finalità di uso secondario può presentare all'organismo responsabile dell'accesso ai dati sanitari una domanda di accesso ai dati, in cui indica le finalità e le caratteristiche del trattamento che intende porre in essere (art. 67). Ricevuta la domanda, l'organismo, sulla base dei principi di minimizzazione e finalità (art. 66) e a seguito di una valutazione del rischio, decide se rilasciare un'"autorizzazione ai dati", la quale vale per finalità e tempo determinati (art. 68). Si noti che gli organismi responsabili possono imporre tariffe per la messa a disposizione dei dati, purché esse siano proporzionali ai costi relativi a tale messa a disposizione, non discriminatorie e trasparenti; una parte delle tariffe può essere riversata ai titolari dei dati per coprire i costi da questi ultimi sostenuti per raccogliere e preparare i dati da condividere (art. 62).

Non vi è dunque un contatto diretto tra titolari e utenti di dati, né un trasferimento di dati personali dall'uno all'altro. L'utente dei dati che abbia ottenuto un'autorizzazione ai dati ha infatti unicamente diritto a trattare tali dati, nei limiti previsti nell'autorizzazione, nell'ambiente di trattamento sicuro fornito dall'organismo responsabile dell'accesso ai dati sanitari. In pratica, questo comporta che i titolari dei dati caricano i dati nell'ambiente sicuro (il quale deve rispettare una serie di requisiti di sicurezza, tracciabilità e interoperabilità), mentre gli utenti accedono a tale ambiente, all'interno del quale potranno trattare i dati per le finalità autorizzate ma dal quale non potranno scaricare tali dati se non in forma statistica anonimizzata (art. 73). Vi è inoltre il divieto per gli utenti dei dati di reidentificare gli interessati (art. 61, par. 3) e, alla luce delle ragioni di interesse pubblico

ISSN 2239-8570

sottese alla disciplina in esame, l'obbligo di rendere pubblici i risultati ottenuti tramite l'uso secondario dei dati (art. 61, par. 4). Si ha dunque un trattamento in cui sono convolti, a diverso titolo, gli organismi responsabili, i titolari e gli utenti dei dati sanitari: vista la complessità dell'intreccio dei rispettivi ruoli, il regolamento si preoccupa di specificare in che misura e rispetto a quali operazioni ciascuno di tali soggetti è da considerarsi titolare o responsabile del trattamento ai sensi del GDPR (art. 74). Oltre che con richieste di accesso, è possibile rivolgersi agli organismi responsabili anche per ottenere una risposta in forma esclusivamente statistica anonimizzata. In tal caso si parla di "richiesta di dati sanitari" e l'organismo responsabile fornisce non l'accesso ai dati, ma unicamente il risultato nella forma indicata (art. 69).

Per rendere più facilmente accessibile il *pool* di dati sanitari elettronici così messo a disposizione, il legislatore prevede che gli organismi responsabili dell'accesso ai dati sanitari pubblichino dei cataloghi in cui indicano e descrivono le serie di dati (sulla base delle informazioni fornite dai titolari dei dati), di modo che chi intende accedere ai dati abbia elementi per valutare in anticipo l'utilità della propria richiesta (art. 77). Tali serie di dati possono inoltre recare un marchio di qualità e di utilità dei dati, volto a veicolare informazioni in merito, ad esempio, alla qualità tecnica dei dati, alla loro copertura e alle eventuali modifiche (art. 78). Dal punto di vista tecnico, per rendere possibile la condivisione dei dati per uso secondario, il legislatore prevede che la Commissione e gli Stati membri istituiscano una infrastruttura transfrontaliera (DatiSanitari@UE o HealthData@EU) che consenta il collegamento tra gli organismi responsabili dell'accesso ai dati sanitari tramite punti di accesso nazionali (art. 75).

Le modalità di condivisione previste dal regolamento in esame sono volte a contemperare l'interesse a che i dati siano messi in circolo per finalità di interesse generale, da un lato, e quello alla protezione dei dati personali, dall'altro. In questo delicato bilanciamento, si prevede che gli interessati possano esercitare il diritto di *opt-out* (chiamato "diritto di esclusione") dal trattamento dei dati sanitari elettronici personali per uso secondario (art. 71): in tal caso i loro dati non possono più essere resi disponibili, fatti salvi invece i trattamenti per i quali sia già stata emessa un'autorizzazione ai dati. Il regolamento lascia agli Stati membri la decisione se consentire l'uso secondario dei dati nonostante l'esercizio dell'*opt-out* laddove la richiesta di accesso provenga da un organismo pubblico o incaricato di svolgere un compito di pubblico interesse e non vi siano alternative efficaci.

Come per vigilare e assicurare l'attuazione delle norme sull'uso primario dei dati è istituita l'autorità di sanità digitale, così un analogo ruolo svolgono, con riguardo all'uso secondario dei dati, gli organismi responsabili dell'accesso ai dati. Essi hanno infatti non solo il compito di intermediazione e vaglio sopra descritto, ma anche quello (a cui si unisce un corrispondente potere sanzionatorio) di vigilare sull'applicazione delle norme sull'uso secondario dei dati sanitari (artt. 57, 63). Anche in questo caso si prevede che tali organismi, laddove constatino una violazione del GDPR, debbano informare le Autorità di controllo in materia di protezione dei dati personali.

ISSN 2239-8570

Queste sono dunque le norme che regolano la circolazione dei dati sanitari elettronici per uso primario e secondario. Il legislatore introduce inoltre ulteriori disposizioni sulla condivisione di tali dati con Paesi terzi e organizzazioni internazionali, prevedendo requisiti stringenti anche laddove si tratti di dati non personali (artt. 88-91). In tale ottica, le domande di accesso provenienti da richiedenti stabiliti in Paesi terzi sono ammesse, a seguito di un atto della Commissione, solo a condizione di reciprocità e, dunque, solo purché il Paese terzo consenta l'accesso ai propri dati sanitari elettronici agli utenti europei a condizioni non più restrittive di quelle europee (art. 91). A livello di governance europea, si istituiscono (i) un Comitato dello spazio europeo dei dati sanitari "per agevolare la cooperazione e lo scambio di informazioni tra gli Stati membri e la Commissione" (art. 92), (ii) un forum dei portatori di interesse per promuovere la cooperazione con riguardo all'attuazione del regolamento (art. 93), (iii) due gruppi direttivi per le infrastrutture transfrontaliere LaMiaSalute@UE e DatiSanitar@UE. Per quanto riguarda i profili sanzionatori, il regolamento rimanda agli Stati membri la determinazione di sanzioni che siano effettive, proporzionate e dissuasive (art. 99), e riconosce il diritto al risarcimento, secondo il diritto degli Stati membri o dell'Unione, in favore di chi abbia patito danni materiali o immateriali come conseguenza di una violazione del regolamento stesso (art. 100).

È chiaro che la condivisione dei dati prevista dal regolamento può verificarsi solo in presenza di condizioni tecniche che la rendano possibile. Per tale motivo, oltre a prevedere l'istituzione delle due infrastrutture transfrontaliere di cui si è detto, una parte importante del regolamento è volta a disciplinare i dispositivi che consentono, a monte, la raccolta in formato elettronico dei dati che sono alla base della complessa architettura disegnata dal legislatore europeo e senza i quali questa non sarebbe possibile. In particolare, il regolamento dedica ampio spazio alla disciplina dei sistemi di cartelle cliniche elettroniche e delle applicazioni per il benessere.

Per quanto riguarda i sistemi di cartelle cliniche elettroniche, da intendersi come "qualsiasi sistema in cui il software oppure la combinazione tra l'hardware e il software del sistema consente ai dati sanitari elettronici […] di essere conservati, intermediati, esportati, importati, convertiti, modificati o visualizzati […]" (art. 2, par. 2, lett. k), il legislatore adotta una regolamentazione di prodotto in cui detta i requisiti (le cui specifiche tecniche sono individuate dalla Commissione) per l'immissione in commercio e la messa in servizio (art. 26). Tali requisiti sono volti a garantire non solo la sicurezza, ma anche, nell'ottica di creare uno spazio comune di dati, l'interoperabilità dei sistemi di cartelle cliniche elettroniche. In particolare, tali sistemi devono includere un "componente software europeo di interoperabilità", che consenta di fornire e ricevere dati sanitari elettronici personali, e un "componente software europeo di registrazione" (art. 35), che fornisca le informazioni sugli accessi a tali dati, entrambe armonizzate a livello europeo.

Per quanto riguarda invece le applicazioni per il benessere, definite come qualsiasi software o combinazione di hardware e software destinato a essere

ISSN 2239-8570

utilizzato "da una persona fisica, per il trattamento dei dati sanitari elettronici, specificamente per fornire informazioni sulla salute di una persona fisica o per fornire cure assistenziali per scopi diversi dalla prestazione di assistenza sanitaria" (art. 2, par. 2, lett. ab), esse sono soggette a un sistema di etichettatura obbligatoria nel caso in cui il fabbricante ne dichiari l'interoperabilità con un sistema di cartelle cliniche elettroniche. In tal caso, infatti, è obbligatorio non solo rispettare i requisiti fissati per i componenti armonizzati di interoperabilità e di registrazione, ma anche indicare tramite un'etichetta che tali requisiti sono rispettati (artt. 47-48). Si noti che l'interoperabilità non comporta un'automatica trasmissione dei dati per la condivisione, in quanto a tal fine è necessario il consenso dell'interessato (art. 48, par. 2). Dunque, mentre i dati contenuti nelle cartelle cliniche elettroniche sono automaticamente condivisi per l'uso primario e secondario salvo l'eventuale *opt-out* dell'interessato, per i dati raccolti tramite le applicazioni per il benessere occorre un *opt-in*.

Se questi sono gli strumenti per creare lo spazio europeo dei dati sanitari, è evidente il netto cambio di rotta, iniziato nel 2020, rispetto alla prospettiva più restrittiva in merito al trattamento privilegiata dal GDPR. Questo sarà possibile solo in presenza di importanti e adeguati investimenti nelle infrastrutture e tecnologie che rendano possibile e sicura la condivisione dei dati (si veda infatti il paragrafo sull'incidenza sul bilancio della proposta di regolamento sullo spazio europeo dei dati sanitari, COM(2022)197final, 3 maggio 2022), nonché, a tutela della fiducia dei cittadini europei, di iniziative di alfabetizzazione digitale e campagne di informazione volte a rassicurare e a far comprendere agli interessati la portata degli interessi generali in gioco (artt. 83-84).

SHAIRA THOBANI

https://data.consilium.europa.eu/doc/document/PE-76-2024-INIT/it/pdf

Comunicato stampa del 21.1.2025

2024/4(2)TDMCDV

2. Pubblicata in GU la direttiva (UE) 2024/2853 del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi ("nuova PLD")

Dopo l'approvazione del testo da parte del Parlamento europeo lo scorso 12 marzo 2024 (su cui v. in questa Rubrica, notizia n. 5 del numero 2/2024 (2024/2(5)TDMCDV]), è stata pubblicata nella Gazzetta ufficiale dell'Unione europea la direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio (la **nuova PLD**). La nuova PLD sostituisce definitivamente la direttiva 85/374/CEE (la **vecchia PLD**), aggiornando la disciplina della responsabilità del produttore

ISSN 2239-8570

alla luce delle moderne evoluzioni delle tecnologie digitali, con particolare attenzione alle caratteristiche evolutive dell'Intelligenza Artificiale.

L'art. 21, co. 2 della nuova PLD statuisce che i riferimenti alla vecchia PLD si intendono fatti alla nuova PLD e si leggono secondo la **tavola di concordanza** allegata (unico allegato) alla nuova PLD.

Di seguito i tratti salienti della nuova PLD.

Innanzitutto, bisogna precisare che la vecchia PLD è abrogata con effetto a decorrere **dal 9 dicembre 2026** e che pertanto essa continuerà ad applicarsi in relazione ai prodotti immessi sul mercato o messi in servizio prima di tale data (art. 21 nuova PLD). Di converso, e di conseguenza, la nuova PLD si applicherà ai prodotti immessi sul mercato o messi in servizio solo dopo il 9 dicembre 2026 (art. 2 nuova PLD).

L'art. 4 della nuova PLD si occupa di aggiornare le definizioni di cui alla vecchia PLD alla luce delle recenti evoluzioni del contesto tecnologico e produttivo. In particolare, si segnala la nuova definizione di "**prodotto**" (art. 4, n. 1 nuova PLD), 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**.

La definizione di "file per la fabbricazione digitale" è la seguente: "una versione digitale di un bene mobile o un modello digitale per un bene mobile contenente le istruzioni funzionali necessarie per produrre un bene tangibile consentendo il controllo automatizzato di macchine o strumenti" (art. 4, n. 2 nuova PLD).

A chiarimento della ratio della previsione interviene il Considerando 16 della nuova PLD: "Mentre i file digitali in quanto tali non sono prodotti che rientrano nell'ambito di applicazione della presente direttiva, i file per la fabbricazione digitale, che contengono le istruzioni necessarie per produrre beni materiali attraverso il controllo automatizzato di macchine o strumenti come trapani, torni, fresatrici e stampanti 3D, dovrebbero essere considerati prodotti al fine di garantire la protezione delle persone fisiche qualora tali file siano difettosi. Ad esempio, un file di progettazione assistita da computer che sia difettoso e venga utilizzato per creare un bene stampato in 3D che causi un danno dovrebbe comportare una responsabilità a norma della presente direttiva qualora tale file sia sviluppato o fornito nel corso di un'attività commerciale. A fini di chiarezza è opportuno precisare che le materie prime, come il gas e l'acqua, e l'elettricità sono prodotti".

Similmente, la definizione di "**fabbricante**" (art. 4, n. 10 nuova PLD) 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.

Secondo l'apposita definizione dell'art. 4, n. 5 della nuova PLD, il "**controllo del fabbricante**" si verifica quando a) il fabbricante di un prodotto esegue o, per quanto riguarda le azioni di terzi, autorizza o consente i) l'integrazione, l'interconnessione o la fornitura di un componente, compresi aggiornamenti e migliorie del software; o ii) la modifica del prodotto, incluse modifiche sostanziali; b) il fabbricante di un

ISSN 2239-8570

prodotto è in grado di fornire aggiornamenti o migliorie del software direttamente o tramite terzi.

L'art. 6 della nuova PLD ha ampliato la previsione delle **tipologie dei danni rilevanti**. Ciononostante, il diritto al risarcimento del danno ai sensi dell'art. 5 della medesima direttiva continua a poter essere fatto valere soltanto con riferimento a determinati danni, e precisamente:

a) morte o lesioni personali, compresi i danni psicologici riconosciuti da un punto di vista medico;

b) danneggiamento o distruzione di qualsiasi bene, tranne i) il prodotto difettoso in sé, ii) un prodotto danneggiato da un componente difettoso che è integrato in tale prodotto o interconnesso con questo dal fabbricante di tale prodotto o sotto il controllo di tale fabbricante, e iii) i beni usati esclusivamente a fini professionali;

c) distruzione o corruzione di dati non usati a fini professionali.

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 nuova PLD, 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. Viene, tuttavia, 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, qualora il fabbricante mantenga il controllo sul prodotto dopo tale momento, il momento in cui il prodotto è uscito dal *controllo del fabbricante*.

L'art. 8 della 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) 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: i) l'importatore del prodotto o componente difettoso; ii) il rappresentante autorizzato del fabbricante; e iii) se non vi è un importatore stabilito nell'Unione o un rappresentante autorizzato, il fornitore di servizi di logistica. Al fabbricante è equiparato chiunque modifichi in maniera

ISSN 2239-8570

sostanziale un prodotto al di fuori del controllo del fabbricante e lo metta successivamente a disposizione sul mercato o in servizio.

L'art. 12 della 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).

Tra le principali novità del nuovo testo ci sono taluni meccanismi finalizzati ad alleviare l'onere della prova dei danneggiati per far fronte alla complessità che caratterizza l'odierna realtà tecnologico-digitale. Tra questi, in primo luogo l'art. 9 della nuova PLD introduce la possibilità per i soggetti danneggiati di ottenere dal produttore la divulgazione (***disclosure***) di elementi di prova, al fine di attenuare l'asimmetria informativa esistente tra professionisti e consumatori relativamente al funzionamento di prodotti tecnologicamente complessi. 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. Tale divulgazione dovrà essere 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.

In secondo luogo, l'art. 10 della nuova PLD introduce tre diverse presunzioni accessibili al danneggiato per assolvere al proprio onere probatorio, che nel suo contenuto è rimasto il medesimo: infatti, l'attore deve provare il **carattere difettoso del prodotto**, il **danno subito** e il **nesso di causalità** tra il difetto e il danno. La **prima presunzione** consente di ritenere provato il carattere difettoso del prodotto qualora sia soddisfatta una delle seguenti condizioni:

a) il convenuto omette di divulgare i pertinenti elementi di prova a norma dell'articolo 9, paragrafo 1 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'uso 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 compatibile con il difetto in questione.

La **terza presunzione** consente al giudice di ritenere provato il carattere difettoso del prodotto o il nesso di causalità tra il carattere difettoso e il danno, o entrambi, qualora, nonostante la divulgazione di prove a norma dell'articolo 9 della nuova PLD e tenuto conto di tutte le circostanze pertinenti del caso:

a) l'attore incontri difficoltà eccessive, in particolare a causa della complessità tecnica o scientifica, nel provare il carattere difettoso del

ISSN 2239-8570

prodotto o il nesso di causalità tra il carattere difettoso e il danno o entrambi; e

b) l'attore dimostri che è probabile che il prodotto sia difettoso o che esista un nesso di causalità tra il carattere difettoso del prodotto e il danno, o entrambi.

Tutte le presunzioni introdotte dall'art. 10 della nuova PLD sono superabili dal convenuto, che quindi è autorizzato a fornire la **prova contraria**.

L'art. 11 della nuova PLD mantiene le **cause di esenzione da responsabilità** di cui al precedente art. 7 della vecchia PLD, apportando alcune novità e articolando alcune prove liberatorie rispetto alle specifiche categorie di soggetti responsabili considerate. Si osservi in particolare che l'esimente del cd. "**rischio da sviluppo**" non è più legato al solo momento di immissione del prodotto sul mercato, ma tiene conto anche del successivo eventuale periodo in cui il produttore ha mantenuto il controllo sul prodotto. Costituisce, poi, assoluta novità quanto previsto dal secondo paragrafo dell'art. 11 della nuova PLD, 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 della 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; e 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 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 della **prescrizione** e del **periodo di scadenza** (artt. 16 e 17 nuova PLD), se non per il coordinamento dell'individuazione del *dies a quo* con le rinnovate caratteristiche dei prodotti nell'era digitale.

TOMMASO DE MARI CASARETO DAL VERME

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202402853

ISSN 2239-8570

2024/4(3)GM

3. Lo European Media Freedom Act (EMFA): regolamento (UE) 2024/1083 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media)

Il 17 aprile 2024 è stato pubblicato il regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di *media* nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE. È il Regolamento europeo sulla libertà dei *media* (da ora anche il **Regolamento** o **European Media Freedom Act** o **EMFA**).

Come emerge dai Considerando del Regolamento, lo EMFA mira a rafforzare la libertà e l'indipendenza dei *media* nell'era digitale, con un approccio flessibile basato su principî. Esso si integra con altre normative europee, in particolare la direttiva (EU) 2018/1808 (**AVMSD**), il regolamento (EU) 2022/2065 (**DSA**) e il regolamento (EU) 2022/1925 (**DMA**), promuovendo un'armonizzazione minima tra gli Stati membri. Lo EMFA estende il suo ambito di applicazione a tutte le possibili minacce alla libertà dei *media* e a tutte le tipologie di servizi multimediali, sia online che offline, con un approccio dinamico che consente di adattarsi alle sfide del digitale. Un'attenzione particolare è riservata alle *very large online platforms* (**VLOPs**), che, oggi, sono diventati i principali strumenti di informazione per i cittadini europei. Lo EMFA riconosce il ruolo cruciale dei *media* indipendenti come "guardiani" della democrazia e promuove un mercato interno dei servizi d'informazione integrato, in linea con l'art. 11 della Carta di Nizza (**CDFUE**). Si pone l'accento sulla necessità che i fruitori di servizi informativi siano a conoscenza della proprietà degli stessi, al fine di poter meglio identificare i possibili conflitti d'interesse. Infine, il Regolamento prevede un dialogo strutturato con i *provider* delle piattaforme digitali più grandi e promuove meccanismi di autoregolamentazione credibili e trasparenti, come codici di condotta, linee guida, standard etici, gestione delle segnalazioni e correzione degli errori.

I. La base giuridica dello EMFA

L'UE radica la propria competenza a legiferare in materia di libertà dei *media* nell'art. 114 del Trattato sul funzionamento dell'Unione europea (**TFUE**), dando, dunque, primaria rilevanza al corretto funzionamento del mercato interno, in luogo della tutela dei diritti. La produzione e il consumo di contenuti multimediali, tra cui le notizie, hanno carattere sovranazionale, per questa ragione, l'adozione di un approccio comune europeo consente di garantire la certezza del diritto, la concorrenza leale tra i diversi fornitori di servizi multimediali e l'opportunità di realizzare investimenti transnazionali per il consolidamento del settore.

Pertanto, sebbene una risposta comune europea sia resa necessaria dalle caratteristiche proprie del fenomeno, il Regolamento deve, comunque, rispettare il principio di proporzionalità, che, nel caso di specie, si declina in una ben equilibrata e armonizzata disciplina, che non ecceda quanto

ISSN 2239-8570

necessario per il raggiungimento di un comune quadro di riferimento normativo, allo scopo di garantire un corretto funzionamento del mercato interno dei servizi multimediali. In particolare, ci si riferisce al divieto di interferire nell'erogazione dei fondi pubblici per l'editoria e nello svolgimento di attività di interesse pubblico (così come previsto, dal Protocollo n. 29 sul sistema di radiodiffusione pubblica negli Stati membri allegato al TUE e al TFUE e dall'art. 4, c. 2 del Trattato sull'Unione europea, **TUE**). Infine, sotto il profilo della sussidiarietà, l'intervento del legislatore europeo risulta essere necessario, in considerazione dell'assenza di diversi possibili strumenti regolatori, che producano effetti equivalenti.

II. I diritti e doveri dei fornitori di servizi di *media* e dei loro destinatari

Coerentemente con l'obiettivo dichiarato dal Regolamento, sin dalle prime righe, è riconosciuto ai destinatari dei servizi multimediali nell'Unione il diritto di ricevere una pluralità di notizie e contenuti di qualità, prodotti nel rispetto della libertà editoriale dei fornitori di servizi multimediali, a beneficio del dibattito pubblico (art. 3 EMFA). Dunque, si pone in una posizione speculare il diritto dei fornitori di servizi multimediali di svolgere pienamente le attività economiche senza alcuna limitazione, diversa da quelle imposte dal diritto dell'Unione (art. 4 EMFA). Per raggiungere tale obiettivo, gli Stati membri devono rispettare la libertà di stampa, non potendo interferire in alcun modo con le decisioni editoriali e non potendo porre in essere alcuna attività di sorveglianza o captazione dei giornalisti, dei fornitori di servizi multimediali e degli individui a essi vicini, ad eccezione dei casi nei quali sussista un pubblico interesse. Al fine di rendere effettiva tale tutela, gli Stati membri devono nominare autorità indipendenti competenti a decidere sulle denunce presentate dai fornitori di servizi multimediali.

Dunque, il fine che il Regolamento si propone è quello di tutelare il pluralismo dell'informazione, inteso come un corollario della libertà di stampa. Tale obiettivo è perseguito assicurando che l'informazione (generata da *provider*, sia pubblici, che privati) offra ai cittadini l'accesso a un'offerta di fonti informative quanto più ampia e plurale possibile. Si tratta di un tema estremamente sensibile, rispetto al quale il legislatore euro-unitario ha una limitatissima potestà legislativa, in considerazione dei limiti stabiliti dal Protocollo n. 29 sul sistema di radiodiffusione pubblica negli Stati membri, allegato al TUE e al TFUE. Non è possibile, pertanto, spingersi a una regolazione che vada oltre la definizione di principi. A maggior ragione, i fornitori di servizi multimediali pubblici devono fornire – in modo imparziale – una pluralità di informazioni e opinioni (art. 5 EMFA). Questo obiettivo è raggiunto a partire da modalità di nomina trasparenti (pubbliche e non discriminatorie) e da una durata dell'incarico del *management*, adeguato e sufficientemente lungo a garantire l'effettiva indipendenza. Inoltre, gli Stati membri devono assicurare risorse economiche adeguate allo svolgimento dell'incarico.

Tuttavia, anche i servizi di informazione privati sono chiamati a osservare alcuni doveri di trasparenza, in considerazione del ruolo d'interesse pubblico che svolgono. Tra di questi, è possibile annoverare

ISSN 2239-8570

l'obbligo di rendere facilmente accessibili le informazioni riguardanti la proprietà dello stesso organo di informazione (art. 6 EMFA). Parimenti a quanto sopra espresso per i *media* pubblici, anche tali fornitori di servizi multimediali devono godere di libertà nella determinazione delle decisioni editoriali e sono obbligati a rivelare potenziali conflitti d'interesse.

III. Il quadro di riferimento per la cooperazione normativa e per il buon funzionamento del mercato interno dei servizi di *media*

L'obiettivo di tutelare in maniera uniforme il pluralismo informativo non può ritenersi raggiunto, laddove permanga una scarsa uniformità normativa nel contesto unionale, che trova la propria origine nella mancata integrazione tra le autorità nazionali competenti. A tal fine, lo EMFA istituisce il Comitato europeo per i servizi di media, il quale, sostituendo *European Regulators Group for Audiovisual Media Services* (cd. ERGA), gode di piena indipendenza nell'esercizio delle proprie attribuzioni (art. 8 EMFA). In tale Comitato siedono i rappresentanti delle autorità regolatorie nazionali. Per esplicita dichiarazione del legislatore, tale organo pone le sue radici nell'art. 30-*ter* AVMSD, che è già stato oggetto di recepimento in quasi ogni Stato dell'Unione.

Dunque, il Comitato si configura come un organismo indipendente (art. 9 EMFA), composto da rappresentanti delle autorità nazionali di regolamentazione, con il compito di fornire consulenza e supporto alla Commissione europea sulle questioni relative ai servizi informativi. È importante notare che tale organo non pregiudica le attribuzioni della Commissione europea o delle autorità nazionali, dal momento che opera in sinergia con gli stessi, fornendo consulenza e supporto tecnico, ma mantenendo, al contempo, la propria autonomia decisionale. Lo EMFA dispone che il Comitato si doti di un proprio regolamento interno, nel quale devono essere previste modalità per la prevenzione e la gestione dei conflitti di interessi dei suoi membri.

Tra le principali funzioni del Comitato, spiccano la promozione della cooperazione tra le autorità nazionali, l'elaborazione di pareri su questioni tecniche e giuridiche, nonché la mediazione in caso di disaccordi tra Stati membri. Inoltre, svolge un ruolo cruciale nel dialogo strutturato tra fornitori di piattaforme online di grandi dimensioni e rappresentanti dei fornitori di servizi di *media*, coerentemente con l'obiettivo di garantire un ecosistema dell'informazione equilibrato e pluralistico.

Da un punto di vista più strettamente operativo, gli artt. 14 e successivi dello EMFA regolano i principi e le modalità attraverso i quali si dovrà realizzare la cooperazione tra le diverse autorità nazionali. Infatti, ciascuna di esse ha la facoltà di chiedere, in qualsiasi momento, alle autorità di altri Stati membri di collaborare, anche attraverso lo scambio di informazioni o l'assistenza reciproca. L'autorità nazionale che riceve la richiesta non può esimersi dal dare corso alla stessa, salvo il caso in cui non sia competente, la sua esecuzione violerebbe il Regolamento o la portata della stessa richiesta non sia giustificata o debitamente motivata. Più nello specifico, l'art. 17 EMFA statuisce che il Comitato coordina le misure adottate, anche dalle autorità nazionali, nei confronti dei fornitori di servizi multimediali stabiliti

ISSN 2239-8570

in un paese terzo, laddove "tali servizi di *media* pregiudichino o presentino un rischio serio e grave di pregiudicare la sicurezza pubblica e la difesa".

IV. L'implementazione del dialogo con le *VLOPs*

Nell'era della digitalizzazione, un regolamento che si propone il fine di tutelare il pluralismo, non può esimersi dal considerare il rilevante ruolo delle piattaforme digitali molto grandi (cd. *very large online platforms*, *VLOPs*). Ai sensi dell'art. 18 EMFA, le piattaforme digitali più grandi devono fornire una funzionalità che consente ai destinatari dei loro servizi, tra le altre cose, di dichiarare di essere editorialmente indipendenti da qualsiasi Stato (sia membro che terzo all'Unione europea) e di operare conformemente ai meccanismi co-regolatori e auto-regolatori. Inoltre, i fornitori di *VLOPs* devono garantire che le informazioni dichiarate siano rese disponibili al pubblico in modo facilmente accessibile e devono confermare di aver ricevuto le dichiarazioni presentate conformemente all'EMFA. Inoltre, sotto la supervisione del Comitato, è favorito il dialogo strutturato tra fornitori di piattaforme online di dimensioni molto grandi, rappresentanti di fornitori di servizi di *media* e rappresentanti della società civile, con l'obiettivo di promuovere l'accesso a offerte diversificate di *media* indipendenti e monitorare l'adesione alle iniziative di autoregolamentazione, volte a proteggere gli utenti da contenuti nocivi (art. 19 EMFA). Proprio al fine di garantire ai cittadini il diritto di accedere a una pluralità di fonti di informazione, gli utenti possono modificare facilmente le impostazioni di *default* dei propri *device* e possono personalizzare, sulla base degli interessi e delle preferenze, l'offerta di *media* audiovisivi.

V. Le regole per il corretto funzionamento del mercato interno dei *media*

Il mercato dei *media* europeo non può funzionare e raggiungere gli obiettivi definiti nello EMFA, se non c'è un pieno allineamento anche delle fonti normative interne a ciascun Stato membro. In questo senso, le misure legislative adottate da ciascuno dei 27, che possano incidere sul pluralismo dei *media* o sull'indipendenza editoriale dei fornitori di servizi informativi del mercato interno, devono essere giustificate, proporzionate, trasparenti, oggettive e non discriminatorie. Inoltre, ciascun fornitore di servizi multimediali è titolare del diritto di proporre appello contro ogni nuova previsione legale dinnanzi a un organo indipendente (anche non giurisdizionale), fermo restando gli ordinari rimedi previsti dall'ordinamento (art. 21 EMFA).

Le concentrazioni nel mercato dei *media* sono evidentemente antitetiche al pluralismo informativo; per questa ragione gli Stati membri prevedono nei propri ordinamenti norme sostanziali e procedurali che definiscano i criteri di apprezzamento (art. 22 EMFA). Dette norme devono essere trasparenti, oggettive, proporzionate e non discriminatorie e possono prevedere obblighi di notifica per gli operatori che costituiscono concentrazioni e/o incaricare le autorità regolatorie nazionali della valutazione delle stesse. Al fine di adottare un criterio valutativo quanto più uniforme possibile, il Comitato, di propria iniziativa o su richiesta della Commissione, elabora un parere sull'impatto di una certa concentrazione sul pluralismo dei *media* e sull'indipendenza editoriale, qualora tale

ISSN 2239-8570

concentrazione possa incidere sul funzionamento del mercato interno dei servizi informativi (art. 23 EMFA).

In conclusione, con riguardo all'allocazione dei fondi pubblici per la pubblicità statale, lo EMFA dispone che le somme di denaro elargite dagli stati (o da altre autorità pubbliche) in favore di fornitori di servizi informativi a fini pubblicitari siano assegnate secondo criteri trasparenti, oggettivi, proporzionati e non discriminatori e attraverso procedure aperte. In questo senso, devono essere resi noti i nomi di tali fornitori, nonché l'ammontare annuo speso per tale attività, distinto per ciascun fornitore (art. 25 EMFA). Le autorità di regolamentazione nazionale monitorano la corretta allocazione delle risorse e l'osservanza di tali obblighi.

Il Regolamento è entrato in vigore il 7 maggio 2024, fatte salve alcune previsioni che entreranno in vigore durante il 2025. Fa eccezione il sopracitato diritto alla personalizzazione dell'offerta di *media*, previsto dall'art. 20, che diventerà effettivo nel 2027.

GIUSEPPE MUTO

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R1083

2024/4(4)FBe

4. Pubblicata la 'CS3D': direttiva (UE) 2024/1760 sul dovere di diligenza delle imprese ai fini della sostenibilità (*Corporate Sustainability Due Diligence Directive*)

La direttiva (UE) 2024/1760 del Parlamento europeo e del Consiglio del 13 giugno 2024 relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la direttiva (UE) 2019/1937 e il regolamento (UE) 2023/2859, nota come *Corporate Sustainability Due Diligence Directive* (CSDDD o *breviter* **CS3D**, di seguito anche solo la **direttiva**), rappresenta un punto di svolta nella legislazione europea della sostenibilità. Essa, in particolare, segna una tappa decisiva nel passaggio da una concezione volontaristica della responsabilità sociale d'impresa alla consacrazione di doveri di diligenza in ambito sociale e ambientale per le società con un impatto significativo sul mercato interno all'Unione (Considerando 16 e 30 CS3D)

Redatta nell'ambito del c.d. *Green Deal* Europeo e in linea con gli obiettivi dell'Accordo di Parigi, la direttiva si concentra sull'«accountability» e mira a garantire che le imprese si impegnino attivamente e in modo dimostrabile nella prevenzione e nella mitigazione dei propri impatti negativi sui diritti umani e sull'ambiente (Considerando 10 CS3D). La CS3D colloca perciò il ruolo delle imprese al centro della transizione ecologica mediante l'istituzione di un quadro vincolante nel quale responsabilità sociale ed ambientale diventano elemento strutturale delle politiche aziendali.

ISSN 2239-8570

Promuovendo un approccio unificato alla sostenibilità all'interno degli Stati membri, la direttiva muove dalla consapevolezza della necessità di armonizzazione per i requisiti di sostenibilità richiesti all'interno dell'UE, così da evitare distorsioni della concorrenza (Considerando 98, artt. 4 e 36 CS3D).

Per espressa previsione normativa, la direttiva non può essere addotta come giustificazione per la riduzione del livello di tutela dei diritti umani, occupazionali e sociali, di protezione dell'ambiente o del clima previsti dai singoli ordinamenti nazionali o da contratti collettivi ivi applicabili (art. 1(2) CS3D). Le novità normative lasciano altresì impregiudicati gli obblighi previgenti in materia di diritti umani, occupazionali e sociali, nonché di protezione dell'ambiente previsti da altri atti legislativi dell'Unione che – qualora richiedano standard più elevati – prevalgono per gli aspetti contrastanti con la CS3D (art. 1(3) CS3D). Ciononostante, il livello di armonizzazione prescelto dal legislatore comunitario (art. 4 CS3D) – seppur in modo selettivo, ossia con le esclusioni previste dall'art. 4(2) CS3D – impedisce agli Stati membri di introdurre nel proprio diritto nazionale disposizioni divergenti da quelle della direttiva. In particolare, si preclude il ricorso a norme, anche più rigorose, in materia di individuazione e valutazione degli impatti negativi effettivi e potenziali (art. 8 CS3D), di attribuzione di priorità agli impatti negativi effettivi e potenziali individuati (art. 10 CS3D) e di arresto degli impatti negativi effettivi (art. 11 CS3D).

La *ratio* di tale scelta è evidente alla luce dell'esigenza di evitare fenomeni di delocalizzazione volti ad incontrare un diverso *favor* legislativo, soprattutto se si considera che la direttiva, richiedendo alle imprese che soddisfino le condizioni definite nell'art. 2 di integrare pratiche di sostenibilità nelle loro operazioni e lungo la propria *supply chain*, riflette l'intenzione dell'Unione di affrontare i rischi derivanti dalla globalizzazione e dalla complessità delle catene di approvvigionamento

La direttiva si applica infatti alle società che sono costituite in conformità della normativa di uno Stato membro, che si trovino in una delle seguenti condizioni:

- aver avuto, in media, più di 1000 dipendenti e un fatturato netto a livello mondiale superiore a 450 milioni di euro nell'ultimo esercizio (art. 2(1)(a) CS3D); o
- società che sono *holding* di un gruppo che ha raggiunto i limiti di cui sopra nell'ultimo bilancio consolidato (art. 2(1)(b) CS3D); ovvero
- società che abbiano concluso o siano capogruppo di società che hanno concluso contratti di *franchising* o di licenza in cambio di diritti di licenza con società terze indipendenti, qualora tali diritti di licenza ammontassero a più di 22,5 milioni di euro nell'esercizio precedente all'ultimo e a condizione di avere generato o essere a capo di un gruppo che abbia generato un fatturato netto superiore a 80 milioni di euro (art. 2(1)(c) CS3D, e cfr. anche Considerando 27-30 CS3D).

Notevole è poi il disposto delle previsioni dell'art. 2(2) lettere (a), (b) e (c) della CS3D, a tenore delle quali la direttiva si applica anche alle società

ISSN 2239-8570

che sono costituite in conformità della normativa di un paese terzo, laddove esse si trovino in una qualunque delle predette condizioni previste per le società costituite in conformità della normativa di uno Stato membro, ad eccezione solo, per la prima condizione, del requisito del livello occupazionale, essendo sufficiente quello del fatturato.

Come ben spiegato dal Considerando n. 30 della CS3D, infatti, il criterio del fatturato è considerato un indicatore degli effetti che le attività delle società con sede in paesi terzi hanno nel mercato interno all'Unione e che crea perciò un collegamento territoriale con la stessa, che giustifica l'applicazione della CS3D.

Anche in considerazione degli sforzi richiesti per il recepimento della nuova normativa in ciascuno Stato membro e dell'adattamento a cui dovranno sottoporsi i suoi destinatari, l'art. 37 CS3D prevede termini scaglionati, determinati sempre in considerazione di criteri dimensionali e di fatturato, per l'introduzione degli obblighi di diligenza negli ordinamenti nazionali. Solo dal 26 luglio 2029 gli obblighi troveranno applicazione per le società con oltre 1.000 dipendenti e un fatturato superiore a 450 milioni di euro.

Un elemento che agevola la posizione delle società con dimensioni meno rilevanti che partecipano alla catena del valore, per le quali gli oneri economici richiesti per attuare le politiche di sostenibilità prescritte potrebbero essere significativamente penalizzanti, è la previsione di cui all'art. 6 CS3D, che consente alle società madri che rientrano nell'ambito di applicazione della CS3D di adempiere agli obblighi di cui agli articoli da 7 a 11 e all'articolo 22 CS3D per conto di società che sono loro filiazioni e che rientrano nel perimetro applicativo della direttiva.

In termini generali, gli obblighi di due diligence sono strutturati secondo un processo chiaro e articolato, descritto in dettaglio negli artt. 5 e seguenti della CS3D. Le società sono puntualmente chiamate ad integrare un dovere di diligenza basato sull'analisi, sulla prevenzione e mitigazione e sulla riparazione del rischio in materia di diritti umani e di tutela dell'ambiente, all'interno dei propri processi aziendali e lungo la catena del valore (artt. 7 – 12 CS3D).

Il concetto di *due diligence* si concretizza perciò nei doveri di:

- integrare concretamente la sostenibilità nelle politiche aziendali;
- individuare e valutare gli impatti negativi sui diritti umani e sull'ambiente dell'attività svolta;
- prevenire, mitigare o porre fine agli impatti negativi potenziali o esistenti;
- offrire adeguati meccanismi di riparazione in caso di danni;
- monitorare e rendicontare periodicamente i risultati delle azioni intraprese.

Dal punto di vista del monitoraggio e della rendicontazione, l'art. 13 CS3D, così come numerosi Considerando della direttiva, sottolineano l'importanza della trasparenza e del dialogo costruttivo con gli stakeholder, definiti, alla lettera n) dell'art. 3 CS3D, attraverso categorie significative di portatori di interessi: dipendenti della società, dipendenti delle sue filiazioni, sindacati e rappresentanti dei lavoratori, consumatori e altre persone fisiche,

ISSN 2239-8570

gruppi, comunità o soggetti i cui diritti o interessi sono o potrebbero essere lesi dai prodotti, dai servizi e dalle attività della società, delle sue filiazioni e dei suoi partner commerciali, compresi i dipendenti dei partner commerciali e i rispettivi sindacati e i appresentanti dei lavoratori, le istituzioni nazionali in materia di diritti umani e ambiente, le organizzazioni della società civile le cui finalità includono la protezione dell'ambiente e i legittimi rappresentanti di tali persone fisiche, gruppi, comunità o soggetti.

Diritti umani e ambiente sono due aspetti ugualmente centrali nella direttiva, che mira a rafforzarne la protezione tramite una serie di misure preordinate a contribuire «allo sviluppo sostenibile e alla transizione economica e sociale verso la sostenibilità attraverso l'individuazione, e, ove necessario, l'attribuzione di priorità, la prevenzione, l'attenuazione, l'arresto, la minimizzazione e la riparazione degli impatti negativi» connessi alle attività delle imprese, delle loro filiazioni e dei loro partner commerciali nella *supply chain* (Considerando 16 CS3D).

Tra gli elementi maggiormente innovativi della direttiva emerge il piano di transizione per la mitigazione dei cambiamenti climatici, a cui è dedicato l'art. 22 CS3D. La norma si allinea con gli impegni dell'Accordo di Parigi e persegue l'obiettivo della neutralità climatica entro il 2050: nel richiedere alle imprese di definire obiettivi specifici e progressivi per la riduzione delle emissioni di gas serra, le impegna a «garantire, con il massimo impegno possibile, che il modello e la strategia aziendali siano compatibili con la transizione verso un'economia sostenibile e con la limitazione del riscaldamento globale».

Preso atto della circostanza che nel diritto internazionale non si configura una rigida dicotomia fra le obbligazioni di mezzi e quelle di risultato, la dottrina più attenta ha già avuto modo di osservare come i criteri di determinazione dell'inadempimento dell'obbligo scaturente dall'art. 22 CS3D non possano che essere plurimi e da valutarsi con riferimento a ciascuna delle prescrizioni contenute nei 3 commi del medesimo articolo, dando opportuno rilievo ai vincoli contenutistici del piano di transizione, ovvero alla diligenza e agli sforzi profusi nella sua fase attuativa.

Da un punto di vista rimediale, infine, sono opportune alcune notazioni.

Anzitutto, la direttiva incarica gli Stati membri di progettare un sistema sanzionatorio di carattere amministrativo-pubblicistico da applicare in caso di violazione delle disposizioni di diritto nazionale che le daranno recepimento (art. 27 CS3D) e ribadisce la centralità dell'effettività e della proporzionalità del rimedio.

Secondariamente, è particolarmente interessante notare come, nonostante il vivace dibattito che ha caratterizzato i suoi lavori preparatori, la direttiva istituisca un regime di responsabilità che obbliga le imprese a risarcire i danni derivanti dalla mancata attuazione delle misure di *due diligence* (art. 29 CS3D). Nello scenario che va delineandosi, tale responsabilità risarcitoria non consegue solo alle proprie operazioni dirette, ma anche a quelle dei fornitori lungo la catena di approvvigionamento, per i quali la fattispecie riecheggia i contorni della *culpa in vigilando*.

L'art. 29 CS3D non menziona la mancata adozione e attuazione del piano di transizione di cui all'art. 22 CS3D fra gli obblighi la cui violazione

ISSN 2239-8570

determina responsabilità extracontrattuale della società. L'assenza di un riferimento espresso alla fattispecie richiamata, tuttavia, non implica necessariamente che l'accesso al rimedio risarcitorio sarà precluso nei singoli Stati membri. Lo stesso art. 29(6) CS3D, infatti, prevede che «le norme in materia di responsabilità civile di cui alla presente direttiva non limitano la responsabilità delle società ai sensi dei sistemi giuridici dell'Unione o nazionali e lasciano impregiudicate le norme unionali o nazionali in materia di responsabilità civile relative agli impatti negativi sui diritti umani o agli impatti ambientali negativi che prevedono la responsabilità in situazioni non contemplate dalla presente direttiva o che prevedono una responsabilità più rigorosa […]».

Complessivamente, perciò, il sistema di *enforcement* contemplato dalla direttiva mantiene l'impostazione da tempo adottata dal legislatore europeo: ai tradizionali poteri di vigilanza (di propria iniziativa o su segnalazione), ispettivi, di controllo e sanzionatori attribuiti alle autorità nazionali competenti (artt. 24 – 26, Considerando 35 CS3D) sono affiancati strumenti di *enforcement* privatistico, tesi a riparare il pregiudizio sofferto dalle vittime di violazioni dei doveri di diligenza.

Anche dal punto della legittimazione ad agire e del possibile ruolo chiave delle azioni rappresentative nella protezione dei diritti umani e dell'ambiente, le implicazioni pratiche della nuova direttiva sono perciò molteplici.

Sul versante dell'adeguamento da parte delle società che ricadono nel perimetro di applicazione della CS3D alle nuove prescrizioni, si richiede una pianificazione delle strategie di sostenibilità che adatti i modelli operativi esistenti alla necessità di implementare di sistemi di monitoraggio e controllo della catena di fornitura, realizzare audit interni ed esterni periodici e strutturare politiche di sostenibilità che si prefiggano di raggiungere obiettivi misurabili. A livello nazionale, l'introduzione del dovere di diligenza induce inoltre a riflettere sulla responsabilità degli amministratori *ex* art. 2392 ss. c.c. e, in uno scenario di politica legislativa guidato dal principio dello sviluppo sostenibile, il combinato disposto della direttiva in commento e delle previsioni introdotte con la direttiva del 2024 di contrasto al *greenwashing* (direttiva (UE) 2024/825el 28 febbraio 2024, che modifica le direttive 2005/29/CE e 2011/83/UE per quanto riguarda la responsabilizzazione dei consumatori per la transizione verde mediante il miglioramento della tutela dalle pratiche sleali e dell'informazione) solleva l'ineludibile questione della natura e degli effetti dei piani di transizione per la mitigazione dei cambiamenti climatici pubblicamente diffusi presso il pubblico di *stakeholders.*

FRANCESCA BERTELLI

https://eur-lex.europa.eu/eli/dir/2024/1760/oj?locale=it

2024/4(5)EMI

ISSN 2239-8570

5. Il nuovo regolamento (UE) 2024/1781 sui requisiti di progettazione ecocompatibile per prodotti sostenibili (ESPR)

Il regolamento (UE) 2024/1781 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili, modifica la direttiva (UE) 2020/1828 e il regolamento (UE) 2023/1542 e abroga la direttiva 2009/125/CE (di seguito anche il **Regolamento**), costituisce un passo significativo verso la promozione di un mercato unico sostenibile attraverso la progettazione ecocompatibile dei prodotti. Il Regolamento, noto anche come *Ecodesign for Sustainable Products Regulation* (**ESPR**) stabilisce un quadro normativo per l'introduzione di requisiti di progettazione ecocompatibile che i prodotti devono rispettare per essere immessi sul mercato o messi in servizio.

L'obiettivo principale del Regolamento è quello di migliorare la sostenibilità ambientale dei prodotti, riducendo l'impronta di carbonio e l'impatto ambientale complessivo durante il ciclo di vita dei prodotti (c.d. *life cycle assessment)*. L'ambito applicativo del Regolamento è volutamente molto ampio. Esso difatti si applica a quasi tutti i beni fisici immessi sul mercato dell'Unione Europea, inclusi componenti e prodotti intermedi, ma esclude specifiche categorie quali i beni alimentari, i medicinali ed alcuni specifici veicoli (**art. 1**). A corredo di ciò, per particolari dispositivi mobili tecnologici, è da menzionare il regolamento (UE) 2023/1670 della Commissione del 16 giugno 2023 che stabilisce le specifiche per la progettazione ecocompatibile di smartphone, telefoni cellulari diversi dagli smartphone, telefoni cordless e tablet a norma della direttiva 2009/125/CE del Parlamento europeo e del Consiglio e che modifica il regolamento (UE) 2023/826 della Commissione che introduce regole e standard specifici per la progettazione ecocompatibile di smartphone, telefoni cellulari diversi dagli smartphone e telefoni cordless.

Il regolamento (UE) 2024/1781, all'**art. 5**, stabilisce criteri chiari ed uniformi per la progettazione ecocompatibile dei prodotti da rispettarsi nella filiera produttiva. Ad essi vanno aggiunti i requisiti di progettazione ecocompatibile contenuti negli atti delegati adottati a norma **dell'art. 4**. Tali criteri mirano a garantire che i prodotti immessi nel mercato europeo non solo siano sostenibili da un punto di vista ambientale ma siano anche sicuri per la salute umana. Simili requisiti possono includere parametri quantitativi e non quantitativi finalizzati al miglioramento delle prestazioni ecologiche dei prodotti, in virtù di quanto disposto dall'art. 6 del Regolamento.

In particolare, all'**art. 7** del Regolamento, si prescrivono specifici obblighi informativi. Ogni prodotto, infatti, deve contenere i riferimenti al c.d. **passaporto digitale** (**art. 2, n. 28** del Regolamento) e, a seconda dei casi, le informazioni in merito a "**sostanze che destano preoccupazione**" (**art. 2, n. 27** del Regolamento). Le informazioni così fornite devono essere chiare, facilmente comprensibili e adattate alle caratteristiche particolari dei gruppi di prodotti interessati e dei destinatari delle informazioni stesse.

Senza dubbio uno degli aspetti più rilevanti del Regolamento è il c.d. **passaporto digitale del prodotto**, ovvero uno strumento destinato a

ISSN 2239-8570

migliorare la trasparenza e la tracciabilità dei prodotti sul mercato. Questo passaporto deve contenere tutte le informazioni, dettagliatamente descritte nel Capo III del Regolamento, sui requisiti di sostenibilità e sulle caratteristiche ecologiche dei prodotti. È prevista l'introduzione entro il 19 luglio 2026 di un **registro generale dei passaporti digitali dei prodotti** (art. 13 del Regolamento). L'obiettivo è di facilitare l'accesso ad informazioni chiare per i consumatori ed a fornire alle Autorità competenti gli elementi idonei alla verifica del rispetto dei requisiti di progettazione prescritti.

Inoltre, il Regolamento dispone la definizione di requisiti obbligatori per gli **appalti pubblici verdi** (nello specifico, **art. 65** del Regolamento). Le amministrazioni pubbliche sono incoraggiate a scegliere fornitori che rispettano standard elevati di sostenibilità nonché a rispettare le c.d. prescrizioni minime finalizzate ad integrare virtuose pratiche ecologiche nell'ambito delle politiche pubbliche.

Come noto, la sostenibilità ambientale impone notevoli oneri economici, specialmente per gli operatori economici più piccoli e meno strutturati. Per tale ragione, il Regolamento prevede una serie di iniziative di supporto, tra cui assistenza tecnica, formazione e accesso a finanziamenti per facilitare l'integrazione della sostenibilità nei processi produttivi delle PMI (**art. 22** del Regolamento).

Ulteriore tassello centrale del Regolamento, come stabilito dall'**art. 23**, è rappresentato dall'obbligo imposto ai produttori ed altri operatori economici (subfornitori o mandatari) di adottare tutte le misure necessarie che ci si può ragionevolmente attendere per evitare la necessità di distruggere i prodotti di consumo invenduti. In effetti il **Capo VI** del Regolamento è interamente dedicato alla **disciplina dei prodotti di consumo invenduti** ed alle misure per evitare sprechi, prevenire la distruzione ed agevolare il passaggio ad una economia circolare, attraverso il riuso e il riutilizzo dei prodotti o di loro singoli componenti.

Infine, il Regolamento attribuisce alle singole autorità nazionali competenti il potere di svolgere controlli regolari sui prodotti immessi nel mercato al fine di verificare la loro conformità ad i requisiti di progettazione stabiliti. In aggiunta e nell'ipotesi di mancata conformità agli standard di sostenibilità prescritti, le Autorità potranno imporre sanzioni economiche per le violazioni accertate. Gli operatori economici latamente intesi (produttori, fornitori, distributori, importatori e mandatari) sono, invece, tenuti a fornire la documentazione tecnica necessaria per i relativi controlli di conformità.

In conclusione, il presente Regolamento rappresenta un momento determinante nel percorso che porta alla definitiva costituzione di un mercato unico sostenibile. Difatti, con l'introduzione di requisiti rigorosi di progettazione ecocompatibile dei prodotti e di un passaporto digitale per ogni prodotto immesso, l'Unione dà rilievo all'esigenza ormai consolidata di un modello economico più sostenibile, sia sotto il profilo ambientale sia sotto il profilo economico. Non a caso, il Regolamento introduce misure volte a ridurre lo spreco e la distruzione dei prodotti invenduti e finalizzate ad un sistema circolare di riutilizzo e di riuso dei beni. È altrettanto

ISSN 2239-8570

evidente, anche alla luce degli incentivi introdotti, che la corretta implementazione di siffatte regole nelle diverse filiere produttive possa fornire nuove opportunità per tutti gli operatori economici.

ENZO MARIA INCUTTI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202401781

2024/4(6)VR

6. Approvato il Cyber Resilience Act (CRA) sui requisiti di cibersicurezza dei prodotti connessi: regolamento (UE) 2024/2847

In seguito ad un iter legislativo cominciato nel settembre 2022 con una proposta della Commissione (COM (2022) 454, su cui v. in questa Rubrica la notizia n. 4 nel numero 3/2022 [2022/3(4)VR], e in *Atlante*, p. 226) è stato approvato definitivamente il regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) c.d. '**Cyber Resilience Act**' (di seguito **CRA** o anche solo il **Regolamento**). L'atto consta di 130 Considerando, 71 articoli e 8 Allegati e conferma in larga misura le soluzioni della proposta del 15 settembre 2022.

Il Preambolo muove dalle *rationes* alla base della regolazione.

Sul versante fenomenologico: l'aumento esponenziale dei dispositivi connessi, l'impatto degli attacchi informatici sull'economia, la democrazia, la salute e la sicurezza dei consumatori. Più precisamente, i due maggiori problemi che il Regolamento ambisce a fronteggiare sono il basso livello di cibersicurezza dei prodotti con elementi digitali e la scarsa comprensibilità delle informazioni, che impedisce agli utilizzatori una scelta consapevole e un utilizzo sicuro dei prodotti (v. Considerando 1 CRA e, specificamente sul deficit di trasparenza, il Considerando 2 CRA). Sul versante normativo, la parzialità e frammentarietà del regime giuridico precedente, che reclamava uniformità quanto ai requisiti essenziali di cibersicurezza per l'immissione sul mercato europeo di prodotti con elementi digitali (Considerando 4 CRA). Si pone, poi, nuovamente l'accento sulla dimensione transfrontaliera del fenomeno e ad essa si accompagna una rinnovata enfasi sulla proporzionalità delle prescrizioni per le microimprese e le PMI e sulla necessità di assistenza degli operatori economici negli adempimenti di *compliance* (v. Considerando 5, 6, 93-97, art. 33 CRA). Conserva importanza, inoltre, il carattere interconnesso degli ambienti digitali, da cui deriva che anche hardware e software a bassa criticità, ove integrati in un sistema di informazione elettronico più ampio o comunque connessi a quest'ultimo, possono fungere da vettore per potenziali attacchi (v. Considerando 9 CRA). Specifica attenzione viene posta sui prodotti

ISSN 2239-8570

destinati ai consumatori vulnerabili, come i giocattoli e sistemi di monitoraggio dei neonati, che rientrano espressamente tra i prodotti con elementi digitali importanti e come tali sottoposti a procedure di valutazione della conformità più rigorose (v. Considerando 10 CRA; cfr. Considerando 43 CRA).

L'orizzontalità delle prescrizioni del Regolamento richiede fatalmente un coordinamento con gli altri regimi normativi di matrice europea. In generale, quanto alle regolazioni settoriali, dettate per determinati prodotti con elementi digitali, al Considerando 28 CRA si chiarisce che l'applicazione delle disposizioni ivi contenute può essere limitata o esclusa laddove siano congiuntamente soddisfatti i criteri di coerenza *(«qualora tale limitazione o esclusione sia coerente con il quadro normativo generale applicabile a tali prodotti»*) ed equivalenza (*«qualora le norme settoriali conseguano almeno lo stesso livello di protezione previsto dal presente regolamento»*). Distinta considerazione guadagna il raccordo con la direttiva (UE) 2024/2853 sulla responsabilità da prodotto difettoso, c.d. **nuova PLD**, anch'essa approvata il 23 ottobre 2024 (su cui v. *supra* in questa Rubrica, su questo numero notizia n. 2 [2024/4(2)TDMCDV]): se la mancanza di sicurezza consiste nell'assenza degli opportuni aggiornamenti (prescritti dal Regolamento) dopo l'immissione sul mercato del prodotto e ciò causa un danno, questo potrebbe fondare la responsabilità del fabbricante (v. Considerando 31 CRA). Più agevole il coordinamento col regolamento UE 2016/679 (**GDPR**), data la piena complementarietà degli scopi e le sinergie tra i requisiti essenziali di cibersicurezza e il diritto dell'Unione in materia di protezione dei dati personali (v. Considerando 32 CRA).

Si ribadisce poi l'obiettivo di garantire la sicurezza dei prodotti digitali lungo tutto il loro ciclo di vita

(in generale, v. Considerando 54 CRA e l'enfasi posta sull'obbligo di assistenza ai Considerando 60-63 CRA).

Più specificamente, a tal fine: in fase di progettazione e sviluppo, ove i fabbricanti integrino componenti provenienti da terzi, essi sono tenuti a esercitare la dovuta diligenza per garantirne la conformità, tenuto conto della natura e del livello di rischio associato al singolo componente (v. Considerando 34 e 35 CRA); i requisiti essenziali di cibersicurezza devono sussistere al momento dell'immissione sul mercato; qualsiasi successiva modifica, alterativa del prodotto in un modo non previsto dal fabbricante nella valutazione dei rischi iniziale e potenzialmente attenuativa degli standard di cibersicurezza, deve qualificarsi modifica sostanziale (v. Considerando 38 CRA). Quest'ultima deve ritenersi sussistente altresì in caso di aggiornamenti del software che modifichino la finalità del prodotto, mutino la natura del pericolo ovvero il livello di rischio e giustifica (v. Considerando 39 CRA), se del caso, una nuova valutazione della conformità (v. Considerando 41 CRA).

L'echeggiato riferimento al criterio di proporzionalità non riguarda solo i destinatari delle prescrizioni ma anche l'oggetto della regolazione. Al riguardo, il Considerando 44 CRA suddivide i prodotti con elementi digitali importanti in due classi (classe I e classe II), sulla base del livello rischio, e

ISSN 2239-8570

alla seconda annoda un maggior rigore delle valutazioni di conformità (v. anche Considerando 90 CRA).

Proseguendo con la tassonomia, al Considerando 46 CRA si introduce la nozione prodotti con elementi digitali critici, definiti come quelli aventi una funzionalità legata alla cibersicurezza e che implicano un rischio significativo di effetti negativi in termini di intensità e capacità di perturbare, controllare o recare danno a un gran numero di altri prodotti con elementi digitali mediante manipolazione diretta.

Sempre a livello di Preambolo, il legislatore europeo tratta dei limiti fisiologici delle prescrizioni di cibersicurezza, cioè a dire le ipotesi in cui alcuni requisiti essenziali non sono applicabili a un prodotto con elementi digitali a cagione della loro incompatibilità con la natura stessa del bene. In questi casi, il fabbricante dovrebbe fornire una chiara giustificazione nella valutazione dei rischi di inclusa nella documentazione tecnica (Considerando 55 CRA).

Tra gli obblighi imposti ai fabbricanti, merita menzione quello di redazione di una dichiarazione di conformità UE che fornisca le informazioni richieste dal Regolamento e, ove applicabili, da altri atti normativi europei pertinenti (Considerando 88 CRA).

L'effettività del quadro uniforme di cibersicurezza dei prodotti digitali richiede un livello uniforme di qualità nello svolgimento della valutazione della conformità. Per garantire quest'ultimo è necessario fissare requisiti da far applicare alle autorità di notifica e agli altri organismi deputati. Allo specifico regime previsto dal Regolamento deve accompagnarsi il sistema di accreditamento di cui al regolamento CE n. 765/2008 (Considerando 99 CRA). Fra i presidi di effettività e di corretta e uniforme applicazione della disciplina v'è poi l'attività di vigilanza del mercato, col naturale *pendant* di adeguati poteri sanzionatori (Considerando 120 CRA). Al riguardo, le norme sulla vigilanza del mercato dell'Unione e sul controllo dei prodotti che entrano nel mercato dell'Unione di cui al regolamento (UE) 2019/1020 si applicano ai prodotti con elementi digitali che rientrano nell'ambito di applicazione del Regolamento (Considerando 106-111 CRA).

Quanto al corpo del Regolamento, anch'esso ricalca in buona parte quello della proposta.

Il Capo I delimita anzitutto l'oggetto (art. 1 CRA), che si articola in: a) norme per l'immissione sul mercato di prodotti con elementi digitali, al fine di garantirne la cibersicurezza; b) requisiti essenziali di progettazione, sviluppo e produzione e relativi obblighi per gli operatori economici c) requisiti essenziali per i processi di gestione delle vulnerabilità e relativi obblighi per gli operatori economici; d) norme sulla sorveglianza del mercato e sull'applicazione della disciplina in oggetto.

Segue la delineazione dell'ambito applicativo (art. 2 CRA), esteso a tutti i prodotti con elementi digitali il cui uso previsto o ragionevolmente prevedibile include una connessione logica o fisica (come definite all'art. 3 nn. 7, 8 CRA) diretta o indiretta di dati a un dispositivo o a una rete.

Quanto alle ipotesi di esclusione, si registra qualche ridotto ampliamento rispetto alla proposta. Restano esclusi: i prodotti disciplinati dal regolamento (UE) 2017/745 (relativo ai dispositivi medici) e dal

ISSN 2239-8570

regolamento (UE) 2017/746 (relativo ai dispositivi medico-diagnostici in vitro), quelli certificati in conformità al regolamento (UE) 2018/1139 (recante norme comuni in materia di aviazione civile) nonché quelli ai cui fa riferimento il regolamento (UE) 2019/2144 (sui requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada). Sono sottratti alla normativa in oggetto altresì: i prodotti sviluppati esclusivamente per scopi di sicurezza nazionale o militari; quelli specificamente progettati per elaborare informazioni classificate; l'equipaggiamento marittimo di cui alla direttiva 2014/90/UE; i pezzi di ricambio messi a disposizione sul mercato per sostituire componenti identici in prodotti con elementi digitali e fabbricati secondo le stesse specifiche dei componenti che sono destinati a sostituire; i prodotti con elementi digitali contemplati da altre norme europee che stabiliscono requisiti che affrontano tutti o alcuni rischi contemplati dai requisiti essenziali di cibersicurezza di cui all'Allegato I, qualora ciò sia coerente con il quadro normativo generale applicabile a tali prodotti e le norme settoriali conseguano lo stesso livello di protezione previsto dal Regolamento o uno maggiore.

L'art. 4 CRA, analogamente alla corrispondente disposizione contenuta nella proposta, imprime una regola di libera circolazione dei prodotti con elementi digitali, vietando agli Stati membri di impedirne la messa a disposizione sul mercato interno.

Nuovo è invece l'art. 5 CRA, il quale – nonostante si tratti di una fonte uniformatrice – consente agli Stati membri di imporre requisiti di cibersicurezza supplementari, seppur solo allorché: l'acquisto o l'utilizzo dei prodotti avvenga per fini specifici; si rispettino i principi di coerenza, necessarietà e proporzionalità agli scopi del diritto dell'Unione.

Il quadro generale dei requisiti essenziali per la conformità e dei relativi processi messi in atto dai produttori è fornito all'art. 6 CRA, riproponendo il rinvio agli Allegati (rispettivamente, All. I, part I e All. I, parte II).

Gli artt. 7 e 8 CRA testimoniano un ampliamento della tassonomia e, per l'effetto, una più capillare disciplina.

La prima diposizione regola i prodotti con elementi digitali cc.dd. importanti, aventi la funzionalità principale di una delle categorie riportate all'Allegato III. Questi, in consonanza col Considerando 44 CRA, sono divisi in **due classi** (classe I e classe II) e devono possedere le caratteristiche indicate al par. 2. Sono inoltre assoggettati alle procedure di valutazione della conformità di cui all'art. 32, parr. 2 e 3 CRA, ancorché tali obblighi non si estendono di per ciò solo al prodotto finale in cui essi siano eventualmente integrati. Infine, alla Commissione è conferito il potere di adottare atti delegati conformemente all'art. 61 CRA, al fine di modificare l'Allegato III nel senso di includere nuove categorie all'interno delle menzionate classi, trasferire una categoria da una classe a un'altra ovvero eliminare una categoria esistente, tenendo conto delle funzionalità relative alla cibersicurezza o della funzione e del livello di rischio.

ISSN 2239-8570

La seconda disposizione regola invece i prodotti con elementi digitali cc.dd. critici. Per essi è conferito alla Commissione il potere di adottare atti delegati conformemente all'art. 61 CRA, al fine di determinare, in ossequio ai parametri del par. 2, quali prodotti aventi la funzionalità principale di una categoria di cui all'Allegato IV debbano ottenere un certificato europeo di cibersicurezza a un livello di affidabilità almeno "sostanziale" nell'ambito di un sistema europeo di certificazione adottato a norma del regolamento (UE) 2019/881.

L'art. 12 CRA "promuove" il raccordo con il regolamento (UE) 2024/1689 (Artificial Intelligence Act, **AIA**) *medio tempore* entrato in vigore, traslando la disciplina, che la proposta relegava al Considerando 16 del Preambolo, nel corpo dell'atto. I prodotti con elementi digitali classificati come sistemi di IA ad alto rischio ex art. 6 AIA sono considerati conformi ai requisiti di cibersicurezza di cui all'art. 15 del Regolamento qualora: *a*) soddisfino i requisiti essenziali di cui all'Allegato I, parte I CRA; *b*) i processi messi in atto dal fabbricante siano conformi ai requisiti essenziali di cui all'Allegato I, parte II CRA; il conseguimento del livello di protezione della cibersicurezza fissato dall'art. 15 CRA sia dimostrato nella dichiarazione di conformità UE. Per tali prodotti, inoltre, si applica la pertinente procedura di valutazione della conformità prevista dall'art. 43 AIA.

Il Capo II del Regolamento tratta degli obblighi degli operatori economici e pone disposizioni in materia di software liberi e open source.

Pietra angolare della disciplina è l'art. 13 CRA. Esso distribuisce, in ben 25 paragrafi, gli obblighi dei fabbricanti, che di seguito si compendiano.

Anzitutto, questi ultimi devono assicurare, all'atto dell'immissione sul mercato (cfr. Considerando 38 CRA), che il prodotto con elementi digitali sia stato progettato, sviluppato e prodotto conformemente ai requisiti essenziali di cibersicurezza di cui all'Allegato I, parte I. L'adempimento di tale obbligo richiede logicamente una previa valutazione dei rischi, da condurre lungo tutte le fasi della produzione *lato sensu* intesa, al fine di minimizzare i rischi, prevenire gli incidenti e ridurne al minimo l'impatto (par. 2 CRA). Tale valutazione deve essere documentata e aggiornata e comprendere almeno un'analisi dei rischi di cibersicurezza basata sulla finalità prevista e sull'uso ragionevolmente prevedibile del prodotto, nonché sulle sue condizioni d'uso, tenendo conto della durata di utilizzo del prodotto prevista (par. 3 CRA). In consonanza coi Considerando 34 e 35 CRA, il par. 5 prescrive un obbligo di diligenza nell'integrazione di componenti provenienti da terzi, affinché essi non compromettano la cibersicurezza del prodotto.

Laddove emergano vulnerabilità in un componente, anche open source, è posto dovere di segnalazione al soggetto incaricato della fabbricazione o della manutenzione e di correzione della vulnerabilità conformemente di cui all'Allegato I, parte II (par. 6).

Come già testimoniato dai Considerando 60-63 CRA, grande enfasi è posta sull'obbligo collaterale di assistenza. In particolare, il par. 8, comma 2 ss. ne regola la durata, prescrivendo in maniera elastica che «i fabbricanti determinano il periodo di assistenza in modo che rifletta la durata di utilizzo

ISSN 2239-8570

prevista del prodotto, tenendo conto, in particolare, delle ragionevoli aspettative degli utilizzatori, della natura del prodotto, compresa la sua finalità prevista, nonché del pertinente diritto dell'Unione che determina la durata di vita dei prodotti con elementi digitali». In ogni caso, il periodo di assistenza dovrà essere di almeno cinque anni o coprire la durata attesa di utilizzo del prodotto, ove inferiore.

Come presidio riequilibrativo di eventuali cc.dd. "asimmetrie informatiche", il par. 18 prescrive ai produttori di accompagnare ai prodotti le informazioni e le istruzioni per l'utilizzatore di cui all'Allegato II, imponendone chiarezza, compensabilità, intellegibilità e idoneità a consentire un'installazione, un funzionamento e un utilizzo del bene sicuri.

La trama regolatoria segue poi, all'art. 14 CRA, con gli obblighi di segnalazione dei fabbricanti.

In sintesi, quest'ultimi debbono notificare simultaneamente al CSIRT designato come coordinatore

conformemente al par. 7, e all'ENISA: *i*) qualsiasi vulnerabilità attivamente sfruttata di cui giungano a conoscenza, seguendo gli adempimenti di cui al par. 2; *ii*) qualsiasi incidente grave (come definito al par. 5) che abbia un impatto sulla sicurezza del prodotto con elementi digitali di cui abbiano conoscenza, conformemente agli adempimenti di cui al par. 4. In ambo i casi la notifica dovrà effettuarsi tramite la piattaforma unica di segnalazione istituita a norma dell'art. 16 CRA.

Per le ipotesti meno gravi – a dire, qualsiasi vulnerabilità o le minacce informatiche che potrebbero incidere sul profilo di rischio di un prodotto con elementi digitali ovvero qualsiasi incidente che abbia un impatto sulla sicurezza del bene – è prevista una mera facoltà di segnalazione (volontaria), peraltro esercitabile anche da persone fisiche (art. 15 CRA).

Similmente all'art. 12 della proposta, l'art. 18 del Regolamento assegna ai cc.dd. rappresentanti autorizzati un ruolo di interlocutore qualificato dell'autorità di vigilanza del mercato.

Si conferma altresì l'attribuzione agli importatori del ruolo di controllo e garanzia (cfr. l'art. 13 della proposta). Questi, in sintesi, sono tenuti a: immettere sul mercato solo prodotti con elementi digitali conformi ai requisiti essenziali di cui all'All. I, parte I e i cui processi risultino conformi all'All. I, parte II; prima dell'immissione sul mercato, garantire l'esatta esecuzione delle procedure di valutazione della conformità *ex* art. 32 CRA, la redazione della documentazione tecnica e l'apposizione della marcatura CE di cui all'art. 30 CRA, assieme alle informazioni e dalle istruzioni di cui all'All. II., da parte del fabbricante; che quest'ultimo abbia soddisfatto i requisiti di cui all'art. 13, parr. 15, 16, 19 CRA.

Qualora l'importatore abbia fondati dubbi sulla conformità del prodotto o dei processi, gli è fatto divieto di immetterlo fino a quando entrambi sono resi conformi. Seguono gli obblighi di segnalazione al fabbricante e a questi e all'autorità di vigilanza del mercato ove si tratti di rischi di cibersicurezza significativi. Ove tale diagnosi si traduca in certezza o fondato sospetto di non conformità, è prescritta l'adozione delle misure correttive necessarie o, se del caso, il richiamo o il ritiro del prodotto.

ISSN 2239-8570

La platea dei destinatari della disciplina termina con i distributori. Anche nella sua versione finale, il Regolamento conferma l'indirizzo di incremento dei doveri di controllo e di modulazione delle garanzie in senso proporzionale all'allungamento della catena (art. 19 CRA).

A fronte di un generale dovere di diligenza, tali operatori sono tenuti, prima della messa a disposizione di un prodotto con elementi digitali, a verificare l'avvenuta apposizione della marcatura CE e l'effettivo assolvimento da parte del produttore e dell'importatore degli adempimenti previsti, rispettivamente, dall'art. 13, parr. 15, 16, 18, 19 e 20, e dall'art. 19, par. 4 CRA. Per il resto, la disposizione ricalca la disciplina predisposta per gli importatori quanto ai fondati motivi di dubbio sulla conformità, originari o sopravvenuti, ai doveri di avviso, correzione e intervento. Gli artt. 21 e 22 CRA, infine, tipizzano i casi in cui i distributori e gli importatori ovvero persone fisiche o giuridiche diverse da essi sono assoggettati agli obblighi imposti ai produttori, ossia immettano sul mercato un prodotto con il proprio nome o marchio o vi effettuino una modifica sostanziale.

Una menzione specifica acquistano i gestori di software open source. L'art. 24 CRA prescrive ad essi, oltre a un obbligo di cooperazione con le autorità di vigilanza, la formalizzazione di una politica in materia di cibersicurezza che, tra l'altro: assicuri un'efficace gestione delle vulnerabilità; ne promuova la segnalazione volontaria di cui all'art. 15 CRA; ne predetermini misure di correzione.

Il Capo III è dedicato alla conformità dei prodotti e, conformemente alla proposta, muove da una regola presuntiva. Ai sensi dell'art. 27 CRA, i prodotti e i processi che risultano conformi alle norme armonizzate si presumono conformi ai requisiti essenziali di cibersicurezza di cui all'Allegato I. Lo stesso vale per i prodotti e i processi per i quali sono stati rilasciati un certificato o una dichiarazione di conformità UE nell'ambito di un sistema europeo di certificazione della cibersicurezza adottato a norma del regolamento (UE) 2019/881, nella misura in cui tali requisiti siano contemplati dai documenti menzionati.

Il par. 2 assegna alla Commissione margini di intervento normativo – per così dire – doppiamente sussidiari. Nello specifico, essa ha il potere di adottare atti di esecuzione che stabiliscono specifiche comuni relative ai requisiti tecnici che forniscono i mezzi per soddisfare i requisiti essenziali di cibersicurezza di cui all'Allegato I. Tale potestà è subordinata ad alcune condizioni, tra cui merita segnalare l'assenza, attuale e ragionevolmente attesa, di pertinenti norme armonizzate.

L'art. 28 CRA disciplina la dichiarazione di conformità UE. Redatta dai fabbricanti in conformità dell'art. 13, par. 12 CRA, essa: attesta il rispetto dei requisiti essenziali di cui all'Allegato I; ha la struttura tipo di cui all'Allegato V (o dell'Allegato VI, ove semplificata *ex* art. 13, par. 20); contiene gli elementi specificati nelle pertinenti procedure di valutazione della conformità di cui all'Allegato VIII; deve essere opportunamente aggiornata. Ai sensi del par. 4, la redazione della dichiarazione comporta per il fabbricante l'assunzione della responsabilità della conformità del prodotto con elementi digitali.

ISSN 2239-8570

Gli artt. 30 e 31 CRA trattano rispettivamente della marcatura CE e della documentazione tecnica. In particolare, la seconda, da redigersi prima dell'immissione del prodotto sul mercato, contiene tutti i dati o i dettagli pertinenti relativi ai mezzi utilizzati dal fabbricante per garantire che il prodotto e i processi siano conformi ai requisiti di cui all'Allegato I nonché gli elementi di cui all'Allegato VII.

Il mantenimento di elevati standard di sicurezza informatica e della fiducia dei soggetti interessati fonda l'enfasi posta al Capo IV sulla notifica agli organismi di valutazione della conformità.

In particolare, gli Stati membri sono tenuti a notificare alla Commissione e agli altri Stati membri l'elenco di tali organismi (art. 35 CRA) e designano un'autorità di notifica – dotata dei requisiti di cui all'art. 37 CRA – responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, nonché della designazione e notifica degli organismi di valutazione della conformità (art. 36 CRA).

Merita evidenziare che gli organismi notificati devono essere in possesso dei requisiti di cui all'art. 39, parr. 2-12 CRA e sono soggetti agli obblighi operativi di cui all'art. 47 del Regolamento.

L'apparato normativo si correda, al Capo V, di un modulo di *public enforcement*: «vigilanza del mercato e applicazione delle norme». Al fine di garantire l'efficace attuazione del Regolamento, ciascuno Stato membro designa una o più autorità di vigilanza.

Laddove vi siano elementi sufficienti per ritenere che un prodotto con elementi digitali presenta un rischio di cibersicurezza significativo, si impone l'avvio di procedure di valutazione, ripartite a livello nazionale ed europeo e gestite, rispettivamente, dall'Autorità di vigilanza del singolo Stato membro (art. 54 CRA) e dalla Commissione (art. 56 CRA).

Di particolare interesse risulta l'art. 57 CRA, che regola l'ipotesi in cui prodotti digitali conformi per i quali sia stata effettuata la valutazione *ex* art. 54 conservino ancora un margine di rischio di cibersicurezza significativo e comportino un rischio per: la salute o la sicurezza delle persone; la conformità agli obblighi – europei o nazionali – a tutela dei diritti fondamentali; la disponibilità, l'autenticità, l'integrità o la riservatezza dei servizi offerti; altri aspetti della tutela dell'interesse pubblico. In tali casi, l'Autorità di vigilanza del mercato di uno Stato membro richiede all'operatore economico di adottare tutte le misure del caso.

Da ultimo, può farsi cenno al Capo VII del Regolamento, che disciplina riservatezza e sanzioni. Specularmente alla proposta, al dovere generale di riservatezza sulle informazioni e sui dati ottenuti dai soggetti interessati nello svolgimento dei loro compiti e delle loro attività (art. 63 CRA) si accompagna la disciplina delle sanzioni (art. 64 CRA).

VALENTINO RAVAGNANI

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202402847

ISSN 2239-8570

2024/4(7)MM

7. L'inizio di applicazione del regolamento (UE) 2023/988 relativo alla sicurezza generale dei prodotti (GPSR)

A partire dal 13 dicembre 2024 è diventato applicabile il regolamento (UE) 2023/988 del 10 maggio 2023 che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio relativo alla sicurezza generale dei prodotti (*General Product Safety Regulation*, **GPSR**, di seguito anche il **Regolamento**). La scelta di sostituire la precedente Direttiva 2001/95/CE con un regolamento, unitamente alla base giuridica individuata nell'art. 114 del Trattato sul funzionamento dell'Unione europea (**TFUE**), delineano un'ambizione a migliorare il funzionamento del mercato interno proponendo una protezione maggiormente armonizzata e uniforme, in grado di affrontare le sfide poste da un contesto tecnologicamente più avanzato, in funzione di garantire che tutti i prodotti immessi sul mercato siano sicuri per l'uso previsto, proteggendo in particolare i consumatori più vulnerabili come bambini, anziani e persone con disabilità. Allo stesso tempo, una normativa identica in tutto il territorio europeo, senza divergenze di recepimento, assicura anche condizioni uniformi per gli operatori economici, evitando distorsioni e garantendo una concorrenza leale.

Entrando nel merito, il Regolamento si applica a tutti i prodotti destinati ai consumatori o che possono essere ragionevolmente da loro utilizzati, inclusi quelli venduti online o tramite altri mezzi a distanza, con l'ulteriore precisazione che -operando secondo logiche tipicamente preventive- la sua applicazione è estesa indirettamente anche ai professionisti, qualora tali beni siano immessi sul mercato dei consumi e siano quindi acquistabili liberamente presso un punto vendita fisico o un sito online.

Sotto il profilo oggettivo, il Regolamento riguarda tutti i prodotti di consumo immessi sul mercato europeo, sia nuovi che usati, riparati o ricondizionati, salvo non esistano altre norme di carattere speciale che ne regolino la sicurezza o che una specifica tipologia di prodotti sia espressamente esclusa dall'ambito di applicazione del Regolamento. Ad esempio, si conferma l'esclusione del settore alimentare, per il quale continua a trovare applicazione il Reg. (UE) 178/2002, in ragione delle peculiarità dell'alimento il quale, essendo destinato a essere ingerito dall'essere umano e avendo un significativo impatto sulla sua salute, continua a beneficiare di una disciplina autonoma e distinta. Sempre sotto questo profilo, si pone anche un tema di coordinamento tra la disciplina contenuta nel Regolamento e nelle normative armonizzate, ove si prevede che l'obbligo generale di sicurezza dei prodotti si applichi anche ai prodotti di consumo ricompresi nelle normative di armonizzazione dell'Unione, qualora queste non contemplino i rischi coperti dalla disciplina in esame. E

ISSN 2239-8570

così, sempre che la normativa di armonizzazione non preveda disposizioni specifiche con lo stesso obiettivo, si applicheranno a tutti i prodotti di consumo gli obblighi dei fornitori di mercati online, gli obblighi degli operatori economici in caso di incidenti, il diritto di informazione e di rimedio, le disposizioni in tema di Safety Gate (*v. infra*), nonché i richiami per la sicurezza dei prodotti.

Si delinea dunque una disciplina di prodotto, che impedisce la circolazione di articoli che non siano sicuri. In tal senso, il Regolamento delinea un concetto di sicurezza che trova il proprio riferimento nell'art. 5, i cui contenuti sono specificati all'art. 3, lett. b). Ai sensi dell'art. 5, "gli operatori economici immettono o mettono a disposizione sul mercato solo prodotti sicuri" (c.d. requisito di sicurezza generale), chiarendo che con "prodotto sicuro" si intende qualsiasi prodotto che, in condizioni normali o ragionevolmente prevedibili di uso, compresa la durata effettiva dell'uso, non presenta alcun rischio o solo rischi minimi compatibili con l'uso del prodotto, considerati accettabili e coerenti con un elevato livello di protezione della salute e della sicurezza dei consumatori (art. 3).

L'articolo 6 offre un quadro piuttosto dettagliato sui criteri da considerare per valutare la sicurezza di un prodotto. Tra questi, rientrano diversi aspetti, come le caratteristiche intrinseche del prodotto stesso, ad esempio la progettazione, le specifiche tecniche, la composizione, l'imballaggio e le istruzioni d'uso. Viene inoltre considerato l'effetto che il prodotto può avere su altri articoli con cui entra in contatto. Attenzione particolare è riservata anche alla presentazione, che comprende elementi come l'etichettatura, le avvertenze e le informazioni fornite al consumatore, sul presupposto che la sicurezza di un prodotto passa anche attraverso l'adempimento di specifici obblighi informativi. Si tiene conto anche delle categorie di consumatori cui il prodotto è destinato, con un *focus* su gruppi particolarmente vulnerabili, come i bambini, e sull'aspetto del prodotto, soprattutto quando questo può richiamare alimenti o risultare particolarmente attraente per i più piccoli. Infine, sono inclusi nei criteri di valutazione anche aspetti legati alla cibersicurezza e alle funzionalità avanzate del prodotto, come quelle evolutive, di apprendimento o predittive, che possono influire sulla sicurezza complessiva.

Per garantire che la valutazione sulla conformità del prodotto sia stata svolta correttamente alla luce dei criteri sopra indicati, l'art. 7 introduce una presunzione di conformità all'obbligo generale di sicurezza di cui all'art. 5. Detta presunzione può essere soddisfatta attraverso due modalità: o il prodotto è stato fabbricato nel rispetto dei processi di carattere tecnico di cui al Reg. (UE) 1025/2012 oppure, in assenza di una normativa armonizzata, questo è conforme alle normative nazionali. Anche in funzione di una maggiore armonizzazione, la Commissione potrà, tramite atti di esecuzione, determinare successivamente i requisiti specifici di sicurezza che devono essere disciplinati dalle norme europee, al fine di garantire che i prodotti conformi a tali discipline soddisfino l'obbligo generale di sicurezza.

L'art. 8, infine, si interessa ai casi in cui la valutazione di sicurezza da svolgere alla stregua dei criteri indicati all'art. 6 non possa essere garantita tramite la presunzione di cui all'art. 7. In tal caso, allora, possono essere

ISSN 2239-8570

presi in considerazione le norme nazionali e internazionali, i sistemi di certificazione volontaria, i codici di buona condotta nonché le ragionevoli aspettative dei consumatori (art. 8).

Fermo restando che il requisito generale di sicurezza deve essere garantito al momento della immissione in commercio del prodotto, vale rammentare che ormai tutti i processi di produzione e distribuzione si muovono secondo logiche di filiera, con la conseguenza che il Reg. 899/2023 ripartisce obblighi e responsabilità a carico dei diversi "operatori economici", con questi intendendo il fabbricante, il rappresentante autorizzato, l'importatore, il distributore, il fornitore di servizi di logistica o qualsiasi altra persona fisica o giuridica soggetta a obblighi in relazione alla fabbricazione dei prodotti o alla loro messa a disposizione sul mercato.

E così, i fabbricanti (qualsiasi persona fisica o giuridica che fabbrica un prodotto, oppure lo fa progettare o fabbricare anche a terzi, e lo commercializza apponendovi il proprio nome o marchio, dunque è considerato fabbricante il titolare del marchio apposto sul prodotto o chi lo vende apponendo la propria denominazione commerciale), che potranno agire anche tramite la nomina di un rappresentante autorizzato, hanno il compito fondamentale di garantire la sicurezza dei prodotti fin dalla fase di progettazione. Tra i loro obblighi rientrano l'analisi interna dei rischi, la redazione della documentazione tecnica e l'adozione di misure immediate qualora un prodotto ormai immesso sul mercato si riveli pericoloso. In questi casi, devono informare sia i consumatori che le autorità nazionali, condividere informazioni sugli incidenti e fornire dettagli sulla sicurezza e tracciabilità dei prodotti o del loro imballaggio. Inoltre, devono garantire la presenza di dati di contatto per la gestione dei reclami, registrarli e analizzarli.

Gli importatori (qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato dell'Unione un prodotto originario di un paese terzo), dal canto loro, hanno responsabilità differenti, considerando che i prodotti provengono da paesi extra-UE. Devono assicurarsi che questi rispettino i requisiti di sicurezza generale previsti dal Regolamento, evitando di immettere sul mercato articoli che non soddisfano tali standard. Sono tenuti a fornire i propri dati di contatto sui prodotti, verificare che questi siano accompagnati da istruzioni e informazioni di sicurezza chiare e prendersi cura dei prodotti durante trasporto e conservazione. In caso di prodotti pericolosi, devono informare i fabbricanti e le autorità di vigilanza, garantendo che anche il pubblico venga adeguatamente avvisato.

I distributori (qualsiasi persona fisica o giuridica nella catena di fornitura, diversa dal fabbricante o dall'importatore, che mette a disposizione sul mercato un prodotto), pur avendo obblighi meno stringenti, devono comunque vigilare sul rispetto dei requisiti del Regolamento da parte di fabbricanti e importatori. Anche loro devono evitare di immettere sul mercato prodotti non conformi, segnalare eventuali rischi alle autorità e ai produttori, e assicurarsi che vengano adottate misure adeguate di sicurezza.

Per quanto riguarda i fornitori di mercati online, il Regolamento introduce una serie di obblighi basati sui requisiti del Regolamento sui servizi digitali (sul DSA v. in questa Rubrica la notizia n. 1 sul numero

ISSN 2239-8570

4/2022 [2022/4(1)ST] e in Atlante, p. 245). Tra questi, l'istituzione di due punti di contatto, uno per le autorità di sorveglianza del mercato e uno per il pubblico. Devono implementare processi interni per la sicurezza dei prodotti e garantire che nessun prodotto venga pubblicato senza una garanzia minima di sicurezza e informazioni sulla tracciabilità fornite dall'operatore economico. Inoltre, sono tenuti a effettuare verifiche casuali sulla sicurezza utilizzando banche dati pubbliche, reagire prontamente agli ordini governativi e avvisi di terzi, e impedire che i prodotti ritirati tornino sul mercato. Devono anche fornire informazioni tempestive ai consumatori in caso di richiami, contattando direttamente chi ha acquistato il bene e pubblicando i dettagli sulla propria pagina web.

Infine, tutti gli operatori economici hanno obblighi comuni e trasversali. Devono istituire processi interni per garantire la conformità al Regolamento, collaborare con le autorità di vigilanza per mitigare i rischi legati ai prodotti e conservare informazioni sui rischi, reclami e misure correttive per dieci anni. Devono anche mantenere dati sulla tracciabilità della catena di fornitura per sei anni, informare le autorità su eventuali incidenti causati da un prodotto e, se richiesto, fornire informazioni dettagliate sui prodotti. In caso di richiami, devono avvisare direttamente i consumatori interessati e offrire almeno due soluzioni tra riparazione, sostituzione o rimborso. Infine, per la vendita a distanza, devono fornire informazioni precontrattuali chiare e complete, simili a quelle disponibili in un negozio fisico.

Definito il quadro degli obblighi, particolare attenzione è poi dedicata al profilo dei controlli, il cui scopo è garantire un approccio uniforme ed efficace, per tutelare i consumatori e il mercato interno. Questi sono affidati alle autorità nazionali di vigilanza del mercato, le quali possono svolgere controlli coordinati e simultanei su vasta scala, allo scopo di verificare la conformità dei prodotti alle normative vigenti e prevenire la distribuzione di articoli non sicuri. Laddove fosse identificato un prodotto pericoloso, potranno richiedere ai produttori informazioni dettagliate su altri articoli che condividono lo stesso processo di produzione, componenti o che appartengono allo stesso lotto. La misura consente di prevenire ulteriori rischi e di agire tempestivamente per proteggere la salute pubblica. Al fine di meglio svolgere i loro compiti di vigilanza e controllo, le Autorità possono collaborare con operatori economici, organizzazioni dei consumatori e altre autorità competenti, sia a livello nazionale che internazionale.

Per rafforzare la sicurezza dei prodotti e tutelare i consumatori, anche la Commissione Europea svolge un ruolo strategico, coordinando una rete composta dalle diverse autorità nazionali. Questa ha il compito di agevolare la collaborazione e lo scambio di informazioni tra i vari attori coinvolti. Grazie a questa struttura, le Autorità possono condividere regolarmente esperienze, competenze e migliori pratiche, promuovendo un'applicazione uniforme delle norme in tutti gli Stati membri.

Un aspetto di interesse che riguarda il lavoro della rete è anche l'organizzazione di progetti comuni, che includono attività di sorveglianza sui prodotti e test mirati, i quali permettono di individuare eventuali criticità

ISSN 2239-8570

e intervenire prontamente. Inoltre, la rete facilita il ritiro e il richiamo di prodotti pericolosi dal mercato, migliorando così la sicurezza generale.

Sempre tra le funzioni assegnate alla Commissione volte a garantire l'efficacia del sistema di vigilanza del mercato e garantire una efficace comunicazione e trasmissione delle informazioni, merita soffermarsi sull'introduzione del sistema *Safety Gate,* che sostituisce il precedente Rapex. Esso si articola in tre sottostrutture: in primo luogo, un sistema di allarme rapido sui prodotti pericolosi non alimentari attraverso il quale le autorità nazionali e la Commissione possono scambiare informazioni su tali prodotti (sistema di allarme rapido *Safety Gate*); in secondo luogo, un portale web destinato a informare il pubblico e consentirgli di presentare reclami (portale *Safety Gate*); e, in terzo luogo, un portale web tramite il quale le imprese possono adempiere l'obbligo di avvisare le autorità e i consumatori riguardo a prodotti pericolosi e incidenti (*Safety Business Gateway*). In estrema sintesi, si tratta di un sistema che consente lo scambio rapido di informazioni tra le autorità sui prodotti pericolosi e sulle misure adottate per gestirli; allo stesso tempo, è prevista anche un'area dedicata ai consumatori, ove sono messe a disposizione informazioni gratuite e liberamente accessibili sui rischi identificati. Questo servizio è pensato, da un lato, per agevolare il dialogo tra autorità e operatori economici; dall'altro, per aumentare la consapevolezza dei consumatori e aiutarli a fare scelte informate.

Sotto quest'ultimo profilo, sono previste anche altre azioni per tutelare i consumatori e aumentare l'efficacia dei richiami. Tra queste, gli operatori dovrebbero incentivare e incoraggiare la registrazione dei prodotti acquistati e, nel caso non fosse possibile contattare direttamente tutti i consumatori, i richiami potranno essere pubblicati sul sito web dell'operatore economico, sui social media e mediante affissione nei punti vendita fisici.

Oltre a queste attività, la Commissione collabora con paesi terzi e organizzazioni internazionali per migliorare la sicurezza globale dei prodotti. Gli scambi di informazioni e le iniziative congiunte contribuiscono a creare standard di sicurezza sempre più elevati.

Infine, la Commissione è responsabile dell'elaborazione di relazioni periodiche sull'attuazione del Regolamento, fornendo un quadro chiaro dei progressi compiuti e delle aree di miglioramento. Ha inoltre il compito di adottare atti normativi, sia esecutivi che delegati, per garantire un'applicazione efficace e uniforme delle norme.

Un ultimo cenno meritano le sanzioni qualora, all'esito dei controlli, emergano irregolarità. La loro determinazione è rimessa ai singoli Stati Membri, chiamati ad adottare un sistema sanzionatorio efficace, con misure che siano proporzionate e, allo stesso tempo, dissuasive.

Provando a svolgere alcune preliminari considerazioni di sintesi, l'implementazione del Regolamento (UE) 2023/988, pur essendo una disciplina di prodotto, introduce responsabilità per imprese e autorità di vigilanza, con l'obiettivo di migliorare la sicurezza dei prodotti e la tutela dei consumatori. Le imprese dovranno investire in strumenti per la tracciabilità, test di sicurezza e conformità, mentre le piattaforme online dovranno rafforzare i controlli sui prodotti venduti da terze parti. Le diverse

ISSN 2239-8570

associazioni di categoria non si sono così sottratte dal rilevare le difficoltà che potrebbero incontrare le PMI nell'adeguarsi ai nuovi standard. Non mancano poi le criticità sotto il profilo delle autorità, che dovranno essere dotate di risorse finanziarie e organizzative adeguate a rendere effettiva l'applicazione del Regolamento, evitando che siano immessi sul mercato articoli non sicuri.

Per quanto il Regolamento segni un passo avanti verso un mercato europeo più sicuro e trasparente, offrendo al consumatore una tutela che si muove secondo logiche di stampo precauzionale e preventivo, il successo della sua attuazione dipenderà dalla collaborazione tra imprese, autorità e Stati membri, oltre che dalla capacità di superare le sfide normative e operative.

MARIO MAURO

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32023R0988&qid=1737820021391

2024/4(8)AS

8. Il regolamento (UE) 2024/903 che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile)

Approvato in esito ad un processo avviato con la proposta della Commissione europea COM(2022) 720 final del 18 novembre 2022 (su cui v. in questa Rubrica la notizia n. 10 del numero 4/2022 [2022/4(10)FDA] e in *Atlante*, p. 267), il regolamento (UE) 2024/903 del 13 marzo 2024, pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 22 marzo 2024 (di seguito il **Regolamento**), stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile), definendo norme comuni e un quadro di governance.

Il Regolamento è stato adottato all'interno del più ampio quadro di obiettivi promossi dal programma Europa digitale per il periodo 2021-2027 per favorire la massima digitalizzazione dei servizi pubblici, delle imprese e dei cittadini. In particolare, l'obiettivo perseguito è quello di accelerare il processo di digitalizzazione del settore pubblico con riferimento all'erogazione di servizi pubblici la cui accessibilità, come si dirà, dovrà essere interamente garantita *online* entro il 2030 in tutta Europa. Per raggiungere tale risultato la chiave è indicata nell'**interoperabilità transfrontaliera**, la cui definizione è data dallo stesso Regolamento quale "*... capacità dei soggetti dell'Unione e degli enti pubblici degli Stati membri di interagire tra loro a livello transfrontaliero condividendo dati, informazioni e conoscenze attraverso processi digitali in linea con i requisiti giuridici, organizzativi, semantici e tecnici relativi a tale interazione transfrontaliera"* (articolo 2).

Il Regolamento evidenzia l'importanza dell'interoperabilità transfrontaliera dei sistemi informativi e delle reti utilizzati per gestire e

ISSN 2239-8570

fornire servizi pubblici all'interno del mercato unico, senza barriere a livello europeo. Questo approccio mira a creare in Europa servizi pubblici digitali ed efficaci, fondamentali per il diritto alla libera circolazione di beni, persone, servizi e capitali. Per servizi pubblici digitali transeuropei il Regolamento si riferisce a quei "*...servizi digitali che i soggetti dell'Unione o gli enti pubblici si prestano tra loro o prestano a persone fisiche o giuridiche nell'Unione e che richiedono un'interazione al di fuori delle frontiere dei singoli Stati membri, tra soggetti dell'Unione, o tra soggetti dell'Unione ed enti pubblici, mediante i loro sistemi informativi e di rete*" (considerando §6). Quale esempio il Regolamento porta quei servizi che, attraverso scambi transfrontalieri di dati, consentono il riconoscimento reciproco di titoli accademici e qualifiche professionali; così come gli scambi di dati dei veicoli a fini di sicurezza stradale; l'accesso ai dati sanitari e della sicurezza sociale, compresi i certificati in caso di pandemia e vaccinazione; l'accesso ai sistemi di sportelli unici; lo scambio di informazioni in materia di fiscalità e dogane; l'accreditamento delle gare d'appalto pubbliche; i registri digitali delle patenti di guida o delle imprese e, in generale, tutti i servizi che applicano il principio «una tantum» per l'accesso a dati transfrontalieri e lo scambio di tali dati.

Il Regolamento impone, ai soggetti cui si rivolge (soggetti dell'Unione ed enti pubblici che regolamentano, forniscono, gestiscono o attuano servizi pubblici digitali transeuropei), una **valutazione di interoperabilità** prima di adottare una decisione su requisiti vincolanti, quali l'apposizione di oneri, obblighi e condizioni aventi un effetto sull'interoperabilità transfrontaliera per l'erogazione di servizi pubblici digitali. All'esito della valutazione dell'interoperabilità emergeranno delle **soluzioni di interoperabilità**.

La valutazione dell'interoperabilità dovrà essere redatta alla luce delle soluzioni proposte dalla Commissione mediante l'adozione di un **Quadro europeo di interoperabilità (QEI)** e **quadri di interoperabilità specialistici** (articolo 6). La procedura per l'adozione del Quadro europeo di interoperabilità (QEI) vede il coinvolgimento del Comitato per un'Europa interoperabile quale soggetto dotato di potere di proposta nei confronti della Commissione e, con riferimento ai quadri di interoperabilità specialistici, quale soggetto dotato di potere di vigilanza sul rispetto del Quadro europeo di interoperabilità (QEI). Il Comitato per un'Europa interoperabile rappresenta la struttura di *governance* introdotta dal Regolamento e, oltre a coadiuvare la Commissione nell'ambito del Quadro europeo di interoperabilità (QEI) e dei quadri di interoperabilità specialistici, può formulare raccomandazioni quali "soluzioni per un'Europa interoperabile" (articolo 7).

Il Quadro europeo di interoperabilità (QEI) e quadri di interoperabilità specialistici, così come le "soluzioni per un'Europa interoperabile", sono pubblicati all'interno di un punto di accesso unico: il portale «Europa interoperabile».

Quale ulteriore strumento giuridico per favorire l'interoperabilità transfrontaliera, il Regolamento riconosce al Comitato un potere di proposta per l'individuazione di specifiche misure di sostegno e, tra queste:

ISSN 2239-8570

- l'elaborazione di progetti a sostegno degli enti pubblici nell'attuazione digitale delle politiche dell'Unione che garantiscono l'interoperabilità transfrontaliera dei servizi pubblici digitali transeuropei (articolo 9);
- l'elaborazione di misure di innovazione per sostenere lo sviluppo e l'adozione di soluzioni di interoperabilità innovative nell'Unione (articolo 10) fino all'istituzione di uno spazio di sperimentazione normativa per l'interoperabilità (articolo 11).

Il Regolamento indica anche le strutture di *governance* dell'interoperabilità transfrontaliera. Tra queste, come già osservato, la più rilevante è il Comitato per un'Europa interoperabile, cui sono attribuiti ampi e specifici poteri per l'effettiva applicazione del Regolamento (articolo 15). Per fornire competenze e consulenza al Comitato per un'Europa interoperabile è istituita la comunità per un'Europa interoperabile (articolo 16). Alla comunità per un'Europa interoperabile partecipano i portatori di interessi pubblici e privati, come anche le organizzazioni della società civile e i membri del mondo accademico, previa registrazione sul portale «Europa interoperabile» quali membri.

A livello nazionale dovranno essere designate una o più autorità competenti responsabili ai fini dell'applicazione del Regolamento. Inoltre, tutti i soggetti che forniscono o gestiscono servizi pubblici digitali transeuropei dovranno designare un **coordinatore per l'interoperabilità** che fornisca supporto trasversale nella messa a punto o nell'adeguamento dei processi interni per attuare la valutazione dell'interoperabilità (articolo 18).

La **pianificazione e il monitoraggio degli obiettivi dell'Europa interoperabile** sono rimessi al Comitato ed alla Commissione. Da una parte, con cadenza annuale, il Comitato dovrà adottare l'**Agenda per un'Europa interoperabile** quale strategia di breve periodo per pianificare e coordinare le priorità per lo sviluppo dell'interoperabilità transfrontaliera dei servizi pubblici digitali transeuropei, alla luce, però, delle strategie a lungo termine in materia di digitalizzazione, dei programmi di finanziamento dell'Unione esistenti e dell'attuazione delle politiche dell'Unione in corso (articolo 19). Alla Commissione, invece, è attribuito il monitoraggio dei progressi negli sviluppi dei servizi pubblici digitali transeuropei, anche mediante la redazione di una relazione annuale da presentare al Parlamento europeo e al Consiglio (articolo 20).

AGOSTINO SOLA

https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=OJ:L_202400903

2024/4(9)AA

9. Il regolamento (UE) 2024/1028 relativo alla raccolta e alla condivisione dei dati riguardanti i servizi di locazione di alloggi a breve termine

ISSN 2239-8570

Il regolamento (UE) 2024/1028 del Parlamento europeo e del Consiglio dell'11 aprile 2024, relativo alla raccolta e alla condivisione dei dati riguardanti i servizi di locazione di alloggi a breve termine che modifica il regolamento (UE) 2018/1724 (il **Regolamento**), introduce norme comuni agli Stati membri per la registrazione delle unità immobiliari e per la condivisione dei dati tra le piattaforme online e le autorità pubbliche.

Il Regolamento, che si applicherà a partire dal 20 maggio 2026 (art. 19, comma 2°), si pone una serie di obiettivi: da un lato, quello della tutela del buon funzionamento del mercato interno euro-unitario, in parte assediato dalla proliferazione degli obblighi di registrazione per via degli interventi legislativi e regolamentari degli Stati membri in materia; dall'altro lato, esso si prefigge non solo di garantire la libera circolazione dei servizi (sia del locatore che del fornitore delle piattaforme digitali), ma anche di fornire alle competenti autorità nazionali una cornice giuridica per ottenere dati necessari a definire ed implementare l'intervento statuale nella regolazione dell'autonomia privata, tramite la creazione di una procedura unica di registrazione delle unità immobiliari funzionali alle locazioni cc.dd. "brevi".

Il Regolamento, inoltre, va coordinato con le recenti norme introdotte dal Digital Services Act (regolamento (UE) 2022/2065: **DSA**) e dal Digital Markets Act (regolamento (UE) 2022/1925: **DMA**) e si interseca tra le competenze dell'Unione e degli Stati membri, in quanto il raggio d'azione del legislatore sovranazionale si amplia verso ambiti riservati agli Stati membri, quale quello delle politiche del turismo e non solo.

Le disposizioni del Regolamento sono suddivise in quattro capi: «Disposizioni generali», laddove sono contenute le norme definitorie e quelle relative all'ambito di applicazione dell'atto legislativo (capo I; artt. 1-3); «Registrazione», con le norme – che dovranno essere comuni tra gli Stati membri – concernenti le procedure di registrazione delle unità immobiliari per l'attribuzione del numero di registrazione e i poteri delle autorità pubbliche (capo II; artt. 4-8.); «Comunicazione dei dati», ovvero la parte in cui si ritrovano le norme relative agli obblighi di condivisione dei dati delle piattaforme online nei confronti delle pubbliche autorità (capo III; artt. 9-12); «Informazione, monitoraggio ed esecuzione», che rappresenta il capo relativo all'esecuzione del regolamento e agli obblighi di informazione tra Stati membri e Unione europea (capo IV; artt. 13-15); «Disposizioni finali» (capo V; artt. 16-19).

Cominciando a delineare l'ambito di applicazione della normativa di nuovo conio, l'art. 1 del Regolamento stabilisce che le norme relative alla raccolta e alla condivisione dei dati da parte delle autorità competenti e dei fornitori di piattaforme online riguardano «la prestazione di servizi di locazione di alloggi a breve termine offerti da locatori attraverso piattaforme online di locazione a breve termine». In tal modo, viene identificato precisamente l'oggetto, individuando quali destinatari della procedura di registrazione le unità immobiliari offerte dai locatori attraverso l'intermediazione di fornitori di piattaforme online.

In merito all'ambito di applicazione, l'art. 2 del Regolamento tenta di apportare un riequilibrio nel campo della regolazione delle locazioni

ISSN 2239-8570

"brevi", identificando i destinatari del Regolamento non solo nei locatori di locazioni "a breve termine", ma anche nelle piattaforme online (la cui definizione si ricava in virtù del rinvio operato dall'art. 3, n. 5 del Regolamento all'art. 3, lett. i) del DSA). A tal proposito, si veda l'art. 3, n. 2 del Regolamento: il 'locatore' è definito come «una persona fisica o giuridica che presta, o intende prestare, a titolo professionale, non professionale, su base regolare o temporanea, un servizio di locazione di alloggi a breve termine fornito a fronte di un corrispettivo, attraverso una piattaforma online di locazione a breve termine». La definizione deve raccordarsi con quella di 'unità immobiliare' quale «alloggio ammobiliato situato nell'Unione che è oggetto della prestazione di un servizio di locazione di alloggi a breve termine», che esclude gli alberghi, gli alloggi simili a questi nonché la fornitura di alloggi in aree di campeggio e aree attrezzate per camper e roulotte (art. 3, n. 1, lettere a) e b) del Regolamento, come risulta anche dal Considerando 7 del Regolamento.

Per quanto riguarda le norme di armonizzazione introdotte dal Regolamento, esse mirano a rendere uniformi le procedure di registrazione previste negli Stati membri: l'art. 3, n. 8, del Regolamento definisce 'procedura di registrazione' «qualsiasi procedura mediante la quale i locatori devono fornire informazioni e documentazione specifiche alle autorità competenti al fine di ottenere un numero di registrazione che permetta loro di offrire servizi di locazione di alloggi a breve termine attraverso piattaforme online di locazione a breve termine».

Le norme del Regolamento si applicano laddove lo Stato membro – sia a livello nazionale sia locale – preveda una procedura diretta all'ottenimento, in capo al locatore, di un numero di registrazione dietro presentazione delle informazioni utili all'identificazione dell'unità immobiliare e dell'eventuale documentazione richiesta, per esercitare il servizio regolamentato. L'imposizione, quindi, riguarderebbe la conformità delle procedure eventualmente previste dal diritto nazionale alle nuove regole comuni contenute nel Regolamento, come chiaramente risulta dall'art. 4(1) e (2) del Regolamento. Inoltre, in forza dell'art. 13 del Regolamento, gli Stati membri devono indicare le zone del proprio territorio dove tali procedure trovano applicazione.

L'art. 4(3) del Regolamento sancisce le caratteristiche obbligatorie delle procedure di registrazione: infatti, esso stabilisce che «Gli Stati membri provvedono affinché: a) le procedure di registrazione siano svolte sulla base delle dichiarazioni dei locatori; b) le procedure di registrazione siano disponibili online e gratuitamente, ove possibile, o a un costo ragionevole e proporzionato, e consentano il rilascio automatico e immediato di un numero di registrazione, che non include dati personali, per un'unità specifica al momento della presentazione, da parte del locatore, delle informazioni di cui all'articolo 5(1) del Regolamento, e, se del caso, dell'eventuale documentazione giustificativa richiesta a norma dell'art. 5(2) del Regolamento; c) le procedure di registrazione siano soggette a meccanismi di ricorso efficaci nello Stato membro; d) un'unità non sia soggetta a più di una procedura di registrazione; e) esistano mezzi tecnici che consentono al locatore di aggiornare le informazioni e la

ISSN 2239-8570

documentazione; f) esistano mezzi tecnici per valutare la validità dei numeri di registrazione; g) esistano mezzi tecnici che consentono al locatore di cancellare un'unità dal registro di cui al paragrafo 5; e h) quando offrono i propri servizi di locazione di alloggi a breve termine tramite una piattaforma online di locazione a breve termine, i locatori siano tenuti a dichiarare alla piattaforma online di locazione a breve termine se l'unità offerta è soggetta a una procedura di registrazione e, in caso affermativo, a fornire il numero di registrazione».

Successivamente, il Regolamento si occupa dei poteri di controllo delle autorità pubbliche (art. 6 Regolamento) sulla veridicità delle informazioni che i locatori devono fornire ai sensi dell'art. 5 del Regolamento. In particolare, l'art. 5(1) del Regolamento, stabilisce che il locatore deve presentare una dichiarazione contenente le seguenti informazioni: a) in riferimento all'unità immobiliare, viene richiesta l'indicazione dell'indirizzo (i), il tipo di unità (ii), se essa rappresenta parte o la totalità dell'abitazione principale o secondaria del locatore, il numero massimo di posti letto e di ospiti (iii), se l'unità è soggetta ad un regime di autorizzazione; b) rispetto al locatore persona fisica, viene richiesta l'indicazione del nome (i), il numero di identificazione personale o altre informazioni utili all'identificazione (ii), l'indirizzo (iii), il recapito telefonico (iv), l'indirizzo di posta elettronica (v); c) in riferimento al locatore persona giuridica, viene richiesta l'indicazione del nome (i), del numero nazionale di registrazione dell'attività (ii), del nome del rappresentante legale (iii), della sede legale (iv), del recapito telefonico di almeno un rappresentante (v), dell'indirizzo di posta elettronica (vi).

L'art. 7 del Regolamento, invece, è riferibile alle piattaforme online, le quali devono modificare le proprie interfacce in modo da consentire la "coabitazione" tra il numero di registrazione emanato all'esito della procedura e il proprio "spazio" digitale. In altre parole, il regolamento richiede alle piattaforme che le proprie interfacce permettano: i) ai locatori di autodichiarare se la propria unità si trovi in una zona dove è prevista una procedura di registrazione (art. 7(1)(a) Regolamento); ii) agli utenti di verificare il numero di registrazione e di avere accesso ad annunci relativi ad unità che abbiano già ottenuto validamente un numero di registrazione (art. 7(1)(b) Regolamento); iii) infine, sulle piattaforme grava l'obbligo di compiere «sforzi ragionevoli per verificare in modo casuale e periodicamente le dichiarazioni dei locatori in merito all'eventuale esistenza di una procedura di registrazione», nonché sulla validità del numero affidato (art. 7(1)(c) Regolamento).

L'art. 9 del Regolamento statuisce un obbligo puntuale in capo alle piattaforme online: raccogliere e trasmettere mensilmente «al punto di ingresso digitale unico dello Stato membro in cui è situata l'unità i dati relativi alle attività per ciascuna unità, assieme al numero di registrazione corrispondente fornito dal locatore, all'indirizzo specifico dell'unità e all'URL dell'annuncio». In più, ai sensi dell'art. 10 del Regolamento è obbligo degli Stati membri che abbiano istituito una procedura di registrazione creare «un punto di ingresso digitale unico per la ricezione e la trasmissione dei dati relativi alle attività, del pertinente numero di

ISSN 2239-8570

registrazione, dell'indirizzo specifico dell'unità e degli URL degli annunci forniti dalle piattaforme online di locazione a breve termine a norma dell'art. 9 [del Regolamento]».

D'altro canto, l'obbligo per le piattaforme online di locazione a breve termine di trasmettere i dati relativi alle attività e i numeri di registrazione di cui all'art. 9 del Regolamento necessita di essere letto in combinato disposto con l'art. 12 del Regolamento che definisce i motivi che legittimano le autorità pubbliche a chiedere alle piattaforme la condivisione dei dati. Sul punto, occorre segnalare che queste ultime possono avere accesso a tali dati non solo per controllare il rispetto delle procedure di registrazione di cui all'art. 4 del Regolamento, ma anche al fine di «attuare norme che disciplinano l'accesso a servizi di locazione di alloggi a breve termine e la prestazione di tali servizi e garantirne il rispetto, conformemente al diritto dell'Unione» (art. 12(1)(b) Regolamento).

Quindi, tramite il quadro giuridico introdotto dal Regolamento, le autorità degli Stati membri possono valersi della condivisione dei dati da parte delle piattaforme online anche per potenziare le norme nazionali che disciplinano l'erogazione del servizio delle locazioni "brevi", in modo tale da garantire l'efficacia di quei regimi normativi restrittivi di una delle libertà fondamentali del mercato interno "comunitario", quale la libertà dei servizi.

In conclusione, sembra potersi affermare che l'intima ragione del Regolamento non sia solo quella di preservare il funzionamento del mercato interno, ma anche di dotare le autorità nazionali competenti di un quadro giuridico efficace per controllare e gestire il servizio delle locazioni "brevi" su piattaforma online, alla ricerca di un modello di turismo sostenibile.

Tale affermazione, del resto, è corroborata dalla lettura complessiva dei Considerando. In particolare, il Considerando 1 del Regolamento afferma che il fenomeno in analisi «ha sollevato preoccupazioni e sfide, in particolare per le comunità locali e le autorità pubbliche, ad esempio il loro contributo a una riduzione della disponibilità di alloggi destinati alla locazione a lungo termine e ad un aumento dei canoni di locazione dei prezzi delle abitazioni». E ancora, si sottolinea che la mancanza di informazioni impedisce alle autorità nazionali non solo di valutare l'impatto effettivo di tale fenomeno nel proprio tessuto, economico e sociale, ma anche e conseguentemente di elaborare «risposte politiche adeguate e proporzionate».

Accanto alla conservazione del funzionamento del mercato interno attraverso l'armonizzazione delle norme e dei relativi obblighi in materia di registrazione in capo alle piattaforme online e ai locatori di "affitti brevi", vi è anche l'esigenza di fornire alle autorità nazionali un quadro giuridico favorevole all'elaborazione e all'implementazione delle proprie politiche pubbliche in materia. Nella trama dei Considerando più volte si evidenzia che il regolamento non intende regolare, né tantomeno limitare, le restrizioni o gli oneri imposti sui servizi di locazione "breve" ai sensi della direttiva 2006/123/CE relativa ai servizi nel mercato interno, al fine di garantire la disponibilità di unità immobiliari per locazioni abitative e per favorire un adeguamento naturale dei canoni. Nello specifico, al Considerando 4 del Regolamento viene affermato che esso «non pregiudica

ISSN 2239-8570

la competenza degli Stati membri ad adottare e mantenere requisiti di accesso al mercato per la prestazione di servizi di locazione di alloggi a breve termine da parte dei locatori, compresi requisiti in materia di salute e sicurezza, norme minime di qualità o restrizioni quantitative, purché tali requisiti siano necessari e proporzionati per tutelare obiettivi di interesse generale conformemente alle disposizioni del trattato sul funzionamento dell'Unione europea e della direttiva 2006/123/CE [relativa ai servizi nel mercato interno]», nonché che «[n]el contesto dei servizi di locazione di alloggi a breve termine, la lotta contro la scarsità di alloggi destinati alla locazione è stata riconosciuta dalla Corte di giustizia dell'Unione europea come motivo imperativo di interesse generale, che giustifica l'adozione di misure non discriminatorie e commisurate all'obiettivo perseguito». Ai limiti al servizio degli "affitti brevi", ai sensi della direttiva 2006/123/CE relativa ai servizi nel mercato interno, fanno riferimento anche i Considerando 11 e 12 del Regolamento.

A ciò conseguono le previsioni dell'art. 2(2) lettere (a) e (b) del Regolamento, che, nel precisare il campo di applicazione del provvedimento, statuisce che esso non pregiudica, *inter alia*, «le norme nazionali, regionali o locali che disciplinano l'accesso ai servizi di locazione di alloggi a breve termine o la prestazione di tali servizi da parte dei locatori, conformemente al diritto dell'Unione» (art. 2(2)(a) Regolamento), né «le norme nazionali, regionali o locali che disciplinano lo sviluppo o l'uso delle terre, la pianificazione urbana e rurale, le regolamentazioni edilizie, gli alloggi e le locazioni» (art. 2(2)(b) Regolamento).

ATTILIO ALTIERI

https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:32024R1028

2024/4(10)VH

10. La sentenza della CGUE del 10.9.2024 nel caso *Google Shopping* (C – 48/22 P) e la conferma della condanna alla sanzione di 2,42 miliardi di euro

Il 10 settembre 2024 la Corte di Giustizia dell'Unione Europea (**CGUE** o la **Corte**) ha pronunciato la sentenza nel caso c.d. *Google Shopping* (C – 48/22 P), relativa all'abuso di posizione dominante (art. 102 del Trattato sul funzionamento dell'Unione europea, **TFUE**) posto in essere, secondo la CGUE, da Google nel mercato digitale dei servizi di comparazione dei prezzi. Con questa importante decisione, la Corte, oltre a chiarire o ribadire numerosi principi giuridici relativi all'abuso di posizione dominante e facendo luce sull'interazione tra norme *antitrust* e innovazione tecnologica, ha respinto nel merito il ricorso presentato da Google, affermando nuovamente la responsabilità della stessa e confermando la condanna a una multa per 2,42 miliardi di euro.

ISSN 2239-8570

La vicenda prende le mosse dalla Decisione del 27 giugno 2017 della Commissione europea, adottata ai sensi dell'art. 102 TFUE e dell'art. 54 dell'accordo sullo Spazio Economico Europeo (**SEE**), la quale ritenne che, in tredici Stati dello SEE, Google avesse (illegittimamente) favorito il proprio servizio di comparazione di prodotti sulla propria pagina dei risultati di ricerca generali, a discapito dei servizi di comparazione concorrenti. Ciò che materialmente venne contestato a Google fu il posizionamento dei risultati del proprio comparatore dei prezzi all'interno di appositi *boxes* (riquadri ad alta attrattività visiva e testuale) in primo piano, quando, al contrario, i risultati dei comparatori di prodotti concorrenti erano presentati come un qualsiasi collegamento ipertestuale (i "link blu" che tipicamente compaiono quando si utilizza il motore di ricerca Google), visibili in una posizione inferiore nella pagina e, a causa degli algoritmi di aggiustamento, soggetti a retrocessione rispetto ai risultati del servizio *Google Shopping*.

La Commissione concluse che queste condotte, oltre a costituire un censurabile abuso di posizione dominante nel mercato digitale dei servizi di ricerca specializzata in materia di comparazione dei prezzi, avessero anche un effetto di sviamento del traffico degli utenti per quanto riguarda i diversi motori di ricerca *online*. Conseguentemente, venne inflitta a Google una multa di 2,42 miliardi di euro, con Alphabet, la società madre di Google, ritenuta responsabile in solido per il pagamento di 523 milioni di euro. Successivamente all'impugnazione avverso tale Decisione, il Tribunale dell'Unione europea, con sentenza del 10 novembre 2021, confermò per la maggior parte il provvedimento disposto dalla Commissione, tranne che per il punto della Decisione in cui si rilevava la violazione dell'art. 102 TFUE anche in relazione al mercato della ricerca generale *online*. Il Tribunale ritenne che non fosse stato dimostrato che le condotte di Google avessero avuto effetti anticoncorrenziali, neppure potenziali, nel mercato della ricerca generale *online*, limitandosi a ravvisare l'abuso di posizione dominante nel solo mercato della ricerca specializzata in materia di comparazione dei prezzi. È in questa cornice, a seguito dell'impugnazione presentata da Google LLC e Alphabet Inc. (le **ricorrenti**) avverso la sentenza del Tribunale, che si inserisce la sentenza del 10 settembre 2024 della CGUE.

Con un articolato ragionamento giuridico, la Corte, in corrispondenza delle argomentazioni delle ricorrenti, ha dato un inquadramento, sul piano dei principi applicabili e dell'onere probatorio, alle condotte poste in essere da Google, alle quali si è già accennato: a) la promozione dei risultati di *Google Shopping* (il servizio di comparazione dei prezzi di Google), attraverso un posizionamento privilegiato e una presentazione accattivante; b) la retrocessione dei servizi di comparazione concorrenti, relegati a una minore visibilità.

In primo luogo, la Corte, come già aveva fatto nella statuizione di primo grado il Tribunale, ha ricondotto il comportamento di Google nella cornice del *self-preferencing*, ossia di quell'insieme di pratiche poste in essere da un'impresa volte a favorire i propri prodotti o servizi. Il *self-preferencing* di per sé non vìola l'articolo 102 TFUE. Tuttavia, si può configurare un abuso di posizione dominante se tale pratica incide negativamente sulla concorrenza e sul benessere dei consumatori. Quindi, per accertare una

ISSN 2239-8570

violazione dell'art. 102 TFUE, è necessario un esame, caso per caso, degli effetti dell'insieme di tali condotte sul mercato di riferimento.

Contrariamente a quanto contestato dai ricorrenti, secondo i quali il comportamento di Google doveva essere inscritto nella dinamica della concorrenza basata sui meriti, la Corte ha ritenuto che un effetto anti-concorrenziale, anche solo potenziale, delle condotte *self-preferencing* si fosse prodotto. Nell'operare questo accertamento, la Corte ha chiarito che, ai fini di questo tipo di valutazione, devono essere prese in considerazione le caratteristiche del mercato e le circostanze fattuali rilevanti; in questo caso e segnatamente: a) gli effetti di rete positivi derivanti dall'aumento del traffico verso un determinato servizio di comparazione dei prezzi, nel senso per cui più un servizio di comparazione dei prezzi viene visitato, maggiore è la rilevanza e l'utilità dei suoi servizi e l'inclinazione degli operatori a utilizzarlo; b) il comportamento degli utenti durante la ricerca *online*, considerato che gli utenti si concentrano tipicamente sui primi tre o cinque risultati di ricerca, prestando poca o nessuna attenzione ai risultati rimanenti; c) l'impatto del traffico deviato, cioè la percentuale di traffico deviato dai servizi di comparazione concorrenti. Dunque, nel ragionamento della Corte, non sono le singole condotte (o il loro insieme) isolatamente prese ad essere intrinsecamente abusive, ma sono le singole condotte (o il loro insieme) estrinsecamente considerate; nelle parole della Corte, condotte valutate in relazione a queste "circostanze rilevanti in grado di caratterizzare l'esistenza di pratiche che esulano dall'ambito della concorrenza basata sul merito".

In secondo luogo, la Corte ha escluso che il *thema decidendum* dovesse essere affrontato con gli strumenti della giurisprudenza del caso *Bronner* (CGUE, 26 novembre 1998, C-7/97), in materia di accesso alle c.d. *essential facilities* (o infrastrutture essenziali), come sostenuto dalle ricorrenti. In estrema sintesi, a partire dalla sentenza citata, la giurisprudenza comunitaria aveva ritenuto che un'infrastruttura presentasse i caratteri dell'essenzialità, e che pertanto dovesse essere permesso ai concorrenti l'accesso all'infrastruttura, quando: a) l'infrastruttura è essenziale per lo svolgimento di un'attività da parte del soggetto richiedente; b) l'infrastruttura è insostituibile e materialmente accessibile da parte del richiedente; c) non sussistono obiettive ragioni che giustifichino un rifiuto da parte del soggetto titolare della risorsa. Ora, le ricorrenti asserivano che ai fini di una corretta impostazione e risposta al quesito circa l'illegittimità delle condotte poste in essere da Google (promozione del proprio servizio e retrocessione dei servizi di comparazione concorrenti) si dovesse stabilire se esse potessero essere qualificate o meno come un legittimo rifiuto di fornire l'accesso ai *box* di *Google Shopping* (che in questa chiave di lettura vengono considerati un'infrastruttura essenziale nel mercato digitale dei servizi di comparazione dei prezzi diversa e ulteriore dal motore di ricerca generale *online* di Google); pertanto, la legittimità di tale rifiuto dovesse essere valutata sulla base dei parametri *Bronner* (sopra ricordati).

La Corte ha respinto questa argomentazione, precisando che non vi era alcun rifiuto esplicito di accesso a una infrastruttura essenziale. In più e soprattutto, i *box* di *Google Shopping*, nell'opinione dei giudici europei, non

ISSN 2239-8570

sono da considerarsi una infrastruttura separata dalla piattaforma di ricerca generale *online* di Google, ma semplicemente un formato di visualizzazione all'interno della pagina dei risultati di ricerca, cui i concorrenti avevano comunque accesso. Per questi motivi, la Corte ha ritenuto che, nel caso in esame, i criteri giuridici in materia di *essential facilities* non fossero applicabili, e che le condotte di Google si risolvessero in un abuso di posizione dominante caratterizzato dal trattamento discriminatorio dei concorrenti e dei loro servizi con effetti distorsivi della concorrenza.

In terzo e ultimo luogo, sul piano dello standard probatorio, la Corte ha affermato che, diversamente da quanto sostenuto dalle parti ricorrenti, non fosse necessario applicare il c.d. test AEC (*as efficient competitor)*. Nel ragionamento della CGUE, le pratiche di Google avevano significativamente, e in maniera evidente, catalizzato il flusso di traffico degli utenti verso il proprio servizio di comparazione dei prezzi. In questa tipologia di mercato, la disponibilità di traffico, sempre secondo l'opinione dei giudici europei, è cruciale per l'esistenza dei fornitori di servizi di comparazione dei prezzi, al punto che, ai fini probatori, non è richiesta una modellizzazione dell'operato e dei comportamenti di un'impresa concorrente e altrettanto efficiente per suffragare l'ipotesi di un abuso di posizione dominante. In maniera analoga, la Corte non ha condiviso le prospettazioni dei ricorrenti per quanto riguarda l'analisi controfattuale alla quale sarebbe stata tenuta la Commissione, ossia all'analisi della situazione e degli effetti che comunque si sarebbero prodotti sul mercato anche in assenza delle pratiche contestate. La Corte ha chiarito che, stante un corretto utilizzo di prove alternative, non è necessario ricorrere a un'analisi controfattuale approfondita per vagliare l'esistenza del nesso causale fra le pratiche contestate e gli effetti anti-concorrenziali.

VICTOR HARTL

https://curia.europa.eu/juris/document/document.jsf?text=&docid=289925&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=27933888

2024/4(11)GD

11. La sentenza della CGUE del 19.9.2024 (causa C-264/23) sulle clausole di parità inserite negli accordi conclusi tra Booking.com e i prestatori di servizi alberghieri

Con sentenza del 19 settembre 2024, la Corte di Giustizia dell'Unione Europea (**CGUE**), Seconda Sezione, si è pronunciata nella causa C-264/23 – *Booking.com BV e Booking.com (Deutschland) GmbH contro 25hours Hotel Company Berlin GmbH e altri* – sull'interpretazione dell'articolo 101 del Trattato sul Funzionamento dell'Unione Europea (**TFUE**) e del regolamento (UE) n. 330/2010 della Commissione, del 20 aprile 2010,

ISSN 2239-8570

relativo all'applicazione dell'articolo 101(3) TFUE a categorie di accordi verticali e pratiche concordate (la **Sentenza**).

Il giudizio in questione trae origine da una controversia sorta in Germania tra *Booking.com BV* e *Booking.com (Deutschland) GmbH* (congiuntamente **Booking**) e la *25hours Hotel Company Berlin GmbH* e altre 62 strutture alberghiere situate in Germania in merito alla validità, alla luce dell'art. 101 TFUE, delle clausole di parità della tariffa utilizzate da Booking nei contratti stipulati con tali prestatori di servizi alberghieri.

Giova premettere che, tramite le clausole di parità (anche dette *Most Favored Nation clauses*), i prestatori di servizi alberghieri si impegnano verso le piattaforme di prenotazione a cui sono affiliati a non offrire, sui propri canali diretti o su altre piattaforme, prezzi o altre condizioni per il pernottamento più vantaggiose o favorevoli per il consumatore rispetto a quanto offerto sulle piattaforme a cui sono affiliati.

Inizialmente in Germania tale divieto si applicava tanto all'offerta sui canali di vendita propri degli albergatori, quanto all'offerta su canali di vendita gestiti da terzi (clausola c.d. di "parità ampia").

In particolare, nel 2013 l'Autorità federale garante della concorrenza tedesca (*Bundeskartellamt*) stabilì che la "clausola di parità ampia" utilizzata dalla *Hotel Reservation Service Robert Ragge GmbH* (**HRS**) si poneva in contrasto con il divieto di intese vigente nel diritto dell'Unione Europea e nel diritto tedesco. Sempre nel 2013, l'Autorità federale garante della concorrenza tedesca avviò un'indagine relativa alla clausola utilizzata dalla Booking, analoga a quella della HRS.

Il 9 gennaio 2015, l'*Oberlandesgericht Düsseldorf* (il Tribunale superiore del Land Düsseldorf) respinse il ricorso proposto da HRS avverso la decisione dell'Autorità federale garante della concorrenza tedesca. Una volta passata in giudicato la sentenza del Tribunale superiore del Land Düsseldorf, a luglio 2015, anche Booking si impegnò a rimuovere la clausola di parità ampia dalle sue condizioni generali di contratto e a sostituirla con una c.d. "clausola di parità ristretta", in base alla quale il divieto posto ai fornitori di servizi alberghieri di offrire le loro camere a prezzi migliori di quelli offerti su *Booking.com* si applicava solo alle offerte fatte attraverso i propri canali di vendita.

A febbraio 2023, il Tribunale di Amsterdam, adito da Booking.com con una domanda diretta a far dichiarare la validità delle clausole di parità ristretta, decise di sottoporre alla CGUE due questioni pregiudiziali riguardanti la compatibilità delle clausole di parità, sia ampia che ristretta, rispetto al diritto dell'Unione Europea in materia di concorrenza.

Con la **prima questione**, il giudice del rinvio aveva chiesto se l'articolo 101(1) TFUE dovesse essere interpretato nel senso che le clausole di parità, sia ampia che ristretta, inserite negli accordi conclusi tra le piattaforme di prenotazione alberghiera online (come Booking) e i prestatori di servizi alberghieri esulano dall'applicazione di tale disposizione per il fatto che sarebbero accessorie a detti accordi.

La questione veniva sottoposta in questi termini alla luce della costante giurisprudenza della CGUE (richiamata nella Sentenza) a tenore della quale una pattuizione comportante a prima vista, ove considerata isolatamente,

ISSN 2239-8570

una restrizione della concorrenza in violazione del divieto dell'art. 101(1) TFUE, può nondimeno ritenersi legittima, a certe condizioni, allorquando essa risulti "accessoria" ad una operazione o attività principale che non ricade nell'ambito di applicazione del principio di divieto sancito dall'articolo 101(1) TFUE, per la sua neutralità o per il suo effetto positivo sul piano della concorrenza.

Al riguardo, la CGUE ha preliminarmente ricordato che, affinché una restrizione possa essere qualificata come "accessoria", nel senso e per i sopra riferiti effetti, occorre esaminare ***i)*** se la realizzazione dell'operazione principale sprovvista di tale carattere anticoncorrenziale risulterebbe impossibile in sua assenza, e ***ii***) se del caso, la proporzionalità della restrizione rispetto agli obiettivi soggiacenti all'operazione in questione.

Secondo la CGUE, non è dimostrato che le clausole di parità della tariffa siano oggettivamente necessarie per la realizzazione dell'operazione principale nonché proporzionate rispetto all'obiettivo da essa perseguito. La circostanza che l'assenza delle clausole di parità della tariffa imposte dalla piattaforma di prenotazione alberghiera possa eventualmente produrre conseguenze negative sulla redditività dei servizi offerti da tale piattaforma, infatti, non implica, di per sé, che esse debbano essere considerate oggettivamente necessarie. Il fatto che, eventualmente, tali clausole tendano a contrastare eventuali fenomeni di parassitismo, e siano indispensabili per garantire incrementi di efficienza o per assicurare il successo commerciale dell'operazione principale, inoltre, non consente di qualificarle come "restrizioni accessorie" nell'accezione intesa ai sensi della giurisprudenza in termini della stessa CGUE sull'articolo 101(1) TFUE.

Con la **seconda questione**, il giudice del rinvio aveva chiesto in che maniera occorra, ai fini dell'applicazione dell'articolo 3(1) del Regolamento (UE) n. 330/2010, definire il mercato di prodotti rilevante in una situazione in cui una piattaforma di prenotazione alberghiera funge da intermediario in transazioni concluse tra prestatori di servizi alberghieri e consumatori.

Rispondendo a tale questione, la CGUE ha precisato che, per determinare la quota di mercato detenuta da Booking come fornitore di servizi di intermediazione online ai prestatori di servizi alberghieri ai fini dell'applicazione dell'articolo 3(1) del Regolamento (UE) n. 330/2010 è necessario esaminare se altri tipi di servizi di intermediazione e altri canali di vendita siano sostituibili ai servizi di intermediazione dal punto di vista della domanda, da un lato, da parte dei prestatori di servizi alberghieri, di tali servizi di intermediazione e, dall'altro, da parte dei clienti finali. Al fine di determinare il mercato rilevante, pertanto, il giudice del rinvio deve verificare se esista concretamente una sostituibilità tra i servizi di intermediazione online e gli altri canali di vendita, indipendentemente dal fatto che questi ultimi presentino caratteristiche diverse e non offrano le stesse funzionalità di ricerca e di comparazione delle offerte di servizi alberghieri.

In sintesi, con la sentenza in commento la CGUE ha statuito che:

"**L'articolo 101, paragrafo 1, TFUE** deve essere interpretato nel senso che **le clausole di parità**, sia ampia che ristretta, inserite negli accordi conclusi tra le piattaforme di prenotazione alberghiera online e i prestatori di

ISSN 2239-8570

servizi alberghieri, **non esulano dall'applicazione di tale disposizione per il fatto che sarebbero accessorie a detti accordi**.

L'articolo 3, paragrafo 1, del regolamento (UE) n. 330/2010 della Commissione, del 20 aprile 2010, relativo all'applicazione dell'articolo 101, paragrafo 3, [TFUE] a categorie di accordi verticali e pratiche concordate, deve essere interpretato nel senso che in una situazione in cui una piattaforma di prenotazione alberghiera online funge da intermediario nelle transazioni concluse tra strutture alberghiere e consumatori, **la definizione del mercato rilevante** ai fini dell'applicazione delle soglie delle quote di mercato stabilite in tale disposizione richiede **un esame concreto della sostituibilità, dal punto di vista dell'offerta e della domanda**, tra i servizi di intermediazione online e gli altri canali di vendita".

In Italia, l'Autorità Garante della Concorrenza e del Mercato (**AGCM**) ha avviato nel marzo 2024 una istruttoria nei confronti di Booking (v. in questa Rubrica, notizia n. 15 nel numero 1/2024 [2024/1(15)GD]) per accertare un possibile abuso di posizione dominante nel mercato dei servizi *online* di intermediazione e prenotazione alberghiera offerti dalle Online Travel Agencies (**OTA**) alle strutture ricettive alberghiere e paralberghiere (procedimento A558 – BOOKING/PROGRAMMI OFFERTI ALLE STRUTTURE RICETTIVE ITALIANE E CONCORRENZA TRA LE OTA). Tale istruttoria, ancora in corso, dimostra come anche l'AGCM sia attenta, tra le altre cose, nel valutare condotte ritenute potenzialmente idonee a produrre effetti assimilabili a quelli derivanti da clausole di parità. Non rimane che attendere l'esito dell'istruttoria per scoprire se e in che misura l'AGCM riterrà decisiva la sentenza della CGUE in commento ai fini della valutazione delle condotte di Booking.

GIORGIA DIOTALLEVI

https://curia.europa.eu/juris/document/document.jsf?text=&docid=290211&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=13496355

2024/4(12)MR

12. La sentenza della CGUE del 4.10.2024 nella causa C-621/22 sulla nozione di legittimo interesse nell'ambito di un'attività commerciale

Con la sentenza del 4 ottobre 2024 (causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*), la Corte di giustizia dell'Unione europea (**CGUE** o la **Corte**) è tornata a pronunciarsi sulla controversa nozione di "legittimo interesse", la base giuridica per il trattamento dei dati personali di cui alla lett. *f*) dell'art. 6(1) del regolamento (UE) 2016/679 (**GDPR**).

La domanda di rinvio pregiudiziale alla Corte nasce nell'ambito di una controversia instaurata da una federazione sportiva costituita in forma di associazione nei confronti dell'Autorità per la protezione dei dati dei Paesi

ISSN 2239-8570

Bassi, che aveva inflitto alla ricorrente una sanzione pecuniaria. L'addebito mosso alla federazione consisteva nell'aver comunicato a due *sponsor*, un fornitore di prodotti sportivi ed uno di giochi d'azzardo, alcuni dati personali di propri affiliati (tra gli altri il nome, l'indirizzo, anche di posta elettronica, la data di nascita, il numero di telefono) a fronte (peraltro) di un corrispettivo. In seguito, i dati personali sarebbero stati utilizzati dagli stessi *sponsor* per compiere attività di *marketing* diretto. L'Autorità garante aveva riscontrato la violazione degli artt. 6(1)(a) e (f) GDPR, in combinato disposto con il principio di liceità, correttezza e trasparenza di cui all'art. 5(1)(a) GDPR.

Poiché, pacificamente, era mancato il consenso degli interessati, il titolare aveva invocato altre basi giuridiche. Nel giudizio di impugnazione della sanzione era in particolare sorta la questione, rimessa poi alla CGUE, se l'interesse puramente commerciale, consistente nella cessione a titolo oneroso agli *sponsor* dei dati personali degli interessati, all'ulteriore scopo di utilizzarli per fini di *marketing* diretto, potesse essere considerato un "legittimo interesse". Inoltre, il giudice comunitario è stato chiamato a pronunciarsi sull'ampiezza di tale base giuridica con particolare riferimento alla necessità che l'art. 6(1)(f) GDPR presupponga o meno che l'interesse legittimo sia determinato dalla legge.

Nel quadro così delineato, la Corte ha richiamato il suo costante orientamento in punto di tassatività delle basi giuridiche di cui all'art. 6 GDPR ed ha riaffermato altresì che le basi diverse dal consenso, fondate sul superiore principio di necessità, devono essere interpretate restrittivamente.

Passando poi ad approfondire la nozione di legittimo interesse, la CGUE ha ricordato che esso giustifica il trattamento a patto che quest'ultimo sia strettamente necessario e che i diritti e le libertà fondamentali dell'interessato non prevalgano all'esito di un giudizio di bilanciamento. Facendo riferimento al recente *dictum* di *Schufa Holding* (sentenza del 7 dicembre 2023, C-26/22 e C-64/22, su cui v. in questa Rubrica notizia n. 19 nel numero 4/2023 [2023/4(19)RMo] e in *Atlante*, p. 452) ha poi specificato che un'ampia gamma di interessi può essere considerata legittima e che, come si evince dal Considerando 47 del GDPR (il quale peraltro richiama l'attività di *marketing*), non è necessaria una disposizione di legge che li preveda in modo specifico. La circostanza che non occorra una norma di legge affinché il titolare del trattamento possa invocare la base giuridica in questione non nega, tuttavia, la necessità che lo stesso interesse sia conforme all'ordinamento, né esonera dall'osservanza di regole e principi sanciti dal GDPR quali, in particolare, il principio di minimizzazione dei dati e l'obbligo di fornire l'informativa. Dando continuità alla propria recente giurisprudenza sul tema, e segnatamente alla sentenza resa dalla Grande Sezione il 4 luglio 2023, *Meta Platforms* C-251/21 (su cui v. in questa Rubrica la notizia n. 7 nel numero 3/2023 [2023/3(7)CAT] e in *Atlante*, p. 381) la CGUE ha ribadito che il giudizio di bilanciamento in merito al legittimo interesse da parte del titolare consiste in una ponderazione dei diritti contrapposti alla luce delle circostanze del caso concreto. A tal fine, ha sottolineato la Corte, occorre considerare le aspettative degli interessati e, in particolare, se questi possano o no

ISSN 2239-8570

ragionevolmente attendersi un trattamento come quello effettuato dal titolare in assenza di consenso, tenuto conto del relativo impatto sul diritto al rispetto della vita privata (art. 8 Carta di Nizza, **CDFUE**, e art. 16(1) del Trattato sul funzionamento dell'Unione europea, **TFUE**).

Nel sottolineare il carattere casistico della valutazione circa la sussistenza del legittimo interesse (la cui prova è peraltro a carico del titolare in conformità al principio di *accountability*) la Corte si spinge sino fornire indicazioni specifiche al giudice del rinvio. Alcune considerazioni svolte in quest'ottica meritano di essere richiamate.

In primo luogo, la Corte osserva che nel caso in esame la federazione sportiva potrebbe «informare previamente i suoi membri e chiedere a questi ultimi se desiderano che i loro dati siano trasmessi a tali terzi a fini di pubblicità o di marketing». Prendere in considerazione tale strada sarebbe necessario qualora si valutasse «l'esistenza di mezzi meno lesivi delle libertà e dei diritti fondamentali degli interessati e altrettanto adeguati». Pur comprendendo la logica alla base di tale osservazione, ci si domanda se non si corra il rischio di stabilire il restrittivo orientamento secondo il quale si può invocare la base legale del legittimo interesse solo qualora non sia possibile chiedere il consenso.

L'altra considerazione della Corte che merita attenzione, e nella quale sembra estrinsecarsi un vero e proprio giudizio di merito, attiene al profilo della «relazione tra l'interessato e il titolare del trattamento» che, secondo il Considerando 47 del GDPR deve rivelarsi «pertinente e appropriata» affinché si possa ritenere sussistente un legittimo interesse. Nel caso di specie, tale relazione è stata giudicata mancante in concreto, tenuto conto che i dati personali sono stati comunicati non solo a un fornitore di prodotti sportivi, ma anche ad uno di giochi d'azzardo e da casinò. A tal proposito, la Corte ha evidenziato che l'attività di *marketing* potrebbe avere effetti negativi sui membri delle associazioni di tennis, esponendoli ai rischi connessi allo sviluppo della ludopatia che, peraltro, non sarebbero insiti nella relazione già esistente tra il titolare del trattamento (la federazione sportiva) e gli interessati (gli associati). Considerazione, questa, che scrutina nel profondo la valutazione a suo tempo compiuta dal titolare nella scelta del legittimo interesse quale base del trattamento e che, in prospettiva, presuppone una valutazione sul successivo trattamento a cui i dati personali raccolti dal primo titolare saranno in un secondo momento sottoposti.

Alla luce delle argomentazioni esposte, la Corte ha dunque concluso che «un trattamento di dati personali consistente nella comunicazione a titolo oneroso di dati personali dei membri di una federazione sportiva, al fine di soddisfare un interesse commerciale del titolare del trattamento, può essere considerato necessario ai fini del legittimo interesse perseguito da tale titolare, ai sensi di detta disposizione, solo a condizione che tale trattamento sia strettamente necessario alla realizzazione del legittimo interesse in questione e che, alla luce di tutte le circostanze pertinenti, non prevalgano su tale legittimo interesse gli interessi o le libertà e i diritti fondamentali dei suddetti membri. Sebbene detta disposizione non esiga che un interesse siffatto sia determinato dalla legge, essa richiede che il legittimo interesse invocato sia lecito».

ISSN 2239-8570

Sul tema del legittimo interesse si deve infine segnalare che sono in corso di elaborazione presso l'EDPB le relative linee guida, la cui prima versione è stata adottata l'8 ottobre 2024 (su cui v. *infra* in questo numero della Rubrica, la notizia n. 22 [2024/4(22)SB]). Mentre si attende la versione finale del documento, a seguito della chiusura della consultazione pubblica (20 novembre 2024), si può sin d'ora rilevare come le Linee guida richiamino in più punti la decisione in commento (si vedano i parr. 17, 46, 50, 121 già dalla versione 1.0, disponibile all'indirizzo https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en). In particolare, si evidenzia proprio il par. 46 delle predette linee guida, ove è previsto che il titolare che intenda basare il trattamento sul legittimo interesse debba considerare gli effetti avversi puntualmente prevedibili («*adverse outcomes that can be specifically foreseen*»). Ogniqualvolta, dunque, si comunichino dati personali a terzi, occorrerà non solo svolgere le valutazioni del caso alla luce del trattamento la cui base sia proprio il legittimo interesse, ma dovrà altresì essere valutato l'impatto dell'ulteriore trattamento effettuato dai destinatari dei dati personali.

MATILDE RATTI

https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62022CJ0621

2024/4(13)DI

13. Pratiche sleali e dati relativi alla salute: la sentenza della CGUE del 4.10.2024 nella causa C-21/23 *Lindenapotheke* (caso dei farmacisti tedeschi)

Il 4 ottobre 2024 la Grande Sezione della Corte di Giustizia dell'Unione Europea (**CGUE**) ha adottato una decisione (*Lindenapotheke*, C-21/23) sulle tutele contro la violazione del regolamento (UE) 2016/679 (**GDPR**) e sulla nozione di «dati relativi alla salute» come lì offerta: "i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute" (art. 4, n. 15 GDPR).

La decisione della CGUE origina da un rinvio pregiudiziale presentato dal *Bundesgerichtshof*, dinnanzi al quale si discuteva il ricorso contro la decisione del giudice di appello (*Oberlandesgericht Naumburg*) che aveva confermato l'accoglimento da parte del giudice di primo grado (*Landgericht Dessau-Roßla*) di una domanda inibitoria, presentata in base alla disciplina tedesca sulle pratiche commerciali scorrette (*Gesetz gegen den unlauteren Wettbewerb* (**UWG**)), da un farmacista contro un concorrente, il quale commercializzava medicinali online. Nella fase di vendita di questi prodotti sulla piattaforma *Amazon-Marketplace*, il concorrente domandava agli acquirenti il loro nome, l'indirizzo di consegna e gli elementi necessari

ISSN 2239-8570

all'individualizzazione dei medicinali. La raccolta di queste informazioni dei clienti avveniva senza avere prima ottenuto il loro consenso al relativo trattamento, come invece richiesto dalla normativa in materia di dati sanitari (art. 9.2.*a*, GDPR). Il farmacista – in nessun modo riconducibile agli acquirenti/interessati del trattamento dei dati sanitari così illecitamente raccolti e trattati – lamentava che questa violazione del GDPR integrasse l'art. 3a, UWG per cui commette un atto sleale colui il quale violi una disposizione di legge che sia altresì destinata a disciplinare il comportamento sul mercato nell'interesse dei soggetti partecipanti al mercato stesso, nel caso in cui la violazione sia idonea a pregiudicare in maniera sensibile gli interessi dei consumatori, di altri soggetti partecipanti al mercato o dei concorrenti.

Di conseguenza, chiedeva la concessione del provvedimento inibitorio previsto dalla legge per tale ipotesi (art. 8, UWG).

Giunto il procedimento dinnanzi al *Bundesgerichtshof*, questi ha rimesso alla CGUE la questione concernente *i*) la possibilità di far cessare, mediante un ricorso dinanzi a un giudice civile e sulla base del divieto delle pratiche commerciali sleali, violazioni delle disposizioni del GDPR; *ii*) la possibilità di qualificare le informazione che i clienti devono inserire nella piattaforma di vendita online, al momento dell'ordine di medicinali, quali il loro nome, l'indirizzo di consegna e le informazioni necessarie all'individualizzazione dei medicinali ordinati, come «dati relativi alla salute».

Rispetto alla questione *i*), la CGUE ha affermato che il GDPR non osta a che gli Stati membri prevedano, nel diritto nazionale, la possibilità di contestare una presunta violazione delle disposizioni sostanziali di detto regolamento in base alla disciplina sulle pratiche commerciali sleali.

Innanzitutto, la CGUE ha rilevato come il capo VIII del GDPR non escluda agli Stati membri di prevedere la possibilità per i concorrenti di una impresa che abbia violato quel regolamento di presentare un'azione inibitoria sulla base del divieto delle pratiche commerciali sleali. In secondo luogo, la CGUE ha riconosciuto che una simile possibilità sia compatibile con gli obiettivi perseguiti dal GDPR. In particolare, l'azione inibitoria ex artt. 3 e 8, UWG non pregiudica il sistema dei mezzi di ricorso previsto dal GDPR, che sono pienamente preservati e che possono sempre essere esercitati dagli interessati, nonché, se del caso, dalle associazioni che rappresentano tali persone. Questa coesistenza di mezzi di ricorso ai sensi del diritto della protezione dei dati e del diritto nazionale sulle pratiche commerciali non crea rischi per l'applicazione uniforme del GDPR, ma, anzi contribuisce incontestabilmente al rispetto di tali disposizioni e, quindi, a rafforzare i diritti degli interessati e ad assicurare loro un elevato livello di protezione. Sul punto, la CGUE ha osservato come un'azione inibitoria di questo tipo da parte di un concorrente possa rivelarsi particolarmente efficace, al pari di quella delle associazioni per la tutela degli interessi dei consumatori, al fine di garantire siffatta tutela, in quanto è idonea a prevenire un gran numero di violazioni dei diritti delle persone interessate dal trattamento dei loro dati personali.

Quanto alla questione *ii*), la CGUE ha dichiarato che le informazioni che un cliente inserisce su una piattaforma online al momento dell'ordine di

ISSN 2239-8570

medicinali la cui vendita è riservata alle farmacie rientrano nella nozione di «dati relativi alla salute». Secondo la CGUE, il nome del cliente, l'indirizzo di consegna e le informazioni necessarie all'individualizzazione dei medicinali ordinati sono dati idonei a rivelare, mediante una semplice operazione intellettuale di raffronto o di deduzione, informazioni sullo stato di salute dell'interessato, in quanto tale ordine implica la creazione di un nesso tra un medicinale, le sue indicazioni terapeutiche o i suoi usi, e una persona fisica identificata o identificabile da elementi quali il nome di tale persona o l'indirizzo di consegna.

A tal proposito, la CGUE ha esaminato anche l'argomento contrario, che fa leva sul fatto che la vendita dei medicinali ordinati possa non essere soggetta a prescrizione medica e che quindi i medicinali acquistati sulla piattaforma *Amazon-Marketplace* dal cliente che procede all'ordine potrebbero essere destinati a terzi. Tale argomentazione viene respinta: la CGUE ha concluso che le informazioni che i clienti immettono quando ordinano online medicinali la cui vendita è riservata alle farmacie senza essere soggetta a prescrizione medica costituiscono dati relativi alla salute, anche se è solo con una certa probabilità, e non con assoluta certezza, che tali medicinali siano destinati a tali clienti. Per un verso, secondo la CGUE un'interpretazione che porti a distinguere in base al tipo di medicinale in questione e al fatto che la sua vendita sia o meno soggetta a prescrizione medica non sarebbe coerente con l'obiettivo di un elevato livello di protezione delle libertà e dei diritti fondamentali delle persone fisiche, in particolare della loro vita privata, rispetto al trattamento dei dati personali che le riguardano. Per altro verso, la CGUE ha aggiunto che non si possa escludere che, anche nell'ipotesi in cui simili medicinali siano destinati a persone diverse dai clienti, sia possibile identificare tali persone e trarre conclusioni sul loro stato di salute (tutte attività che richiedono il consenso dell'interessato o altra base prevista dall'art. 9.2, GDPR).

DANIELE IMBRUGLIA

https://tinyurl.com/yckbuedk

2024/4(14)RA

14. La sentenza della CGUE del 14.11.2024 nella causa C-646/22 sulla nozione di consumatore medio e sulle distorsioni cognitive

Con la sentenza in commento, la Corte di Giustizia dell'Unione europea (**CGUE**) è tornata a chiarire le nozioni di *consumatore medio* e di *pratica commerciale aggressiva*, rilevanti ai sensi della direttiva 2005/29/CE sulle pratiche commerciali sleali (**UCPD**).

La pronuncia trae origine dalla pratica posta in essere da Compass Banca S.p.A. (**Compass** o **Banca**), tra il gennaio 2015 e il luglio 2018. Segnatamente, in tale periodo di tempo, la Banca ha proposto ai propri clienti di sottoscrivere – contestualmente alla stipula di un finanziamento

ISSN 2239-8570

personale – una polizza assicurativa a copertura di determinati rischi non (del tutto) collegati al finanziamento sottoscritto, senza specificare che tale sottoscrizione era, a dire il vero, meramente facoltativa. In altri termini, pur non essendo la sottoscrizione di una polizza assicurativa un presupposto necessario per la concessione del finanziamento personale, essa è stata comunque proposta da Compass ai propri clienti in (un solo apparentemente necessario) abbinamento con il finanziamento concesso.

Nel settembre 2018, l'Autorità Garante della Concorrenza e del Mercato (**AGCM** o **Autorità**) ha avviato un procedimento nei confronti di Compass, al fine di accertare se la pratica posta in essere dalla Banca potesse reputarsi *sleale* ai sensi della UCPD. Nel corso di tale procedimento, Compass ha presentato una proposta di impegni – finalizzati a chiarire al consumatore la *non obbligatorietà* della sottoscrizione della polizza – che comprendeva la previsione di un diritto del consumatore di recedere dal contratto di assicurazione, senza tuttavia perdere il finanziamento. La Banca non ha tuttavia accettato di impegnarsi, come invece richiesto dall'Autorità, a prevedere in favore dei propri clienti pure un periodo di riflessione di sette giorni tra la data di sottoscrizione del contratto di finanziamento e quella di sottoscrizione del contratto assicurativo.

L'AGCM ha dunque, dapprima, respinto gli impegni proposti da Compass e, poi, con decisione del 27 novembre 2019 (comunicata il successivo 23 dicembre 2019), constatato che la Banca aveva posto in essere una *pratica commerciale aggressiva* (e, quindi, *sleale* ai sensi della UCPD), consistente nell'abbinamento forzoso, al momento della stipula dei contratti di finanziamento personale, di prodotti assicurativi non collegati al credito. Di conseguenza, l'Autorità ha vietato la continuazione di detta pratica, irrogando altresì una sanzione pecuniaria di importo pari a oltre 4 milioni di Euro.

Compass ha proposto ricorso avverso la decisione dell'AGCM dinnanzi al Tribunale Amministrativo Regionale per il Lazio (Sezione Prima), il quale lo ha respinto con sentenza n. 9516/2021. Avverso quest'ultima pronuncia, la Banca ha adìto il Consiglio di Stato (Sezione Sesta), che, con ordinanza del 10 ottobre 2022, ha sospeso il procedimento di appello, rimettendo alla CGUE talune questioni pregiudiziali, che hanno sollecitato la decisione in commento.

In particolare, il Consiglio di Stato ha operato un rinvio pregiudiziale in relazione alle seguenti questioni:

> 1) "*Se la nozione di consumatore medio di cui alla direttiva* [2005/29/CE] *inteso come consumatore normalmente informato e ragionevolmente attento ed avveduto – per la sua elasticità ed indeterminatezza – non debba essere formulata con riferimento alla miglior scienza ed esperienza e di conseguenza rimandi non solo alla nozione classica dell'homo oeconomicus ma anche alle acquisizioni delle* [teorie] *sulla razionalità limitata che hanno dimostrato come le persone agiscono spesso riducendo le informazioni necessarie con decisioni "irragionevoli" se parametrate a quelle che sarebbero prese da un soggetto ipoteticamente attento ed avveduto*[,] *acquisizioni che impongono*

ISSN 2239-8570

una esigenza protettiva maggiore dei consumatori nel caso – sempre più ricorrente nelle moderne dinamiche di mercato – di pericolo di condizionamenti cognitivi";

2) "*Se possa essere considerata di per sé aggressiva una pratica commerciale nella quale, a causa dell'incorniciamento delle informazioni (framing)*[,] *una scelta possa apparire come obbligata e senza alternative tenendo conto dell'articolo 6, paragrafo 1, della direttiva [2005/29/CE] che considera ingannevole una pratica commerciale che in qualsiasi modo inganni o possa ingannare il consumatore medio "anche nella sua presentazione complessiva*";

3) "*Se la direttiva* [2005/29/CE] *giustifichi il potere dell'[AGCM] (una volta rilevato il pericolo di condizionamento psicologico legato*[, in primo luogo,] *allo stato di bisogno in cui normalmente versa chi chiede un finanziamento,* [in secondo luogo,] *alla complessità dei contratti sottoposti alla firma del consumatore,* [in terzo luogo,] *alla contestualità dell'offerta presentata in abbinamento,* [in quarto luogo,] *alla brevità dei tempi concessi per la sottoscrizione dell'offerta), di prevedere una deroga al principio della possibilità di abbinamento tra vendita di prodotti assicurativi e vendita di prodotti finanziari non connessi imponendo uno spazio temporale di 7 giorni tra le firme dei due contratti*";

4) "*Se, in relazione a tale potere repressivo delle pratiche commerciali aggressive, la direttiva* [(UE)2016/97 sulla distribuzione assicurativa], *ed in specie l'articolo 24*[,] *paragrafo 3 della stessa, osti all'adozione di un provvedimento dell'*[AGCM] *adottato sulla base degli articoli 2, lettere d) e j), 4, 8 e 9 della direttiva* [2005/29/CE] *e della normativa nazionale di recepimento* […] *dopo il rigetto di una istanza di impegni a seguito del rifiuto di una società di servizi di investimento, nel caso di vendita abbinata di un prodotto finanziario ed un prodotto assicurativo non connesso al primo – ed in presenza di un pericolo di condizionamento del consumatore legato alle circostanze del caso concreto desumibili anche dalla complessità della documentazione da esaminare – di concedere al consumatore uno spatium deliberandi di 7 giorni fra la formulazione della proposta abbinata e la sottoscrizione del contratto assicurativo*";

5) "*Se il considerare pratica aggressiva il mero abbinamento di due prodotti finanziari e assicurativi potrebbe finire per risolversi in un atto di regolazione non consentito e non finirebbe per addossare sul professionista (e non sull'AGCM, come dovrebbe essere) l'onere (difficile da assolvere) di dimostrare che non si tratta di pratica aggressiva in violazione della direttiva* [2005/29/CE] *(tanto più che la direttiva citata non consente agli Stati membri di adottare misure più restrittive di quelle da essa definite, neppure al fine di assicurare un livello superiore di tutela dei consumatori) o se invece tale inversione dell'onere della prova non sussista purché, sulla base di elementi oggettivi, sia ritenuto il concreto pericolo di un*

ISSN 2239-8570

condizionamento del consumatore bisognoso di ottenere un finanziamento a fronte di una offerta abbinata complessa".

La risposta alla *prima questione* ha consentito alla CGUE di chiarire la (sempre più ricorrente) questione concernente l'interpretazione della nozione di *consumatore medio* ai sensi della UCPD e, in particolare, se tale nozione vada intesa non solo con riferimento a un consumatore normalmente informato e ragionevolmente attento ed avveduto, ma pure tenendo conto del fatto che la capacità decisionale di un individuo è falsata da limitazioni, quali le distorsioni cognitive. Invero, le ricerche (neuro-)scientifiche hanno dimostrato, ormai in maniera costante a partire dalla seconda metà dello scorso secolo, come il ragionamento umano devii sistematicamente dalle predizioni della logica classica, della teoria della probabilità e, soprattutto, della scelta razionale.

Ebbene, la CGUE – procedendo dal Considerando 18 della UCPD, secondo il quale il consumatore medio è quello "*normalmente informato e ragionevolmente attento ed avveduto, tenendo conto di fattori sociali, culturali e linguistici*" – ha sottolineato che "*tale nozione non è statica*", giacché essa va interpretata, sempre secondo il medesimo Considerando 18, in maniera conforme alla giurisprudenza della CGUE. E proprio la CGUE ha già rilevato che un consumatore medio può essere indotto in errore, in modo tale da non riuscire a effettuare le proprie scelte commerciali in maniera consapevole ed efficiente (v., in tal senso, sentenza CGUE del 19 dicembre 2013, caso Trento Sviluppo c. Centrale Adriatica, C-281/12). Pertanto, anche alla luce dei risultati degli studi neuro-scientifici, non può dubitarsi che la caratteristica consistente nell'essere "*normalmente informato*" debba essere intesa "*come riferita alle informazioni che si possono ragionevolmente presumere note ad ogni consumatore, tenendo conto dei pertinenti fattori sociali, culturali e linguistici*", pertanto essa "*non esclude che una pratica commerciale possa falsare in misura rilevante il comportamento di tale consumatore virtuale a causa di una carenza informativa di quest'ultimo*". Del pari, "*il fatto che la nozione di «consumatore medio» debba essere intesa con riferimento a un consumatore «ragionevolmente attento ed avveduto» non esclude la presa in considerazione dell'influenza di distorsioni cognitive su tale consumatore medio, purché sia dimostrato che tali distorsioni possano colpire una persona normalmente informata nonché ragionevolmente attenta ed avveduta, e ciò in misura tale che il suo comportamento ne risulterebbe falsato in misura rilevante*".

In altre parole, la capacità decisionale di un consumatore (medio) può senz'altro "*essere falsata da un insieme di limitazioni, come le distorsioni cognitive*". Tuttavia, occorrerà di volta in volta dimostrare che, "*nelle specifiche circostanze di una situazione concreta, una siffatta pratica sia tale da incidere sul consenso di una persona normalmente informata nonché ragionevolmente attenta ed avveduta, e ciò in misura tale che il suo comportamento ne sarebbe falsato in misura rilevante*", spettando "*agli organi giurisdizionali nazionali determinare la reazione tipica del consumatore medio in una determinata situazione*".

ISSN 2239-8570

Con la risposta alla *seconda questione*, invece, la CGUE ha chiarito se una pratica commerciale di c.d. *framing* (quale è quella posta in essere da Compass) possa essere considerata *in ogni caso aggressiva* e, quindi, *in ogni caso sleale* ai sensi della UCPD. Sul punto, la Corte ha ribadito il principio secondo cui – ai sensi dell'art. 8 della UCPD – una pratica è da considerarsi aggressiva solamente quando, mediante molestie, coercizione o indebito condizionamento, limiti o sia idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore medio, e pertanto lo induca o sia idonea a indurlo ad assumere una decisione di natura commerciale che altrimenti egli non avrebbe preso.

Escluse le ipotesi di comportamenti molesti o coercitivi insiti nel *framing*, la CGUE ha espunto anche la possibilità di ricondurre tale condotta a un indebito condizionamento, il quale – ai sensi dell'art. 2, lett. j) della UCPD – consiste propriamente nello sfruttamento di una posizione di potere nei confronti del consumatore al fine di esercitare una pressione, anche senza il ricorso alla forza fisica o la minaccia di tale ricorso, in modo da limitare notevolmente la capacità del consumatore di prendere una decisione consapevole. Invero, secondo la CGUE, "*una prassi consistente nel presentare simultaneamente ad un consumatore un'offerta di finanziamento personale e un'offerta di un prodotto assicurativo non collegato a tale finanziamento, senza che gli venga lasciato un periodo di riflessione* […] *non implica, di per sé, l'esistenza di atti di pressione*" idonei a configurare un indebito condizionamento e, dunque, una pratica commerciale aggressiva.

Pertanto, pur escludendo che la pratica commerciale di *framing* costituisca *di per sé* una *pratica commerciale aggressiva* (o, comunque, *in ogni caso sleale*), la Corte ha precisato che il giudice del rinvio dovrà comunque accertare se, *in concreto*, la Banca abbia fatto ricorso a molestie, coercizione o indebito condizionamento ovvero se, pure in assenza di tali condotte, la pratica commerciale realizzata da Compass sia comunque, *in concreto*, *sleale* e, in particolare, riconducibile alla diversa *species* delle *pratiche commerciali ingannevoli*. Occorrerà dunque che il giudice del rinvio – qualora accerti che la condotta posta in essere dalla Banca non presenti i caratteri di una pratica commerciale aggressiva – verifichi se essa abbia ciononostante ingannato (o, comunque, fosse idonea a ingannare) il consumatore medio (nel senso sopra chiarito), facendogli credere che non fosse possibile ottenere il finanziamento senza sottoscrivere un prodotto assicurativo. Per tale ragione, la CGUE ha restituito al mittente anche la *quinta questione* sottoposta al rinvio pregiudiziale.

Con la risposta alla *terza questione*, poi, la CGUE ha dichiarato che la UCPD va interpretata nel senso che un'Autorità nazionale – una volta accertato il carattere *aggressivo* o, comunque, *sleale* di una pratica commerciale – può imporre a un professionista di concedere al consumatore un periodo di riflessione ragionevole tra le date della sottoscrizione del contratto di assicurazione e del contratto di finanziamento, a meno che non esistano altri mezzi meno lesivi della libertà d'impresa che risultino altrettanto efficaci per porre fine al carattere *aggressivo* o, più in generale, *sleale* di detta pratica.

ISSN 2239-8570

E, come si legge nella risposta alla *quarta questione*, all'imposizione di tale misura non osta, nel caso di specie, l'art. 24, paragrafo 3 della direttiva (UE) 2016/97 sulla distribuzione assicurativa, ai sensi del quale se un prodotto assicurativo è accessorio rispetto a un bene o a un servizio diverso da un'assicurazione, il distributore dei prodotti assicurativi deve offrire al cliente la possibilità di acquistare il prodotto o il servizio separatamente.

RICCARDO ALFONSI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62022CJ0646

2024/4(15)RDO

15. La sentenza della CGUE del 15.1.2024 nella causa C-33/22 sull'applicabilità del GDPR agli atti dei parlamenti nazionali e i regolamenti del Parlamento italiano in materia di "diritto all'oblio"

Con la sentenza C-33/22 del 16 gennaio 2024 (la **Sentenza**), la Corte di giustizia dell'UE (di seguito **CGUE** o **Corte**) ha affrontato, nella sua composizione più autorevole (Grande Camera), il tema dell'applicazione delle disposizioni del regolamento UE 2016/679 (**GDPR**) ai trattamenti di dati personali effettuati da organi dei parlamenti nazionali degli Stati membri.

Pronunciata dalla Corte sulla questione pregiudiziale posta dal *Verwaltunsgerichshof* austriaco nel caso *Österreichische Datenschutzbehörde* c. *WK* (con intervento del presidente della Camera bassa del Parlamento austriaco), la sentenza fissa alcuni punti fermi in merito al dibattuto problema se le attività dei parlamenti nazionali rientrino nella portata applicativa del diritto dell'Unione - e quindi del GDPR – oppure ne siano escluse, trattandosi di materia riservata all'esclusiva competenza degli Stati membri.

La controversia oggetto del procedimento principale è sorta dalle misure adottate dall'Autorità austriaca di protezione dei dati (*Datenschutzbehörde*) in merito agli atti di una commissione di inchiesta parlamentare, insediata nel 2018 da una camera del parlamento (*Nationalrat*) allo scopo di acquisire elementi di conoscenza in relazione a fenomeni criminosi rilevanti per la sicurezza nazionale (nella specie, si trattava dell'infiltrazione di elementi estremisti all'interno dell'Ufficio federale per la protezione della Costituzione e l'Antiterrorismo, il *Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*). Nel corso dei suoi lavori la commissione aveva ascoltato un testimone (un funzionario di polizia sotto copertura) in una pubblica audizione, il cui verbale veniva pubblicato sul sito istituzionale del Parlamento senza provvedere ad anonimizzare i dati dell'audito malgrado questo ne avesse fatto esplicita richiesta.

ISSN 2239-8570

L'interessato ha proposto reclamo al *Datenschutzbehörde*, asserendo violato il suo diritto fondamentale alla protezione dei dati - tutelato dall' art. 1 GDPR - in conseguenza della pubblicazione del resoconto dell'audizione con modalità tali da rivelare la sua identità senza il suo consenso. L'Autorità ha adottato nel 2019 una decisione di rigetto, dichiarandosi incompetente sulla base del principio costituzionale di separazione dei poteri, che preclude all'Esecutivo, nella cui sfera essa si incardina nell'ordinamento austriaco, di esercitare il proprio sindacato sull'attività del Legislativo, di cui è espressione la commissione parlamentare d'inchiesta.

L'interessato ha quindi adito il Tribunale amministrativo federale (*Bundesverwaltungsgericht*), che nel 2020 ne ha accolto il ricorso rilevando l'applicabilità del GDPR all'attività parlamentare considerata. A seguito dell'impugnazione dell'Autorità di protezione dei dati dinanzi al *Verwaltunsgerichshof*, questa Corte ha posto la questione pregiudiziale ora decisa dalla CGUE.

Il giudice del rinvio ha sottoposto alla CGUE tre questioni. La prima verte sull'ambito di applicazione del diritto dell'Unione ai sensi dell'art, 16 del Trattato sul funzionamento dell'Unione europea (**TFUE**) e pone il quesito se vi siano incluse le attività di una commissione di inchiesta istituita dal Parlamento di uno Stato membro in esercizio del suo potere di controllo sull'Esecutivo, con la conseguenza che il trattamento di dati personali effettuato da tale commissione sarebbe disciplinato dal GDPR. La seconda questione si collega alla risposta affermativa data al primo quesito: una volta appurata l'applicazione del GDPR alle attività di trattamento di dati personali poste in essere da una commissione parlamentare di inchiesta, si è chiesto se dette attività, in quanto riferite allo svolgimento di funzioni di polizia e dunque a materie di rilievo per la sicurezza nazionale, non ricadano – ai sensi del Considerando 16 del GDPR – negli ambiti esclusi dall'applicazione della disciplina di protezione dei dati (*ex* art. 2, lett. *a*, GDPR). La terza questione (relativa all'interpretazione dell'art. 51 GDPR) è stata formulata dal giudice del rinvio in relazione all'eventuale risposta negativa data al secondo quesito, e riguarda la competenza dell'Autorità nazionale di controllo ad esaminare i reclami di soggetti interessati avverso il trattamento dei propri dati personali da commissioni parlamentari di inchiesta, nel caso in cui in uno Stato membro sia stata istituita un'unica Autorità (come in Austria ed anche in Italia).

Investita della questione, la Corte ha fatto proprie le argomentazioni svolte nelle conclusioni dell'Avvocato generale Szpunar presentate l'11 maggio 2023, e ha sostenuto l'applicabilità alle attività parlamentari del diritto alla protezione dei dati.

Essa ha affermato, in primo luogo, che tanto il TFUE (art. 16, par. 2, prima frase) quanto il GDPR (art. 2, par. 2, lett. *a*) non devono essere interpretati nel senso di escludere una determinata attività dall'ambito di applicazione del diritto dell'Unione - e pertanto del GDPR - per il solo motivo che essa è esercitata da una commissione di inchiesta istituita dal Parlamento di uno Stato membro nell'esercizio del suo potere di controllo del potere esecutivo. In secondo luogo, la corretta interpretazione della predetta disposizione del GDPR non consente di considerare le attività di

ISSN 2239-8570

una commissione parlamentare di inchiesta di uno Stato membro, seppure finalizzate ad indagare sull'operato degli organi di polizia e dunque a sindacare l'azione del Governo in ambiti particolari, come di per sé riguardanti la sicurezza nazionale. Infine, la Corte ha fatto leva sui caratteri di obbligatorietà e diretta applicabilità della fonte regolamentare (*ex* art. 288 TFUE) per affermare che le previsioni del GDPR sul diritto di proporre reclamo ad un'autorità di controllo (art. 77, par. 1) e sulla competenza di tali autorità (art. 55, par. 1) devono intendersi nel senso che a queste ultime è direttamente conferita la competenza a conoscere dei reclami relativi a trattamenti di dati personali effettuati da commissioni parlamentari d'inchiesta, anche quando lo Stato membro, nell'istituire una o più autorità di controllo (*ex* art. 51 GDPR), non abbia espressamente previsto tale compito. Il rilievo della Corte ben si comprende ove si consideri che la facoltà rimessa dal GDPR agli Stati di istituire più di una autorità, pur preordinata al rispetto della struttura costituzionale e amministrativa degli Stati membri (come precisato dal Considerando 117 del regolamento), risponde all'esigenza di assicurare, per questa via, l'effettivo primato del diritto dell'Unione anche rispetto alle fonti normative di rango costituzionale vigenti negli ordinamenti degli Stati membri.

In altre parole, secondo la CGUE non vi sono attività da considerare escluse dall'ambito di applicazione materiale del diritto dell'Unione - e per quanto rilevi, del GDPR – in ragione del solo fatto che esse sono esercitate da una commissione di inchiesta istituita dal Parlamento di uno Stato membro; l'esercizio dei poteri di controllo parlamentare sull'Esecutivo non è, come tale, materia sottratta alla *data protection* europea. Né il fatto che il controllo parlamentare riguardi questioni relative alla sicurezza nazionale vale per ciò stesso a sottrarre all'applicazione delle norme europee il trattamento di dati personali effettuato in un simile contesto. Il limite posto dal GDPR all'applicazione delle proprie previsioni (art. 2) soggiace infatti ad un'interpretazione stringente e va riferito ai soli «trattamenti di dati personali effettuati dalle autorità statali nel contesto di un'attività volta a salvaguardare la sicurezza nazionale», ossia alle attività che, in modo diretto e concreto, sono finalizzate a questo scopo. Compete pertanto al giudice nazionale accertare se, in disparte la qualità pubblica o le attribuzioni del soggetto che lo effettua, il trattamento sia concretamente effettuato al fine di proteggere funzioni ed interessi fondamentali dello Stato e della società (requisito di cui, nel caso deciso, la Corte non ha ravvisato la sussistenza in relazione all'attività di inchiesta parlamentare su temi di generale rilevanza per la sicurezza nazionale).

Il perimetro applicativo del GDPR è quindi da intendere in senso ampio e in coerenza con la "lettura inclusiva" delineata dalla giurisprudenza della stessa Corte, orientata ad una interpretazione restrittiva delle deroghe all'applicazione delle regole di protezione dei dati personali; da queste non sono esentate le attività che si svolgono nella sfera delle funzioni parlamentari, non rilevando a tal fine la natura pubblica del potere o quella dei compiti da questo svolti.

Nella sua impostazione, la sentenza si pone nel solco tracciato dalla CGUE in una precedente occasione, in cui le prerogative dei parlamenti

ISSN 2239-8570

nazionali egualmente non sono state di ostacolo a che le loro attività fossero ricomprese nell'ambito applicativo del GDPR: nel caso deciso nel 2020 su rinvio pregiudiziale del tribunale amministrativo di Wiesbaden, la Corte ha stabilito che se un organo parlamentare determina, da solo o con altri soggetti, le finalità e i mezzi del trattamento (si trattava della "commissione per le petizioni" del Land tedesco dell'Assia), esso deve essere qualificato come "titolare del trattamento" (ai sensi dell'art. 4), e nei suoi confronti l'interessato può esercitare i diritti che gli sono riconosciuti (all'art. 15) tra cui quello alla cancellazione (CGUE 9.7.2020, C-272/19).

Nella filigrana di queste linee evolutive può riconoscersi la vocazione del GDPR a porsi come *lex generalis*, la cui disciplina non si cura di distinguere tra diritto pubblico e diritto privato - anzi solo in modo residuale riserva apposite norme ai poteri pubblici -, e tende progressivamente, nel segno di un'interpretazione generalizzante della portata applicativa del diritto europeo, a penetrare in profondità spazi solo in apparenza presidiati da norme di carattere sostanzialmente derogatorio.

In tale prospettiva la sentenza si segnala anche per le implicazioni che ne derivano per il tema dell'applicabilità del "diritto all'oblio" alle informazioni personali contenute negli atti parlamentari, da alcuni anni venuto all'attenzione con riferimento alla cancellazione di dati personali contenuti in tali atti e documenti o, per meglio dire, alla loro deindicizzazione al fine di impedirne o di limitarne la indiscriminata accessibilità on-line. Al riguardo si distingue il caso italiano, ove si consideri che già nel 2013 entrambe le Camere hanno provveduto a definire, con autonome deliberazioni, modalità omogenee di esercizio del "diritto all'oblio" relativamente ai dati personali presenti negli atti parlamentari pubblicati attraverso i siti istituzionali. Le procedure contemplate allo scopo nei regolamenti adottati dal Senato della Repubblica (testo coordinato delibere del Consiglio di Presidenza del Senato n. 31 del 18 dicembre 2013 e n. 62 del 7 maggio 2015 sul diritto all'oblio) e dalla Camera dei deputati (testo coordinato deliberazioni dell'Ufficio di Presidenza della Camera dei Deputati n. 46/2013, n. 53/2013 e n. 169/2022), mentre era ancora vigente la direttiva 95/46/CE (salvo per la modifica introdotta nel 2022 nel regolamento della Camera dei Deputati con deliberazione n. 169/2022), sono rivolte a perseguire il bilanciamento tra il principio costituzionale di pubblicità dei lavori parlamentari (art. 64 Cost.) e la tutela dei diritti della persona, suscettibili di essere violati quando informazioni a carattere personale non più attuali e potenzialmente lesive della reputazione di un individuo (quali possono essere ad esempio contenute in atti di sindacato ispettivo) siano rese permanentemente accessibili sui siti istituzionali e possano essere facilmente reperibili mediante l'uso di motori di ricerca.

L'adozione di autonome previsioni regolamentari da parte delle Camere ha fondamento radicato nell'autonomia costituzionale del Parlamento e nell'insindacabilità dei suoi *interna corporis*, principio di cui la giurisprudenza della Corte costituzionale ha nel tempo definito i contorni riferendoli agli ambiti strettamente correlati alle funzioni primarie delle Camere. Coerentemente, il Codice dei dati personali (d. lgs. 30.6.2003 n. 196, come modificato dal d. lgs. 10.8.2018, n. 101 di "adattamento" al

ISSN 2239-8570

GDPR, di seguito il **Codice**) include nello spettro dei trattamenti di "categorie particolari di dati personali" motivati da un rilevante interesse pubblico (accanto a quelli generalmente necessari alla «documentazione delle attività istituzionali di organi pubblici»), le analoghe operazioni ricorrenti nelle attività parlamentari qualora comportino un trattamento di dati, quali «la redazione di verbali e resoconti delle attività di assemblee rappresentative», lo «svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo», o in modo più ampio «l'esercizio del mandato degli organi rappresentativi» (art. 2-*sexies*, c. 2, *f*, *g*, *h*, del Codice). Di questi trattamenti il Codice rimette la disciplina all'autonomia delle Camere (e degli altri organi costituzionali), tenute a declinarla in conformità ai loro ordinamenti e nel rispetto dei principi generali di diritto comune (art. 2-*novies* del Codice).

Si tratterà di stabilire se il quadro di riferimento delle richiamate deliberazioni parlamentari debba ritenersi innovato ovvero possa diversamente interpretarsi alla luce della sentenza qui riportata.

ROBERTO D'ORAZIO

https://curia.europa.eu/juris/document/document.jsf?docid=281303&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=IT&cid=24430068

2024/4(16)MM-FN

16. La sentenza della CEDU del 5.11.2024 nel caso 25578/11 contro l'Italia sulla necessità di adire il Garante privacy in relazione al principio del previo esaurimento dei rimedi

Con decisione 25578/11 (di seguito la **Decisione**) notificata il 28 novembre 2024, la Corte Europea dei Diritti dell'Uomo (**CEDU** o la **Corte**) ha stabilito che i ricorsi a Strasburgo, per presunte violazioni di dati personali, sono ammissibili solo nel caso in cui il ricorrente abbia già presentato un reclamo all'autorità per la protezione dei dati personali del proprio Stato. La decisione riconosce all'autorità italiana (l'Autorità Garante per la Protezione dei Dati Personali, di seguito anche **GPDP** o il **Garante**) il ruolo di organismo indipendente e dotato della capacità di adottare misure effettive di tutela, pur non essendo un organo giurisdizionale. Nella decisione, la Corte ha infatti stabilito inammissibile il ricorso di un cittadino italiano contro l'Italia in cui il ricorrente accusava lo Stato di non aver garantito la tutela del diritto al rispetto della vita privata, previsto dall'articolo 8 della Convenzione europea dei diritti dell'uomo (**Convenzione EDU**), che include la protezione dei dati personali.

Il caso in questione riguarda una fuga di dati personali relativa al Servizio per le informazioni sul contribuente (**Serpico**), database dell'anagrafe tributaria, che conserva dati ed informazioni provenienti da

ISSN 2239-8570

dichiarazioni e reclami indirizzati agli uffici delle autorità finanziarie e dalle relative indagini, nonché dati e informazioni che possono essere rilevanti ai fini fiscali. Il registro include informazioni riguardanti spese di gas, acqua, elettricità e telefono, spese per interessi su passività, contributi previdenziali, bonifici bancari, dati sulla registrazione dei veicoli nel registro pubblico delle automobili, iscrizioni a club sportivi e spese di viaggio dei contribuenti. La fuga di dati è avvenuta nel 2010, ad opera di un Ufficiale della Guardia di Finanza, che ha sottratto in modo illecito informazioni riguardanti più di trecento individui e trasmesse ad un giornalista di una nota rivista italiana.

I fatti avevano dato luogo all'apertura di un procedimento penale dinanzi al giudice per l'udienza preliminare del Tribunale di Brescia condannando con sospensione condizionale della pena di un anno i soggetti interessati dal procedimento (paragrafo 8 della Decisione). Nel corso del giudizio, il giudice delle indagini preliminari aveva riscontrato che pur avendo l'ufficiale il diritto di accedere al database, aveva effettuato 1.372 accessi ingiustificati, non legati ai suoi compiti. Tali accessi erano finalizzati all'acquisizione indebita di informazioni finanziarie su personalità di spicco della magistratura, della cultura, della politica e delle istituzioni italiane, su richiesta del giornalista.

Tra le vittime figurava anche il ricorrente (L.C), il quale si è rivolto alla CEDU sostenendo che le autorità italiane non avessero protetto da usi impropri e abusi i suoi dati personali, conservati nel database Serpico, violando così il suo diritto al rispetto della vita privata, previsto dall'Articolo 8 della Convenzione EDU.

La Corte, nel suo ragionamento, ha innanzitutto stabilito l'applicabilità dell'Articolo 8 della Convenzione alla questione in esame, riconoscendo che i dati personali conservati nel database Serpico rientrano nella sfera della vita privata e, pertanto, meritano tutela ai sensi della Convenzione. Successivamente, ha valutato se vi fosse stata una violazione di tale diritto e se l'appellante potesse essere considerato vittima ai sensi dell'art. 34 della Convenzione EDU. Questo duplice esame ha permesso di definire sia il quadro giuridico applicabile sia la posizione dell'applicante rispetto ai fatti contestati.

In primo luogo, la CEDU ha riconosciuto l'applicabilità dell'art. 8 della Convenzione EDU in questo caso, considerando che i dati conservati nel sistema Serpico riguardavano informazioni private e sensibili, come il nome, la data di nascita, l'indirizzo e dettagli finanziari, tra cui reddito, patrimonio netto e pendenze con le autorità fiscali. Ad avviso della Corte, la loro natura intrinsecamente personale rientra nella sfera della vita privata, protetta dall'art. 8 della Convezione EDU. Di conseguenza, il trattamento di tali dati senza adeguate misure di protezione da parte delle autorità nazionali rappresenta un potenziale rischio per il rispetto della privacy dell'appellante.

In secondo luogo, la CEDU ha esaminato il concetto di status di vittima dell'appellante in relazione alle due dimensioni del reclamo dell'appellante: ovverosia (1) l'abuso e uso improprio dei dati personali

ISSN 2239-8570

da parte della Guardia di Finanza e (2) il rischio di uso improprio dei dati personali da parte di terzi

Quanto al primo aspetto (1), la Corte ha riconosciuto che l'appellante era stato direttamente e personalmente coinvolto nella violazione. In particolare, è stato dimostrato che un ufficiale della Guardia di Finanza aveva effettuato accessi non autorizzati al database utilizzando le sue credenziali personali per scopi non connessi ai suoi doveri istituzionali, trasferendo successivamente le informazioni a un giornalista.

Tale condotta, unita all'incapacità dello Stato di prevenire tali accessi abusivi attraverso misure di sicurezza adeguate, ha consentito alla CEDU di qualificare l'applicante, *ratione personae*, come vittima ai sensi della Convenzione EDU.

Sul secondo profilo (2), occorre rilevare che nelle sue argomentazioni l'appellante ha sostenuto che, in qualità di contribuente italiano, era esposto al rischio di abuso dei suoi dati personali da parte di terze parti con accesso al database. Tuttavia, la Corte ha ritenuto che il semplice fatto di appartenere a una categoria generale di persone i cui dati erano conservati nel database non fosse sufficiente per qualificare l'applicante come vittima. La mancanza di prove concrete di un rischio imminente e reale di abuso ha, infatti, portato la Corte a concludere che lo status di vittima non potesse essere riconosciuto, in virtù del principio di incompatibilità *ratione personae*, non sussistendo peraltro neppure circostanze eccezionali.

Prima di concludere l'analisi circa la violazione del diritto alla protezione dei dati personali, la Corte si è soffermata su un aspetto procedurale cruciale, che ha inciso sull'ammissibilità del ricorso. Essa, infatti, ha esaminato non solo l'esistenza di una possibile violazione, ma anche se l'applicante avesse esaurito i rimedi interni prima di adire la Corte Europea dei Diritti dell'Uomo.

In tal senso, la Corte ha sottolineato il principio fondamentale secondo cui, ai sensi dell'art. 35 della Convenzione EDU, il ricorso alla giustizia internazionale è ammissibile solo dopo aver dato alle autorità nazionali l'opportunità di esaminare il caso e di porre rimedio, ove possibile, alle violazioni contestate.

Ed invero, nel caso *de quo*, la CEDU ha dichiarato inammissibile il ricorso in oggetto per non avere l'appellante esaurito i rimedi interni disponibili, in particolare per quanto concerne la possibilità di presentare un reclamo al Garante.

La Corte ha ribadito, infatti, il consolidato principio giuridico secondo cui il ricorso alla Corte Europea è ammissibile soltanto dopo che i ricorrenti abbiano consentito alle autorità nazionali di esaminare e, ove possibile, sanare le violazioni attraverso i rimedi previsti dall'ordinamento nazionale (in particolare per il principio citato dalla Decisione, il caso *Akdivar e altri c. Turchia*, sentenza CEDU del 16 settembre 1996, ricorso n. 21893/93, nonché *Selmouni c. Francia*, sentenza CEDU del 28 luglio 1999, ricorso n. 25803/94, e *Kudła c. Polonia*, sentenza CEDU del 26 ottobre 2000, ricorso n. 30210/96).

ISSN 2239-8570

L'argomentazione ha inoltre messo in evidenza come il Garante, in quanto organismo indipendente e autonomo, costituisse un rimedio adeguato ed efficace per affrontare le problematiche sollevate nel caso. In particolare, il GPDP, pur avendo la possibilità di facilitare la risoluzione delle controversie, non solo può adottare misure correttive, incluse quelle di natura tecnologica e operativa per garantire la protezione dei dati personali, ma ha anche il potere di emettere decisioni vincolanti e di intervenire, sia su richiesta delle parti interessate sia di propria iniziativa. La possibilità di sottoporre poi le decisioni del Garante a revisione giudiziaria, configura un meccanismo completo per tutelare i diritti dei cittadini italiani.

Ebbene, nel caso in esame, l'appellante non ha presentato alcuna denuncia all'Autorità Garante per evidenziare le presunte carenze di sicurezza nella gestione dei dati personali. Tale omissione è stata ritenuta insufficiente a configurare l'esaurimento dei rimedi interni.

La Corte ha, pertanto, ritenuto che il ricorrente non avesse fornito alle autorità nazionali l'opportunità di prevenire o correggere le violazioni della Convenzione EDU oggetto del ricorso. In linea con il consolidato principio giuridico dell'esaurimento dei rimedi interni, la Corte ha sottolineato l'obbligo di ricorrere ai meccanismi giuridici nazionali prima di adire la giustizia internazionale. Proprio a causa dell'assenza di tale passaggio preliminare, il ricorso è stato dichiarato inammissibile per non aver rispettato i requisiti procedurali stabiliti dall'art. 35 della Convenzione EDU.

La decisione della CEDU evidenzia con chiarezza la rilevanza del principio di sussidiarietà, ponendo in rilievo come il previo esaurimento dei rimedi interni, nello specifico il ricorso al GPDP, costituisca non soltanto un requisito procedurale imprescindibile, ma anche uno strumento idoneo a garantire una tutela effettiva dei diritti fondamentali. Tale orientamento conferma il ruolo centrale delle autorità nazionali nel rafforzare la protezione del diritto alla privacy, promuovendo un modello di governance che integra efficacemente le esigenze di protezione dei dati personali con i principi sanciti dall'ordinamento sovranazionale.

MATILDE MARÉ/FEDERICO NESPEGA

https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%2225578%22],%22itemid%22:[%22001-238444%22]}

2024/4(17)MEU

17. La decisione del dicembre 2024 dell'EDPS di accertamento della violazione dell'EUDPR da parte della Commissione europea in relazione ad alcune pratiche di online microtargeting su utenti della piattaforma X a supporto di una pubblicità commissionata dalla Commissione europea

ISSN 2239-8570

Come già riportato in questa Rubrica (v. notizia n. 16 del numero 4/2023 [2023/4(16)TB] e in *Atlante*, p. 446) alla fine del 2023 l'organizzazione NOYB (None of Your Business) ha promosso un ricorso contro la Commissione europea (la **Commissione**) e uno contro X in relazione ad alcune pratiche di online microtargeting a supporto di una pubblicità commissionata dalla Commissione.

Il primo ricorso, depositato il 16 novembre 2023 dinanzi al Garante europeo della protezione dei dati (di seguito **EDPS** o **l'Autorità**), contesta il coinvolgimento della Commissione nel trattamento dei dati personali di utenti specifici della piattaforma X. Il secondo, del 14 dicembre 2023, è stato presentato contro la stessa piattaforma X davanti all'Autorità olandese per la protezione dei dati (**DPA olandese**). Tuttavia, quest'ultima non si è ancora espressa in merito, mentre l'EDPS ha adottato una decisione diffusa da NOYB con comunicato in data 13 dicembre 2024 (di seguito la **Decisione**). Di conseguenza, il seguente contributo si concentrerà sul ricorso sottoposto da NOYB all'EDPS e alla Decisione, valutandone le implicazioni giuridiche alla luce del quadro normativo europeo in materia di protezione dei dati personali.

Passando ad esaminare il caso che ci occupa, NOYB ha promosso un'azione legale nei confronti della Commissione, dinanzi allo EDPS, al fine di denunciare la violazione della normativa sulla protezione dei dati personali applicabile alla Commissione 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 **EUDPR** o il **Regolamento**).

L'asserito inadempimento ha tratto origine da una campagna di *microtargeting* condotta dalla Commissione dal 15 al 28 settembre 2023 attraverso l'utilizzo della piattaforma X, con la finalità di promuovere la proposta di regolamento della Commissione COM/2022/209 avente ad oggetto il contrasto agli abusi sui minori e alla circolazione di materiale pedopornografico tra gli utenti della piattaforma (di seguito la **Proposta**).

La Commissione, in particolare, ha utilizzato una lista di *keywords*, al fine di selezionare, mediante un meccanismo di inclusione ed esclusione, gli utenti a cui rivolgere la Proposta. L'utilizzo delle *keywords* mediante la piattaforma X si è rivelato, come ammesso dalla stessa istituzione europea, lo strumento principale attraverso cui applicare la *targeting strategy*, onde garantire un uso efficiente delle risorse.

A tale tecnica si è, poi, affiancata, la procedura del *look-alike*, che ha permesso, attraverso il raffronto di dati appresi da diversi soggetti, di individuare e profilare utenti con caratteristiche affini. In tal modo, si è favorita una maggiore diffusione della campagna, indirizzandola a coloro che avessero comportamenti simili agli utenti già identificati.

I meccanismi appena descritti hanno determinato, a parere della ricorrente, il trattamento di dati sensibili, in quanto indirizzati alla racconta ed all'elaborazione di informazioni sulla base dell'orientamento politico e religioso di singoli utenti. Secondo quanto ricostruito da NOYB, in particolare, la campagna della Commissione sarebbe stata concepita in

ISSN 2239-8570

modo che gli annunci pubblicitari, relativi alla Proposta, giungessero esclusivamente agli utenti di X che non fossero interessati a parole chiave come #Qatargate, Brexit, Marine Le Pen, Alternative für Deutschland, Vox, Christian, Christian-phobia o Giorgia Meloni. In sostanza, gli annunci promozionali avrebbero avuto l'obiettivo di influenzare l'opinione degli utenti, facendo leva sull'importanza, presumibilmente, attribuita dai partecipanti ad un sondaggio sulla lotta contro gli abusi sui minori, ritenuta superiore rispetto alla tutela della privacy online.

Il ricorrente, dunque, ha sostenuto che tali tecniche hanno violato il Regolamento nella parte in cui hanno utilizzato categorie di dati complessi degli utenti al di fuori dei casi eccezionali ammessi dallo stesso Regolamento, e senza aver previamente ottenuto il consenso espresso dei legittimi titolari.

La Commissione, secondo la ricostruzione offerta, rappresenta l'ente che ha commissionato la campagna pubblicitaria, diffusa per il tramite della piattaforma X, fondata sull'uso dei dati personali. L'istituzione, dunque, avrebbe determinato le finalità del trattamento dei dati, sia i mezzi a cui ricorrere per realizzarlo. L'insieme di queste considerazioni ha consentito all'istante di affermare che la Commissione ha rivestito il ruolo di titolare del trattamento e, in quanto tale, sia responsabile della violazione delle normative in materia di protezione dei dati.

Alla luce della disamina effettuata, il reclamante ha, quindi, sostenuto che la Commissione ha violato l'art. 10 del Regolamento, che dispone il divieto di trattamento di categorie particolari di dati personali, salvo che non ricorrano i casi eccezionali espressamente disciplinati dal paragrafo 2 dalla norma. Il ricorrente ha, dunque, evidenziato che nessuna delle eccezioni previste dalla norma citata è applicabile al caso di specie e che, per tali ragioni, la Commissione ha trattato dati sensibili senza un'adeguata base legale. L'uso scorretto ha comportato, perciò, la violazione del principio di liceità dell'art. 4(1)(a) EUDPR.

Le argomentazioni appena esposte sono state respinte dall'istituzione europea.

La Commissione, infatti, ha sostenuto che la campagna di *microtargeting* è stata realizzata nel rispetto di un contratto, con l'obiettivo di promuovere la diffusione delle sue politiche e attività in materia di Affari Interni, e che la selezione delle parole chiave non è stata basata su dati personali specifici di utenti, ma su un'analisi algoritmica per indirizzare persone con interessi simili a quelli di altri account. La convenuta si è quindi difesa affermando di aver agito con il convincimento che qualsiasi trattamento di dati personali derivante dalla campagna fosse giustificato come necessario per l'esecuzione di un compito nell'interesse pubblico, in quanto la comunicazione su iniziative legislative è parte delle sue attività quotidiane. La Commissione ha, inoltre, respinto l'accusa di aver trattato categorie particolari di dati personali, sostenendo che, in ogni caso, il trattamento di dati personali era stato conforme al Regolamento, poiché giustificato dalla necessità di svolgere un compito pubblico.

Sulla base delle argomentazioni svolte dalle parti, l'EDPS si è pronunciata ed ha accertato la violazione degli articoli 4(1)(a), 4(2), 5, 10

ISSN 2239-8570

(1) e 26 del Regolamento da parte della Commissione, avendo quest'ultima trattato illecitamente i dati del reclamante, comprese le categorie particolari di dati, senza che vi fosse una valida base giuridica che ne giustificasse l'utilizzo.

L'Autorità, in primo luogo, ha affermato che, nel caso di specie, non troverebbe applicazione l'articolo 5(1)(a) EUDPR, poiché non viene in rilievo alcuna esigenza che giustifichi il trattamento dei dati per l'esecuzione di un compito di interesse pubblico, ma soprattutto per l'insussistenza di una legge che abbia investito la Commissione dei poteri pubblici necessari per perseguire un simile interesse. La Commissione, in ultima analisi, avrebbe dovuto richiedere il consenso esplicito in relazione al trattamento di categorie di dati particolari, come stabilito dall'articolo 10(2)(a) del Regolamento. In tale prospettiva, ha osservato l'Autorità, è indubbio che l'istituzione non abbia adempiuto a tale prescrizione.

L'EDPS, in conclusione, ha adottato nei confronti della Commissione la misura dell'ammonimento come misura correttiva e proporzionata, non potendo ignorare che si trattasse di violazioni afferenti a categorie particolari di dati personali. Lo scopo dell'irrogazione, come evidenziato dall'art. 58(2)(b) EUDPR è quello di ottenere un effetto dissuasivo, oltre che quello di evidenziare all'istituzione dell'UE interessata la violazione della normativa.

Posta la discrezionalità che il Regolamento riconosce all'Autorità, quest'ultima si è, dunque, determinata contemperando la gravità della violazione con la necessità di garantire un livello elevato e coerente di protezione dei dati personali, mediante la puntuale applicazione della normativa sulla protezione dei dati. Si evidenzia, infine, che l'EDPS ha considerato come elemento attenuante la circostanza che la Commissione abbia interrotto la campagna oggetto di contestazione e che, dunque, il trattamento non sarebbe, attualmente, più in corso. Per tali ragioni, osserva l'Autorità, non sarebbe necessario procedere all'adozione di altre misure volte a far conformare la Commissione al Regolamento.

MARIA ELENA URSITTI

https://noyb.eu/sites/default/files/2024-12/EDPSDecision_printed_Redacted.pdf

2024/4(18)LC

18. La sanzione di quasi 800 milioni di euro irrogata a Meta dalla Commissione europea il 14.11.2024 per pratiche abusive relative a Facebook Marketplace

Con comunicato stampa del 14 novembre 2024, la Commissione europea ha annunciato di aver sanzionato Meta per 797,72 milioni di euro e di aver ordinato la cessazione e vietato la reiterazione di condotte ravvisate come anticoncorrenziali, sulla base delle risultanze di un procedimento formale avviato nel giugno 2021. L'accertamento ha riguardato la violazione delle

ISSN 2239-8570

norme antitrust eurounitarie a causa della connessione del servizio di annunci online al più noto servizio di social networking (Facebook), definito dalla Commissione come un *"illegal tie"*. Attraverso tale operazione, Meta avrebbe imposto condizioni commerciali inique agli altri fornitori di servizi di annunci pubblicitari già presenti sul mercato. Tra questi si annoverano piattaforme come eBay, Leboncoin in Francia, Marktplaats in Olanda, Subito in Italia, Blocket in Svezia e Finn.no in Norvegia, ma anche nuove iniziative imprenditoriali che stanno registrando negli ultimi anni un discreto successo entro i confini europei, come Vinted. Meta è tra le Big Tech statunitensi che ha come suo *core business* il servizio di social network personale, denominato Facebook, all'interno del quale è possibile accedere, dal 2016, all'offerta di un servizio ulteriore di annunci online, denominato Facebook Marketplace, che rappresenta uno spazio virtuale in cui gli utenti possono acquistare e vendere beni. Proprio con riferimento a queste attività, l'indagine della Commissione ha rilevato che Meta detiene una posizione dominante nello Spazio economico europeo non solo nel mercato dei social network, ma anche nei mercati nazionali della pubblicità online che trovano i loro principali spazi sui social media. In particolare, come anticipato, Meta avrebbe abusato delle sue posizioni dominanti in violazione dell'art. 102 del Trattato sul funzionamento dell'Unione europea (TFUE), connettendo il servizio di annunci online Facebook Marketplace al social network Facebook. Da ciò ne è derivato un'automatica e costante esposizione di tutti gli utenti iscritti a Facebook al relativo servizio di marketplace, indipendentemente da una loro espressa volontà in tal senso. Tale pratica avrebbe indebitamente escluso gli altri operatori sul mercato dal gioco della leale concorrenza, poiché tale legame conferisce a Facebook Marketplace un vantaggio di distribuzione sostanziale che i concorrenti non potrebbero eguagliare. Inoltre, secondo la Commissione, imporre unilateralmente condizioni commerciali inique ad altri fornitori di servizi di annunci online che pubblicizzano sulle piattaforme di Meta, consente alla stessa società di utilizzare i dati relativi agli annunci generati da altri inserzionisti a suo esclusivo vantaggio. Pertanto, la Commissione ha sanzionato Meta per 797,72 milioni di euro e ha imposto la cessazione e la reiterazione di simili condotte anticoncorrenziali. Nel definire l'importo della sanzione, la Commissione ha tenuto conto della durata e della gravità delle condotte violative del diritto antitrust, nonché del fatturato di Facebook Marketplace.

LUCIO CASALINI

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5801

2024/4(19)TB

19. Il report del 9.10.2024 della Commissione europea al Parlamento e al Consiglio sulla prima revisione periodica circa il

ISSN 2239-8570

funzionamento della decisione di adeguatezza sullo EU-US Data Privacy Framework

In data 9 ottobre 2024 la Commissione Europea ha pubblicato un report sulla prima revisione periodica circa il funzionamento della sua decisione di adeguatezza adottata in data 10 luglio 2023 sullo *EU-U.S. Data Privacy Framework* (**DPF**) (su cui v. in questa Rubrica, notizia n. 2 nel numero 3/2023 [2023/3(2)CR] e in *Atlante*, p. 372).

Tale relazione, siglata COM(2024) 451 final e intitolata *Report from the Commission to The European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework* (di seguito la **Relazione**), è stata pubblicata all'esito della prima attività di riesame condotta a norma dell'art. 3 del DPF, che impone appunto alla Commissione di svolgere revisioni periodiche sullo stato di implementazione del DPF stesso.

Nella Relazione viene in primo luogo esaminato il procedimento di certificazione e ricertificazione annuale cui le società americane devono sottoporsi onde poter dimostrare la propria conformità ai requisiti previsti dalla DPF in materia di protezione dei dati personali. La conformità a tali requisiti viene verificata da parte del Dipartimento del Commercio statunitense (**DoC**).

All'esito della revisione, è risultato che più di 2800 società statunitensi – di cui il 70% sarebbero PMI ed il 47% opererebbe nel settore ICT - hanno ottenuto la certificazione al DPF, numero superiore rispetto a quello raggiunto nel primo anno di operatività della precedente decisione di adeguatezza (il c.d. "*Privacy Shield*", adottato nel 2016 e successivamente dichiarato nullo dalla CGUE per il tramite della sentenza emessa in data 16 luglio 2020 nella causa C-311/18, meglio nota come "*Schrems-II*", su cui v. in questa Rubrica, notizia n. 1 nel numero 3/2020 [2020/3(1)CR] e in *Atlante*, p. 25).

Secondo quanto previsto dal DPF, il DoC è responsabile del monitoraggio sull'osservanza dei principi del DPF tramite l'utilizzo di vari strumenti, inclusi controlli d'ufficio, verifiche *ad hoc* e questionari di conformità.

La Commissione ha riconosciuto che, in questo primo anno di operatività del DPF, il DoC doveva concentrare i propri sforzi nella definizione del procedimento di certificazione. Andando avanti, secondo la Commissione, il DoC dovrà incrementare i propri sforzi nel monitoraggio e nella verifica della compliance con i principi del DPF.

Per quanto concerne la possibilità di proporre reclami, il DPF fornisce ai cittadini diversi strumenti, tra i quali i seguenti:

- la possibilità di contattare direttamente un'organizzazione certificata ai sensi del DPF, che deve fornire una risposta entro 45 giorni. Secondo quanto riferito dalle associazioni di categoria, le società certificate DPF avrebbero ricevuto un numero assai limitato di reclami,
- il ricorso avanti gli organismi indipendenti appositamente designati secondo il meccanismo di ricorso indipendente (**IRM**),

ISSN 2239-8570

vale a dire organismi di risoluzione alternativa delle controversie od autorità di protezione dei dati personali ai sensi del regolamento (UE) 2016/679 (**GDPR**). Anche per questo strumento, la Relazione evidenzia che sarebbe stato proposto un numero molto limitato di reclami;

- l'opzione di adire il centro internazionale per la risoluzione delle dispute, vale a dire la divisione internazionale dell'Associazione Arbitrale statunitense. Al momento della revisione, il meccanismo arbitrale non è stato adito da nessun individuo.

Tali strumenti di reclamo, a partire dall'entrata in vigore del DPF, sono stati oggetto di campagne informative condotte dal DoC con la finalità di aumentare la consapevolezza circa la loro esperibilità.

Dal punto di vista degli sviluppi legislativi, la Relazione evidenzia che negli USA sono intervenute diverse novità normative. A livello federale, il Presidente ha emesso numerosi Ordini Esecutivi, tra cui il 14117 del 28 febbraio 2024, che proibisce – o comunque limita – le transazioni relative a determinate categorie di dati personali sensibili (ad esempio dati relativi alla salute, identificatori biometrici, dati sul genoma umano). A livello statale, 20 Stati hanno introdotto ampie leggi sulla privacy, delle quali otto già entrate in vigore (California, Colorado, Oregon, Virginia, Connecticut, Utah, Texas e Florida). Inoltre, 17 Stati hanno adottato normative relative al trattamento automatizzato (o, almeno ad alcune sue forme) che in genere consentono *l'opt -out* per determinati tipi di decisioni basate sulla profilazione.

In aggiunta, la Commissione Federale per il Commercio (*Federal Trade Commission*, **FTC**) ha annunciato recenti sviluppi nel suo approccio al trattamento automatizzato ed all'intelligenza artificiale.

Per quanto concerne le regole che disciplinano la raccolta e l'utilizzo, da parte di autorità pubbliche statunitensi, di dati personali trasferiti dall'UE alle società certificate DPF, la Relazione affronta soltanto gli sviluppi relativi all'ambito della sicurezza nazionale.

Le conclusioni raggiunte nel DPF in merito all'accesso ai dati da parte di agenzie di *signal intelligence* si basano sull'analisi delle condizioni e dei limiti che si applicano alle loro operazioni– in particolare ai sensi della Section 702 del Foreign Intelligence Surveillance Act (**FISA**) e dell'Ordine Esecutivo 12333-del 4 dicembre 1981, complementate e rafforzate dal recente Ordine Esecutivo 14086 del 7 ottobre 2022 (**EO 14086**) (sul quale v. in questa Rubrica, notizia n. 4 nel numero 1/2023 [2023/1(4)CR] e *Atlante*, p. 301), sul rafforzamento delle salvaguardie per le attività di *signal intelligence* negli USA.

Le salvaguardie disposte dall'EO 14086 a tutte le attività di *signal intelligence*, indipendentemente dall'autorità da cui promanano e dal luogo in cui vengono condotte, sono finalizzate a proteggere i dati dei cittadini non statunitensi (inclusi i cittadini dell'UE). Tale ordine esecutivo introduce inoltre un nuovo meccanismo di ricorso tramite il quale queste l'applicazione di queste salvaguardie vincolanti possa essere invocata da individui nell'UE.

ISSN 2239-8570

L'EO 14086 prevede una lista di obiettivi legittimi per cui le attività di *signal intelligence* possono essere condotte utilizzando *database* di dati personali. Per quanto riguarda la modifica o l'aggiunta di potenziali ulteriori obiettivi, l'EO 14086 prevede in particolare la necessità di consultazione dell'Ufficio per le Libertà Civili (**CLPT**) costituito in seno all'Ufficio del Direttore dell'Intelligence Nazionale statunitense (**ODNI**) ogni qualvolta si debba valutare se una priorità promuova uno o più obiettivi legittimi elencati nell'EO 14086; o se non era stata progettata, né previsto che potesse risultare tra gli obiettivi proibiti elencati nell'EO 14086; o ancora se è stata stabilita dopo attenta considerazione per la privacy e le libertà civili di tutti gli individui.

La Section 702 della FISA, che era prevista scadere al termine del 2023, è stata rinnovata per due anni con una serie di cambiamenti.

In primo luogo, sono state introdotte tre modifiche al perimetro delle attività di sorveglianza:

- è stata definitivamente proibita la raccolta degli *abouts* dalle comunicazioni, vale a dire gli elementi rilevanti ai fini dell'applicazione della FISA (come gli indirizzi *email*) che non si trovino nel campo mittente o destinatario;
- la definizione di informazioni rilevanti per l'*intelligence* straniera è stata allargata in modo tale da includere informazioni relative al contrasto alla diffusione di narcotici (soprattutto in relazione alla gravità della crisi Fentanyl)*;*
- è stata ampliata anche la definizione di fornitore di servizi di comunicazione elettronica. Tale allargamento ha suscitato contestazioni da parte di varie organizzazioni non governative(**NGO**) ed è stata proposta una modifica che risulta essere in fase di discussione al Congresso.

Nel corso della revisione è stato comunque confermato che le salvaguardie dell'EO 14086 continuano ad applicarsi nella loro totalità a tutte le attività di raccolta ed utilizzo dei dati ai sensi della Section 702 FISA, anche all'esito delle recenti modifiche.

In secondo luogo, sono stati apportati dei cambiamenti a livello istituzionale e procedurale, tra cui i seguenti:

- l'aggiunta di requisiti in termini di *accountability*, monitoraggio e relazione sulle attività svolte, con particolare riferimento alle attività svolte ai sensi della Section 702 FISA da parte del personale dell'FBI;
- l'introduzione di limitazioni all'utilizzo da parte dell'FBI di dati raccolti, e di un divieto di verifica automatica di informazioni non minimizzate, ai sensi della Section 702 FISA;
- la modifica di alcune norme relative allo status ed al ruolo degli *amici curiae*, ossia degli individui designati come esperti per assistere la Corte per la Sorveglianza dell'Intelligence Estera (**FISC**) in materie relative a privacy e libertà civili o fornire chiarimenti su problematiche tecnologiche. In particolare, la FISC può ora nominare uno o più *amici curiae*, benché le informazioni fornite da questi ultimi debbano essere limitate alle specifiche problematiche

ISSN 2239-8570

identificate dalla stessa corte (le cui aree di applicazione rimangono comunque ampie).

A livello statistico, il *report* annuale di trasparenza pubblicato dall'ODNI mostra un incremento del numero delle richieste ai sensi della Section 702 FISA (da 245073 a 268590). Molte società certificate DPF (tra cui Google e Meta) sfruttano la possibilità concessa dalla legge statunitense di pubblicare relazioni di trasparenza relativi al numero di richieste ricevute in un determinato periodo ai sensi di tale disposizione.

Molte NGO hanno sollevato domande e perplessità sulle nuove forme di acquisizione dei dati da parte delle agenzie di *intelligence*, con particolare riferimento all'utilizzo di *data broker*, che si collocherebbe al di fuori dal perimetro della FISA e dall'EO 14086.

La Relazione evidenzia però che qualsiasi tipo di condivisione volontaria di dati con terze parti è soggetta a numerose dettagliate condizioni ai sensi del DPF, tra cui l'obbligo di notiziare gli individui coinvolti e fornire loro una scelta, nonché la possibilità di effettuare la condivisione solo per scopi limitati e specifici, e soltanto se il contratto impone alla terza parte di fornire il medesimo livello di protezione garantito dai principi del DPF. Inoltre, la FTC ha adottato azioni coattive contro *data broker* coinvolti in attività di vendita di dati sensibili dei consumatori.

L'attività delle agenzie di *intelligence* statunitensi è soggetta alla supervisione di differenti autorità, tra cui i CLPO, l'Ispettorato Generale della Comunità d'Intelligence ("**ICIG**"), il Congresso e il Comitato per la Supervisione sulla Privacy e le Libertà Civili ("**PCLOB**"). La conformità dell'operato delle agenzie con l'EO 14086 è costantemente verificata dall'ICIG come parte delle sue funzioni di revisione. Le agenzie devono peraltro dotarsi di funzionari esperti, muniti di adeguate competenze legali e di *compliance*, al fine di assicurare la conformità alla legge statunitense.

L'EO 14086, cui si aggiunge un Regolamento Attuativo del Procuratore Generale, ha introdotto inoltre un nuovo meccanismo di ricorso per gestire e risolvere i reclami proposti in relazione all'attività delle agenzie di *signal intelligence* statunitensi, che ciascun individuo nell'UE è legittimato a proporre con riferimento a trasferimenti di dati negli USA in violazione della propria *privacy* e delle sue libertà civili.

Il meccanismo prevede la possibilità di proporre un ricorso tramite l'autorità di protezione dei dati nazionale in ciascuno Stato membro, che viene veicolato tramite il segretariato dell'EDPB. Dopodiché vi sono due fasi: un'iniziale indagine condotta dall'ODNI CLPO e (ii) la possibilità per gli individui di impugnarne gli esiti avanti la Corte per la Revisione sulla Protezione dei Dati (**DPRC**) indipendente. Le decisioni dell'ODNI CLPO e della DPRC sono vincolanti per le agenzie di intelligence.

I giudici della DPRC sono selezionati, ai sensi dell'EO 14086, sulla base di particolari requisiti ed includono *ex* giudici di corti federali distrettuali e corti d'appello, un *ex* procuratore generale ed un *ex* membro del PCLOB. In aggiunta, due avvocati speciali, muniti di competenze in materia di privacy e sicurezza nazionale, sono stati nominati con la funzione di rappresentare gli interessi degli individui avanti la DPRC.

ISSN 2239-8570

La gestione dei reclami è regolata sulla base dell'Intelligence Community Directive 126 adottata dall'ODNI il 6 dicembre 2022, che regola in dettaglio diversi aspetti del processo di indagine e decisione dei reclami.

Una serie di misure aggiuntive sono inoltre state adottate nell'UE e negli USA per informare la generalità del pubblico in relazione alle caratteristiche dei meccanismi di ricorso, nonché per facilitare la presentazione e la gestione dei reclami, tra cui una nota informativa adottata dall'EDPB che include un modello di reclamo standard.

Ciò premesso, la Relazione sottolinea che, al momento della revisione, nessun reclamo risulta essere stato presentato mediante il nuovo meccanismo di ricorso, la cui applicazione deve pertanto essere ancora vagliata all'atto pratico.

In conclusione, la Commissione osserva che le autorità statunitensi hanno posto in essere le strutture e le procedure necessarie per assicurare che il DPF funzioni in modo effettivo, pur rilevando che – dopo un solo anno dall'adozione dello stesso – l'applicazione pratica delle salvaguardie ivi previste sia necessariamente limitata. Pertanto, la Commissione continuerà a monitorare gli sviluppi rilevanti nei prossimi anni, con particolare riferimento alle relazioni del PCLOB sull'implementazione dell'EO 14086 ed al funzionamento dei meccanismi di ricorso; (2) a possibili ulteriori modifiche alla Section 702 FISA; e (3) alla nomina ed all'elezione di membri del PCLOB per l'assegnazione dei posti vacanti.

La Commissione ritiene inoltre importante che:

- il DoC utilizzi pienamente i diversi strumenti forniti dal DPF per il monitoraggio della conformità delle società ai principi ed alla rilevazione di dichiarazioni fraudolente di partecipazione al framework;
- la FTC sviluppi ulteriormente il suo approccio proattivo all'investigazione e all'*enforcement* della conformità delle società certificate ai sensi del DPF; e
- il DoC, la FTC e le autorità di protezione dei dati europee sviluppino linee guida comuni sui requisiti chiave ai sensi dei principi del DPF, ad esempio sulla nozione di dati relativi alle risorse umane (*HR Data*) ed ai trasferimenti ulteriori (*Onward Transfers*).

La Commissione suggerisce infine lo svolgimento della prossima revisione periodica dopo tre anni (in luogo del massimo di quattro previsto dalle norme applicabili), così che si possa consolidare una maggiore esperienza sull'applicazione pratica del DPF e tenere conto degli sviluppi destinati ad avere luogo prossimamente.

TIMOTEO BUCCI

https://commission.europa.eu/document/download/25695177-8073-4ce3-bf81-eb816dc6b468_en?filename=Report%20on%20the%20first%20periodic%20review%20of%20the%20functioning%20of%20the%20adequacy%20decision%20on%20the%20EU-US%20Data%20Privacy%20Framework.pdf

ISSN 2239-8570

20. Il report del 4.11.2024 dell'EDPB sulla prima revisione periodica circa il funzionamento della decisione di adeguatezza sullo EU-US Data Privacy Framework

Successivamente alla pubblicazione del report della Commissione europea del 9 ottobre 2024, di cui al contributo precedente (v. sopra), in data 4 novembre 2024 anche il Comitato Europeo per la Protezione dei Dati (**EDPB**) ha pubblicato una sua relazione sulla decisione di adeguatezza del 10 luglio 2023 sullo *EU-U.S. Data Privacy Framework* (**DPF**), intitolata *EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-U.S. Data Privacy Framework* (la **Relazione EDPB del 4.11.2024**). Anche questa relazione è stata redatta all'esito della revisione periodica prevista ai sensi dell'art. 3 del DPF, ed in particolare dopo una riunione a ciò dedicata, cui hanno partecipato nel luglio 2024 anche cinque rappresentanti dell'EDPB.

La Relazione EDPB del 4.11.2024 è focalizzata in particolare sugli aspetti commerciali dello DPF e sull'accesso da parte delle autorità pubbliche statunitensi ai dati personali trasferiti dall'Europa alle organizzazioni certificate ai sensi del DPF.

Con riferimento agli aspetti commerciali del DPF, l'EDPB rileva come il Dipartimento del Commercio statunitense (**DoC**) abbia intrapreso tutti i passaggi rilevanti per l'implementazione del procedimento di certificazione per le società statunitensi.

Al contempo, l'EPDB evidenzia tuttavia la mancanza di attività di supervisione d'ufficio e di azioni strutturali di *enforcement* da parte del DoC, della Commissione Federale per il Commercio (**FTC**) e del Dipartimento del Trasporto statunitense (**DoT**) con riferimento alla conformità sostanziale delle organizzazioni certificate ai sensi del DPF rispetto ai principi del medesimo.

Per questo motivo, l'EPDB invita il DoC e la FTC ad incrementare indagini d'ufficio per la verifica di tale conformità, sottolineando che tale profilo sarà oggetto di specifico riesame nel corso della successiva attività di revisione del DPF.

Con riferimento alle organizzazioni uscite dal DPF ed a quelle classificate come inattive in ragione della scadenza delle loro certificazioni, l'EDPB sottolinea la necessità che il DoC verifichi l'effettività della restituzione, della cancellazione o della conservazione – a seconda dei casi - dei dati ricevuti ai sensi del DPF. In caso di conservazione, l'organizzazione è obbligata a continuare ad applicare i Principi del DPF e ad identificare un punto di contatto per future comunicazioni.

Quanto al sistema di ricorso multilivello previsto dal DPF, l'EPDB nota positivamente come sia stato aggiornato ed attuato in modo tale da fornire

ISSN 2239-8570

una gamma di percorsi agevolmente accessibili per i reclami da parte di cittadini europei.

Allo stesso tempo, l'EDPB evidenzia come l'esiguo numero di reclami ammissibili nel primo anno di applicazione del PDF appaia confermare le precedenti preoccupazioni dell'EDPB circa la necessità di prevedere una serie di verifiche proattive da parte delle autorità statunitensi sulla conformità agli elementi sostanziali dei principi DPF.

L'EDPB ha altresì invitato il DoC ad elaborare e pubblicare linee guida pubbliche sull'*accountability* per gli ulteriori trasferimenti (*onward transfers*) ai sensi del DPF, destinate agli importatori dei dati negli USA, allo scopo di chiarire i requisiti cui le società certificate DPF che ricevono dati personali da esportatori europei devono conformarsi per potere trasferire tali dati in Paesi terzi.

Un ulteriore punto di interesse toccato dalla Relazione EDPB del 4.11.2024 consiste nella evidenziazione della necessità di risolvere la divergenza tra le diverse interpretazioni date dalle autorità statunitensi ed europee alla nozione di dati relativi alle risorse umane (**HR Data**), già messa in luce in diverse occasioni da parte dell'EPDB. Sotto questo profilo, mentre a parere del DoC solamente il trattamento di dati di dipendenti all'interno dello stesso gruppo societario ricade nella categoria di HR Data ai sensi del DPF, l'EPDB ha sempre ritenuto che tale categoria ricomprenda qualsiasi dato personale riguardante un dipendente nel contesto di una relazione lavorativa, indipendentemente dal fatto che il dato venga trasferito all'interno di un gruppo societario o ad un diverso operatore commerciale. Sul punto, l'EPDB evidenzia l'importanza di assicurare la competenza delle autorità di protezione dei dati dell'UE in tutti i casi nei quali HR Data vengano trasferiti ai sensi del DPF.

In relazione agli sviluppi legislativi in materia di protezione dei dati negli USA, la Relazione EDPB del 4.11.2024 rileva positivamente l'adozione di ampie normative privacy in venti Stati, di cui nove già entrate in vigore, pur osservando espressamente che le possibilità di adozione di una legge federale in materia di protezione di dati, che contribuirebbe ad assicurare la stabilità della decisione di adeguatezza, appaiono esigue.

Con riferimento all'accesso da parte di autorità pubbliche statunitensi ai dati personali trasferiti dall'UE ad organizzazioni certificate ai sensi del DPF, la Relazione EDPB del 4.11.2024 richiama il fatto che la decisione di adeguatezza si basa in particolare sulla valutazione positiva della Commissione circa l'Ordine Esecutivo 14086 del 7 ottobre 2022 (sul quale v. in questa Rubrica, notizia n. 4 nel numero 1/2023 [2023/1(4)CR] e *Atlante*, p. 301) (**EO 14086**), il quale dispone l'applicazione di salvaguardie aggiuntive, tra cui spicca l'introduzione dei concetti di necessità e proporzionalità nel sistema normativo statunitense sulle attività di *signal intelligence* e stabilendo un nuovo meccanismo di ricorso.

Sull'implementazione dei principi di necessità e proporzionaità, l'EPDB riconosce che le *policy* e le procedure interne della Comunità d'Intelligence statunitense sono state aggiornate e pubblicate, rilevando però – ak contempo - che nel corso dell'attività di revisione non vi è stata occasione di

ISSN 2239-8570

discutere esempi che identificassero chiaramente come i principi in questione siano specificamente interpretati ed applicati a livello di agenzie.

La Relazione EDPB del 4.11.2024 rileva inoltre che molte – se non tutte – tali *policy* e procedure prevedono eccezioni alla loro applicazione in determinate ipotesi, ad esempio in funzione dell'immediatezza o della gravità di una minaccia alla sicurezza nazionale. Sul punto, L'EDPB esprime una richiesta di migliore comprensione di tali eccezioni e delle potenziali implicazioni pratiche, così da poterne stimare l'impatto reale sulla protezione dei dati personali.

In relazione agli obiettivi predefiniti previsti dall'EO 14086 per l'esecuzione di attività di *signal intelligence*, ed alla possibilità di aggiornare ed aggiungere – anche non pubblicamente - tali obiettivi, l'EDPB sottolinea l'importanza di assoggettare la possibilità di stabilire obiettivi segreti a meccanismi di supervisione aggiuntivi ed indipendenti. Sotto questo profilo, l'EPDB accoglie con favore la possibilità che il Comitato per la Protezione della Privacy e delle Libertà Civili (**PCLOB**) possa effettuare revisioni su aggiornamenti segreti della lista degli obiettivi legittimi dopo una richiesta di informazioni confidenziali.

Nell'opinione sulla prima bozza del PDF, l'EPDB aveva segnalato come criticità la mancanza nel sistema legale statunitense di requisiti di autorizzazione preventiva da parte di un'autorità indipendente in caso di raccolta di dati in blocco ai fini di un accesso governativo, contrariamente a quanto stabilito dalla giurisprudenza della Corte di Giustizia dell'Unione Europea. Su questo aspetto l'EDPB rileva che non vi sono stati ulteriori sviluppi e sottolinea nuovamente le criticità sollevate.

Circa l'approvazione della nuova versione della Section 702 del Foreign Intelligence Sureveillance Act (**FISA**), l'EDPB rileva positivamente le modifiche normative dirette ad irrobustire la protezione dal punto di vista privacy e richiama la piena applicabilità dell'EO 14086 ai fini delle richieste di accesso agli atti ai sensi della Section 702 FISA. Per converso, l'EPDB esprime rammarico per la mancata incorporazione di alcune salvaguardie delll'EO 14086 nella versione aggiornata della Section 702 FISA, esprimendo in particolare preoccupazione in merito alla vaghezza della definizione di fornitore di servizi di comunicazione elettronica, che non apparirebbe integrare il requisito di diritto chiaro, preciso ed accessibile. Sul punto l'EDPB evidenzia l'importanza del monitoraggio da parte della Commissione sui futuri sviuppi della Section 702 FISA ed incoraggia il PCLOB a dare seguito a tali sviluppi.

L'EDPB ha poi riconosciuto dei significativi miglioramenti In relazione all'efficacia dei meccanismi di ricorso adottati con il DPF, con particolare riferimento ai poteri ed all'indipendenza della Corte per la Revisione sulla Protezione dei Dati (**DPRC**). Sotto questo profilo, la Relazione sottolinea la pregnanza dei criteri di selezione dei giudici della DPRC, che corrispondono a quelli utilizzasti per la nomina dei giudici federali, con l'aggiunta di requisiti di appropriata esperienza in materia di diritto della *privacy* e sicurezza nazionale.

L'EDPB pone inoltre in risalto la campagna informativa condotta negli USA in relaizone ai meccanismi di ricorso per il tramite deii siti

ISSN 2239-8570

delk'Ufficio del Direttore dell'Intelligence Nazionale statunitense (**ODNI**) e del Dipartimento di Giustiia (**DoJ**), nonché i corrispettivi sforzi profusi dall'EDPB stesso per rendere operativi i meccanismi di ricorso dal lato europeo, come ad esempio l'adozione di un modello di reclamo volto a facilitare la presentazione e la gestione dei reclami.

Ciò premesso, la relazione osserva tuttavia che, alla data della sua pubblicazione, nessun reclamo risulta essere stato proposto ai sensi del nuovo *framework* e che – pertanto – i meccanismi di ricorso non sono ancora stati testati all'atto pratico.

Quanto all'accesso governativo a dati commerciali, la Relazione EDPB del 4.11.2024 ha evidenziato le criticità, in una prospettiva di *privacy*, della prassi invalsa negli USA di acquisto di tali dati da parte di agenzie di *intelligence* presso intermediari di dati ed altre entità commerciali. Siffatto acquisto non ricade nell'ambito di applicazione dell'EO 14086 e – conseguentemente – non è sottoposto alle salvaguardie previste nello stesso, inclusi i meccanismi di ricorso. Sotto questo profilo le autorità USA avrebbero segnalato l'applicabilità di ulteriori normative che definirebbero i limiti e le condizioni di legittimità di tali acquisti, quali l'Ordine Esecutivo 12333 del 4 dicembre 1981 e il *Binding Intelligence Community Policy Framework* recentemente pubblicato dall'ODNI. Tuttavia, come osservato dalla Corte di Giustizia dell'UE nella sentenza c.d. "*Schrems II"* del 16 luglio 2020, nella causa-C 311/18 (su cui v. in questa Rubrica, notizia n. 1 nel numero 3/2020 [2020/3(1)CR] e in *Atlante*, p. 25), l'EO 12333 non garantisce un livello di protezione essenzialmente equivalente a quello stabilito dal Reg. UE 2016/679 in materia di protezione dei dati personali (**GDPR**). L'EDPB sottolinea quindi la necessità di garantire un adeguato livello di protezione a livello esteso, includendo la particolare forma di accesso governativo ai dati in commento.

Infine, la Relazione EDPB del 4.11.2024 commenta positivamente sul suggerimento della Commissione di effettuare la prossima revisione periodica del DPF entro tre anni da quella recentemente conclusa (in luogo del massimo di quattro anni stabilito per la revisione), suggerendo di tenere in considerazione i numerosi punti segnalati come oggetto di stretto monitoraggio.

TIMOTEO BUCCI

https://www.edpb.europa.eu/our-work-tools/our-documents/other/edpb-report-first-review-european-commission-implementing_en

2024/4(21)SB

21. Le Linee guida EDPB 2/2023 (versione 2.0) del 7.10.2024 sul campo tecnico di applicazione dell'art. 5(3) della direttiva e-Privacy

ISSN 2239-8570

Il 7 ottobre 2024 il Comitato europeo per la protezione dei dati (**EDPB**) ha approvato la versione definitiva (2.0) delle Linee guida 2/2023 sull'ambito di applicazione dell'art. 5(3) della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (**direttiva e-Privacy** o **ePD**) come da ultimo modificata dalla direttiva 2009/136/CE.

La versione definitiva (di seguito soltanto le **Linee guida**) non si discosta dalla versione provvisoria del 14 novembre 2023 sulla quale si è svolta la pubblica consultazione (sulla quale v. in questa Rubrica la notizia n. 10 nel numero 4/2023 [2023/4(10)SB] e in *Atlante*, p. 436).

Rinviando, quindi, al precedente commento, qui, in via riassuntiva, ricordiamo che le Linee guida intendono offrire una lettura dell'art. 5(3) ePD quanto più estesa possibile così da renderlo generalmente applicabile anche alle nuove tecniche di archiviazione di informazioni e/o di accesso ai dati memorizzati in apparecchiature terminali connesse o, comunque, in grado di connettersi (cfr. Linee guida, par. 15 e nota n. 9) ad una rete di comunicazione pubblica. E ciò per evitare che attraverso nuove tecniche di archiviazione/accesso e, più in generale, di tracciamento delle informazioni degli utenti di apparecchiature terminali connesse (o in grado di connettersi) ad una rete pubblica, si eluda l'obbligo di raccolta del consenso e, prima ancora, quello di una corretta informativa all'utente. In buona sostanza, dunque, lo scopo delle linee guida è quello di rendere effettivo (o maggiormente effettivo) quanto previsto dal Considerando 24 della ePD, e, aggiungeremmo noi, dal Considerando 7 ePD, cioè l'esigenza di tutela della riservatezza e, in particolare dei diritti fondamentali (tra i quali rientra anche il diritto alla riservatezza quale espressione della sfera privata tutelata dall'art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea, **CDFUE**) delle persone fisiche e degli interessi legittimi delle persone giuridiche dall'accresciuta capacità dei soggetti operanti nell'ambito di una rete pubblica di comunicazioni (società di comunicazione, provider di servizi internet etc.) di accesso, memorizzazione e, in ultima analisi, di trattamento dei dati degli abbonati e degli utenti.

La struttura delle Linee guida è a due livelli: una parte generale in cui sono richiamate le nozioni di "informazioni", "archiviazione/memorizzazione", "accesso" ad informazioni già archiviate, "apparecchiatura terminale", "rete pubblica di comunicazione"; una parte speciale dedicata all'esame di alcune tecniche di memorizzazione/accesso e, in generale, di tracciamento delle informazioni che vengono trasmesse/ricevute su una rete di comunicazione pubblica (URL pixel tracking, local processing, tracciamento basato solo su IP, segnalazione intermittente e mediata da parte di dispositivi *IoT-Internet of Things*, sui sistemi di tracciamento e rilevamento delle informazioni tramite *unique identifier*, cioè il tracciamento e rilevamento dei dati personali c.d. persistenti quali il nome e cognome dell'utente, la sua email etc). Con l'avvertenza finale che le tecniche prese in considerazione dall'EDPB non costituiscono una lista esaustiva, dovendo l'operatore professionale comunque confrontarsi con la parte generale delle Linee guida per verificare

ISSN 2239-8570

se la tecnica di memorizzazione/accesso/tracciamento che intende adottare è conforme all'art. 5(3) della direttiva e-Privacy.

STEFANO BARTOLI

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en

2024/4(22)SB

22. Le Linee guida EDPB 1/2024 sottoposte a consultazione pubblica, sul trattamento dei dati personali basato sul legittimo interesse

L'8 ottobre 2024, il Comitato europeo per la protezione dei dati (**EDPB**) ha pubblicato per la consultazione pubblica la bozza di linee guida n. 1 del 2024 (le **Linee guida**) relative al trattamento dei dati personali fondato sul legittimo interesse di cui all'art. 6(1)(f) del Regolamento UE 2016/679 (**GDPR**). La pubblica consultazione si è chiusa il 20 novembre 2024.

Come noto, il legittimo interesse è una delle sei basi giuridiche previste dall'art. 6 del GDPR che rendono lecito il trattamento dei dati personali, le altre cinque essendo basate: sul consenso (art. 6(1)(a), GDPR); sulla necessità di adempiere un'obbligazione contrattuale (art. 6(1)(b), GDPR), o un dovere di legge (art. 6(1)(c), GDPR), o per salvaguardare gli interessi vitali dell'interessato o altra persona fisica (art. 6(1)(d), GDPR), oppure ancora per l'esecuzione di un compito legato all'esercizio di pubblici poteri (art. 6 (1)(e), GDPR).

La nozione di legittimo interesse non è nuova nell'ambito della normativa sul trattamento dei dati personali; già l'art. 7(f) della vecchia direttiva 95/46/CE "***relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*****" prevedeva, infatti, una disposizione analoga a quella oggi presente nel GDPR (l'art. 6(1)(f) del GDPR innova rispetto all'art. 7(f), Dir. 95/46/CE richiedendo una speciale cautela nel trattamento dei dati dei minori), e già il WP29 aveva pubblicato nel 2014 il Parere n. 6 "***sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE***" (di seguito **Opinion 6/2014**).

Come precisato dall'EDPB, le Linee guida non intendono discostarsi dall'Opinion 6/2014, quanto, piuttosto, aggiornarla alla luce non solo della nuova normativa introdotta dal GDPR ma anche della (copiosa) giurisprudenza formatasi negli ultimi anni ad opera della Corte di Giustizia dell'Unione europea (CGUE), ad es. nell'importante sentenza *Meta v. Bundeskartellamt* del 4 luglio 2023, C-252/21 (su cui v. in questa Rubrica la notizia n. 7 nel numero 3/2023 [2023/3(7)CAT] e *Atlante* p. 381).

In primo luogo, l'EDPB ricorda come il GDPR, nel disciplinare all'art. 6(1) le basi giuridiche per il trattamento dei dati personali, non crei alcuna

ISSN 2239-8570

gerarchia tra di esse e che, pertanto, il legittimo interesse non debba essere visto esclusivamente come una sorta di ultima risorsa per il caso in cui le altre basi giuridiche non fossero applicabili; allo stesso tempo, il ricorso al legittimo interesse non dovrebbe essere scelto dal titolare solo perché ritenuto meno stringente quanto a requisiti per rendere lecito il trattamento rispetto alle altre basi giuridiche.

Al fine di verificare se sussista o meno un legittimo interesse per il trattamento di dati personali le Linee guida indicano tre condizioni ("*three-step process*") che devono essere positivamente e cumulativamente soddisfatte. Qualora anche solo una delle tre condizioni non dovesse essere positivamente riscontrata, il titolare non potrà considerare come lecito ("*lawful*") il trattamento dei dati (almeno non sulla base giuridica relativa al legittimo interesse). Naturalmente, il triplice test dove essere condotto prima che il titolare proceda al trattamento dei dati e deve essere effettuato per ciascuna finalità per le quali il trattamento è richiesto, anche per ragioni di informativa all'interessato (art. 13 GDPR) che ha diritto di sapere quale base giuridica viene individuata (o quali basi giuridiche vengono individuate) dal titolare per il trattamento dei dati personali.

Le tre condizioni sono: 1) la sussistenza di un interesse che sia legittimo; 2) la necessità di trattare i dati sulla base dell'interesse legittimo; 3) l'esigenza che, dalla comparazione e dal bilanciamento degli interessi in gioco – da una parte l'interesse al trattamento, dall'altra parte i diritti fondamentali degli interessati – i diritti degli interessati non siano preminenti rispetto al trattamento (qualora il bisogno di tutela dei diritti degli interessati dovesse prevalere sull'interesse al trattamento, esso non potrà essere effettuato su tale base giuridica).

Quanto al primo requisito, cioè la natura legittima dell'interesse, salvo alcuni esempi richiamati ai Considerando 47 e 49, il GDPR non fornisce una puntuale definizione della legittimità dell'interesse perseguito dal titolare. Prendendo atto di ciò, le Linee guida richiamano a titolo di esempio casi già oggetto di scrutinio da parte della Corte di Giustizia (ad es. il caso *Google Spain*, C-131/12, sul diritto all'oblio e l'interesse all'accesso alle informazioni online, o il recente caso *SCHUFA Holding*, giudizi riuniti C-26/22 e C-64/22 in cui la Corte ha, tra le altre cose, riconosciuto come legittimo l'accesso ai dati di una persona per l'esame del merito c.d. creditizio) ma, soprattutto, delineano un ulteriore triplice test per la verifica della legittimità e anche in questo caso le tre condizioni devono tutte essere cumulativamente soddisfatte: 1) l'interesse deve essere lecito, quindi non contrario a norme eurounitarie o dei singoli diritti nazionali; 2) l'interesse deve essere chiaramente individuato perché solo nel momento in cui il titolare delinea in modo puntuale l'interesse che intende perseguire è anche in grado di effettuare il bilanciamento (essenziale) tra l'interesse stesso e i diritti degli interessati; 3) nel momento in cui il titolare pianifica il trattamento, l'interesse deve essere attuale e concreto e non, quindi, meramente ipotetico.

Il secondo e il terzo requisito, cioè quello attinente alla necessarietà del trattamento e quello relativo al bilanciamento dell'interesse del titolare con i diritti degli interessati, sono strettamente correlati. La necessità del

ISSN 2239-8570

trattamento, infatti, viene individuata quasi per sottrazione, dovendosi ritenere ottemperato il requisito della necessità quando, per eseguire il trattamento, il titolare non è in grado di individuare altre misure meno invasive dei diritti degli interessati tenuto conto dei principi applicabili al trattamento dei dati (art. 5 GDPR) e al principio di accountability (art. 25 GDPR). Infatti, proprio in tale contesto, il titolare deve essere in grado di dare conto e descrivere: 1) quali diritti ha preso in esame nella sua valutazione; 2) la valutazione relativa all'impatto del trattamento sugli interessati; 3) le ragionevoli aspettative degli interessati circa il trattamento (ad es. se si entra in banca è ragionevole aspettarsi l'esistenza di un sistema di videosorveglianza, mentre nessuno si aspetterà l'esistenza di videocamere in una sauna); 4) eventuali misure, ulteriori rispetto a quelle già da adottarsi in ottemperanza alle previsioni del GDPR, per mitigare l'impatto del trattamento sui diritti degli interessati.

STEFANO BARTOLI

https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

2024/4(23)BG

23. La dichiarazione dell'EDPB 5/2024 del 4.11.2024 sulle 42 raccomandazioni dell'High Level Expert Group istituito dalla Commissione Europea in materia di accesso ai dati personali per le attività di contrasto

Nel giugno 2023, è stato istituito, su impulso della Presidenza del Consiglio dell'Unione europea e della Commissione europea, l'High-Level Expert Group sull'Accesso ai Dati per un'Efficace Attività di Contrasto (**HLEG** o **Gruppo**) il cui obiettivo è stato analizzare le principali sfide poste dall'accesso ai dati da parte delle forze dell'ordine dell'Unione europea (**UE**), al fine di identificare potenziali soluzioni e raccomandazioni per superarle. L'HLEG si è concentrato su tre casi d'uso più critici e ricorrenti: accesso ai dati a riposo nei dispositivi degli utenti, accesso ai dati a riposo nel sistema di un fornitore di servizi e accesso in tempo reale ai dati di comunicazione, ciascuno dei quali è stato discusso in un gruppo di lavoro dedicato.

All'esito dell'analisi, nel giugno 2024, il Gruppo ha pubblicato 42 raccomandazioni per l'ulteriore sviluppo delle politiche e della normativa dell'UE (le **Raccomandazioni**). Le Raccomandazioni sono articolate in tre capitoli: *Capacity Building measures*, *Cooperation with Industry and Standardisation* e *Legislative measures*.

In sintesi, il documento identifica e analizza le difficoltà che le forze dell'ordine si trovano ad affrontare nell'accedere ai dati in un formato leggibile a causa: della mancanza di obblighi armonizzati di conservazione dei dati, dell'uso crescente della crittografia end-to-end e della mancanza di

ISSN 2239-8570

cooperazione da parte di alcuni servizi di telecomunicazione. Pur accogliendo con favore la normativa sulle prove elettroniche (il regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali, e la direttiva (UE) 2023/1544 recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali), le Raccomandazioni evidenziano i limiti di tale normativa nell'affrontare le sfide poste dalla crittografia e invocano conseguentemente una cooperazione più forte tra le autorità giudiziarie e le forze dell'ordine con i fornitori di servizi per favorire un dialogo permanente e una comprensione reciproca delle esigenze operative, tecniche e commerciali, e per superare le difficoltà nell'accesso ai dati crittografati.

Sebbene le Raccomandazioni non siano ancora operative, il Comitato europeo per la protezione dei dati personali (**EDPB**) ha ritenuto opportuno condividere delle considerazioni preliminari, sul rilievo che alcune delle Raccomandazioni potrebbero avere risvolti significativi sui diritti alla protezione dei dati personali e al rispetto della vita privata e familiare. Pertanto, il 4 novembre 2024 è stato adottato lo *Statement 5/2024 on the Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement* (la **Dichiarazione**).

Alla base della Dichiarazione vi è la considerazione che la rapida digitalizzazione di quasi tutti gli aspetti della vita pubblica e privata abbia dato origine ad un approfondito dibattito circa i limiti e le modalità di accesso ai dati elettronici per scopi di applicazione della legge e giustizia penale. In questo contesto, numerose voci di esperti di protezione dei dati e privacy si sono levate contro la concessione di poteri eccessivi alle forze dell'ordine, in quanto questi possono portare, di fatto, a una sorveglianza di massa della cittadinanza e pertanto interferire gravemente con il pieno godimento dei diritti fondamentali. Tale considerazione permea le intere Raccomandazioni ed è particolarmente presente nelle considerazioni relative alla conservazione dei dati e alla crittografia.

Con riguardo al primo tema, l'EDPB ha certamente accolto positivamente l'intenzione espressa nelle Raccomandazioni di stabilire un regime armonizzato dell'UE sulla conservazione dei dati, al fine di garantire uniformità e certezza del diritto per tutti gli stakeholder, in piena conformità con la giurisprudenza della Corte di Giustizia dell'Unione Europea (**CGUE**).

Tuttavia, l'EDPB ha parimenti condiviso preoccupazioni circa la raccomandazione di cui al punto 27(II) della sezione *Legislative measures* delle Raccomandazioni, laddove si suggerisce che l'ambito di applicazione di un futuro regime armonizzato sulla conservazione debba includere i "*data handlers*", ovvero i fornitori di servizi di qualsiasi tipo che potrebbero fornire accesso a prove elettroniche, presenti e futuri. Si rileva, difatti, come tale raccomandazione andrebbe ad ampliare il numero dei soggetti tenuti alla conservazione ben oltre quanto imporrebbe il rispetto del criterio di necessità e proporzionalità.

ISSN 2239-8570

A tale riguardo, si ricorda quanto dichiarato dalla CGUE, ossia che la conservazione generalizzata di tutti i dati di traffico è, in linea di principio, vietata e può essere giustificata solo sulla base della protezione della sicurezza nazionale, se lo Stato membro interessato si trova ad affrontare una grave minaccia alla sicurezza nazionale che può essere categorizzata come reale e attuale o prevedibile.

In questo contesto, l'EDPB ritiene che obbligo di conservazione dei dati in forma elettronica da parte di tutti i presenti e futuri *data handlers* estenderebbe l'ambito personale e materiale della conservazione dei dati oltre i limiti stabiliti nella giurisprudenza europea (sentenza della CGUE del 6 ottobre 2020, *La Quadrature du Net* e altri, cause riunite C-511/18, C-512/18 e C-520/18, punto 137), che deve essere interpretata in maniera restrittiva.

La Dichiarazione si sofferma in particolare sul c.d. Caso Hadopi (C-470/21) della CGUE, che di tale principio è esemplificativa. In tale sede, la Corte ha avuto modo di stabilire che gli Stati membri possono imporre agli *internet service provider* un obbligo di conservazione generalizzato e indifferenziato relativo agli indirizzi IP per ragioni di contrasto ai reati in generale, purché tale conservazione non consenta di trarre conclusioni precise sulla vita privata dell'interessato. Ciò può essere realizzato mediante modalità di conservazione che garantiscano una separazione effettivamente stagna degli indirizzi IP e delle altre categorie di dati personali, in particolare i dati relativi all'identità civile. Gli Stati membri possono inoltre, a determinate condizioni, autorizzare l'autorità nazionale competente ad accedere ai dati relativi all'identità civile riferentisi a indirizzi IP, purché sia assicurata una conservazione tale che garantisca una separazione stagna delle diverse categorie di dati. Allorché, in situazioni atipiche, le specificità di un procedimento nazionale che disciplina un accesso siffatto possono, per il fatto di mettere in relazione dati e informazioni raccolti, consentire di trarre conclusioni precise sulla vita privata dell'interessato, l'accesso deve essere assoggettato a un previo controllo da parte di un giudice o di un ente amministrativo indipendente.

A tal riguardo, l'EDPB insiste nel precisare che la valutazione espressa dalla CGUE, che giustifica la conservazione degli indirizzi IP, non può in alcun modo essere automaticamente estesa ad altri (più sensibili) dati di traffico e di localizzazione, che potrebbero facilmente consentire di creare un profilo dettagliato dell'utente.

Con riferimento al secondo macro-tema affrontato dalla Dichiarazione, l'EDPB prende posizione sui passaggi delle Raccomandazioni nei quali l'HLEG menziona la crittografia come una "sfida" in relazione alla necessità di consentire l'accesso ai dati. Questo tema è affrontato da diverse raccomandazioni specifiche, che coprono i casi d'uso dell'intercettazione delle comunicazioni, l'accesso ai dati sui dispositivi e nel contesto della fornitura di servizi.

Pur comprendendo l'importanza per le autorità di contrasto di avere possibilità tecniche per l'accesso legale a determinati dati, l'EDPB sottolinea ancora una volta che la crittografia è essenziale per garantire la sicurezza e la riservatezza dei dati personali e delle comunicazioni

ISSN 2239-8570

elettroniche, poiché fornisce forti garanzie tecniche contro l'accesso a tali informazioni da parte di chiunque non sia l'utente e i destinatari da questi scelti, inclusi i fornitori.

L'EDPB considera la protezione e l'efficacia della cifratura uno strumento fondamentale per evitare ripercussioni negative sul rispetto della vita privata e della riservatezza e per garantire che siano salvaguardate la libertà di espressione e la crescita economica, che dipendono da tecnologie affidabili. In particolare, nel contesto delle comunicazioni interpersonali, una reale crittografia end-to-end (**E2EE**) che protegge i dispositivi finali e i dati in essi contenuti con le chiavi di decrittazione detenute esclusivamente dagli utenti, è uno strumento cruciale per garantire la riservatezza delle comunicazioni elettroniche.

La Dichiarazione sottolinea pertanto che le raccomandazioni relative alla cifratura non dovrebbero in alcun modo impedirne l'uso né indebolire l'efficacia della protezione che questa fornisce.

Impedire l'uso della crittografia o indebolire l'efficacia della protezione che essa fornisce, avrebbe un grave impatto sul rispetto della vita privata e della riservatezza degli utenti, sulla loro libertà di espressione, nonché sull'innovazione e la crescita dell'economia digitale, che si basa sull'alto livello di fiducia che tali tecnologie offrono.

È cruciale notare che l'indebolimento della protezione fornita dalla crittografia può derivare da diverse misure tecniche che non si limitano all'introduzione di una "*backdoor*" all'interno del processo di crittografia stesso. Per valutare appieno l'indebolimento effettivo risultante dalle possibili misure, è necessario non solo accertare come viene influenzato il processo di crittografia, ma anche se le misure introdotte rendono nulle o indeboliscono significativamente le garanzie fornite dalla crittografia. Ad esempio, l'introduzione di un processo, lato "*client*", che consenta l'accesso remoto ai dati prima che siano crittografati e inviati su un canale di comunicazione, o dopo che siano stati decifrati presso il destinatario, in concreto indebolirebbe l'efficacia della crittografia.

In generale, è cruciale supportare qualsiasi raccomandazione che comporti l'uso di una soluzione tecnica con una valutazione della fattibilità pratica e della conformità di tale soluzione con gli obblighi di protezione dei dati e della privacy fin dalla progettazione e per impostazione predefinita. Come principio, l'EDPB osserva che qualsiasi requisito tecnico per i fornitori che abbia il potenziale di influenzare i diritti e le libertà fondamentali degli individui dovrebbe essere stabilito per legge, che rispetti l'essenza dei diritti e delle libertà fondamentali e sia ritenuto necessario e proporzionato in una società democratica.

Allo stesso tempo, l'EDPB riconosce la necessità di trovare il giusto equilibrio tra i diritti e gli interessi in gioco, per evitare, tra l'altro, l'effettiva impunità degli autori di determinati reati, soprattutto quelli commessi online, come recentemente sottolineato dalla stessa CGUE.

Pur sostenendo l'obiettivo di un'efficace attività di contrasto, l'EDPB esprime dubbi sul fatto che tutte le misure suggerite dal Gruppo siano conformi alla Carta dei diritti fondamentali dell'UE (**CDFUE**), in particolare i diritti alla protezione dei dati personali (art. 8 CDFUE) e al

ISSN 2239-8570

rispetto della vita privata e familiare (art. 7 CDFUE), dato il loro potenziale grave carattere intrusivo. Pertanto, l'EDPB invita la Commissione e gli Stati membri a valutare la fattibilità giuridica delle Raccomandazioni con la dovuta diligenza e nel pieno rispetto delle norme sulla protezione dei dati e sulla privacy.

BEATRICE GALLUCCI

https://www.edpb.europa.eu/news/news/2024/edpb-adopts-its-first-report-under-eu-us-data-privacy-framework-and-statement_it

https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-52024-recommendations-high-level-group-access_it

2024/04(24)EB

24. Il parere EDPB 22/2024 del 7.10.2024 sugli obblighi dei titolari del trattamento di dati personali in conseguenza di incarichi affidati a responsabili e sub-responsabili ex art. 28 GDPR

Il 7 ottobre 2024 il Comitato europeo per la protezione dei dati (**EDPB** o **Comitato**) ha pubblicato l'Opinion 22/2024 circa determinati obblighi dei titolari del trattamento di dati personali conseguenti all'affidamento da essi riposto sull'operato dei responsabili e dei sub-responsabili del trattamento nominati ai sensi dell'art. 28 del regolamento (UE) 2016/679 (**GDPR**).

L'Opinion è stata pubblicata a seguito di una richiesta ai sensi dell'art. 64(2) GDPR da parte dell'Autorità danese per la protezione dei dati personali. L'articolo 64(2) GDPR prevede, infatti, che qualsiasi autorità di protezione dei dati possa chiedere al Comitato di emettere un parere su questioni di applicazione generale o che producono effetti in più di uno Stato membro.

Nel caso di specie sono stati posti diversi quesiti all'EDPB circa l'interpretazione degli articoli 24 e 28 GDPR, ossia la precisazione degli obblighi normativi in capo a un titolare del trattamento ex artt. 4 n. 7) e 24 del GDPR nell'ipotesi di affidamento di un incarico nei confronti di un responsabile (o sub-responsabile) del trattamento.

In particolare, il Garante danese ha formulato i seguenti quesiti:

Quesito 1.1: Considerando gli articoli 5(2) e 24(1) del GDPR, il titolare del trattamento, quando si avvale di un responsabile, deve documentare la conformità agli articoli 28(1) e 28(2) GDPR, nello specifico:

a. Il titolare deve identificare tutti i sub-responsabili lungo tutta la catena di trattamento o solo la prima linea di sub-responsabili?

b. In quale misura e dettaglio il titolare deve verificare e documentare:

i. la sufficienza delle garanzie offerte dai responsabili e sub-responsabili;

ISSN 2239-8570

ii. il contenuto dei contratti tra il Responsabile iniziale e i sub-responsabili per accertare che siano state imposte le stesse obbligazioni previste dall'articolo 28(4) del GDPR;

iii. se i responsabili e sub-responsabili presentino le garanzie sufficienti al trattamento indicate dal Titolare secondo l'articolo 28(1).

Quesito 1.2: In caso di trasferimenti o ulteriori trasferimenti di dati da un (sub-)responsabile a un altro, in conformità con le istruzioni del titolare, in che misura il titolare deve, ai sensi dell'articolo 28(1) in combinato disposto con l'articolo 44, valutare e dimostrare attraverso la documentazione che il livello di protezione dei dati personali non sia compromesso dai trasferimenti successivi?

Quesito 1.3: L'estensione degli obblighi ai sensi degli articoli 28(1) e 28(2) del GDPR, letti in combinato disposto agli articoli 5(2) e 24 GDPR, varia in base al rischio associato all'attività di trattamento? Se sì, qual è l'entità di tali obblighi per le attività a basso rischio e per quelle ad alto rischio?

Quesito 2: Un contratto o altro atto giuridico di nomina ai sensi dell'articolo 28(3) del GDPR deve contenere l'eccezione prevista dall'articolo 28(3)(a) ("*salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento*") per essere conforme al GDPR?

Quesito 2a: Se la risposta al quesito 2 è negativa, un contratto o atto giuridico che amplia l'eccezione dell'articolo 28(3)(a) per includere anche l'eventualità di un ordine governativo di uno stato terzo o la legge di un paese terzo, costituisce di per sé una violazione dell'articolo 28(3)(a) del GDPR?

Quesito 2b: Se la risposta al quesito 2a fosse negativa, tale eccezione ampliata dovrebbe invece essere interpretata come un'istruzione documentata del titolare ai sensi dell'articolo 28(3)(a) del GDPR?

L'EDPB è stata, dunque, chiamata a pronunciarsi circa i doveri concreti di titolari e responsabili nel garantire la compliance al GDPR, in contesti, sempre meno rari, in cui la catena di sub-responsabili sfugge totalmente al controllo del titolare che tuttavia resta il primo garante della *compliance* di fronte alle autorità di controllo e agli interessati.

Il Comitato ha chiarito come i titolari del trattamento dovrebbero avere sempre a disposizione le informazioni sull'identità (ovvero nome, indirizzo, punto di contatto) di tutti i responsabili e sub-responsabili del trattamento, in modo da poter adempiere ai propri obblighi ai sensi dell'articolo 28 del GDPR. A tal fine, è compito del responsabile del trattamento fornire proattivamente al titolare tutte le informazioni circa i sub-responsabili e mantenerle sempre aggiornate. Questo, sia nel caso in cui il Titolare abbia concesso un'autorizzazione generale al ricorso a sub-responsabili, che nel caso in cui l'autorizzazione sia speciale e quindi *ad hoc*.

Il titolare, dunque, deve sempre avere a disposizione un elenco aggiornato di responsabili e sub-responsabili, ciò, non solo in virtù del fatto che, sebbene la catena di trattamento possa essere piuttosto lunga, il titolare mantiene il ruolo centrale nella determinazione delle finalità e dei mezzi del

ISSN 2239-8570

trattamento (EDPB Guidelines 07/2020, par. 152); ma anche in virtù di altre norme del GDPR che giustificano la necessità per il titolare di identificare tutti i soggetti coinvolti nel trattamento (articoli 13(1)(e), 15 e 19 GDPR).

Fatta questa premessa, l'EDPB ribadisce che, per quanto concerne l'assunzione di eventuali ed ulteriori sub-responsabili del trattamento da parte del responsabile del trattamento cd. iniziale, è necessaria la previa autorizzazione scritta, specifica o generale, da parte del titolare del trattamento.

In caso di **autorizzazione speciale**, il titolare del trattamento deve indicare, appunto, quale sub-responsabile del trattamento è autorizzato, per quale specifica attività di trattamento e per quanto tempo, nonché deve fornire una serie di criteri volti a orientare la scelta del responsabile del trattamento (es. garanzie in termini di misure di sicurezza tecniche ed organizzative; conoscenze specialistiche; affidabilità; risorse).

In caso di **autorizzazione generale**, il responsabile del trattamento deve dare al titolare l'opportunità di approvare un elenco di sub-responsabili del trattamento, al momento della firma della cd. autorizzazione generale, assegnando, al contempo, un congruo lasso di tempo per opporsi a qualsiasi modifica successiva dei sub-responsabili del trattamento.

Nella scelta dei soggetti da nominare quali responsabili o sub-responsabili l'articolo 28(1) del GDPR stabilisce che i titolari del trattamento hanno l'obbligo di avvalersi di soggetti che forniscano "*garanzie sufficienti*" per implementare misure "*adeguate*" in modo che il trattamento soddisfi i requisiti del GDPR e garantisca la protezione dei diritti degli interessati. Il punto è di difficile interpretazione, a causa della vaghezza delle c.d. garanzie sufficienti e soprattutto alle modalità di verifica più adeguate.

L' occasione è quindi gradita all'EDPB, che nell'Opinione si rivolge alle autorità di controllo nazionali, le quali nel valutare l'accountability dei titolari (articolo 24(1) GDPR) all'articolo 28(1) GDPR, dovrebbero verificare che il coinvolgimento di responsabili e sub-responsabili non comporti una riduzione del livello di protezione dei diritti e delle libertà degli interessati.

Difatti, l'obbligo del titolare di verificare se i (sub) responsabili offrano "garanzie sufficienti" per implementare le misure adeguate dovrebbe valutarsi in astratto e applicarsi indipendentemente dal rischio concreto per i diritti e le libertà degli interessati correlato al trattamento affidato a questi.

Circa la valutazione del livello di adeguatezza delle garanzie offerte, l'EDPB svincola la stessa dal rischio, tuttavia questo può fungere da criterio orientativo. Difatti, per trattamenti che presentano un alto rischio per i diritti e le libertà degli interessati, si dovrebbe aumentare il grado di verifica delle informazioni fornite e viceversa.

L'EDPB specifica ulteriormente nell'Opinione che, sebbene il responsabile iniziale debba assicurarsi di proporre sub-responsabili che offrano garanzie sufficienti, la decisione finale di nominare un sub-responsabile specifico e la relativa responsabilità, compresa la verifica delle garanzie, rimangono in capo al titolare. Questi può scegliere di fare affidamento sulle informazioni ricevute dal suo responsabile e ampliarle se

ISSN 2239-8570

necessario (ad esempio, se sembrano incomplete, imprecise o sollevano dubbi). Viene precisato comunque che, ai sensi del GDPR, il titolare non ha l'obbligo di richiedere sistematicamente i contratti di sub-trattamento per verificare se le obbligazioni in materia di protezione dei dati previste nel contratto iniziale siano state trasferite lungo la catena di trattamento. Bensì, il titolare dovrebbe valutare caso per caso se richiedere una copia di tali contratti o esaminarli in seguito ai sensi del principio di *accountability*.

Venendo ora ai quesiti circa il trasferimento dei dati all'estero, l'EDPB chiarisce che quando i trasferimenti di dati personali al di fuori dello Spazio Economico Europeo (SEE) avvengono tra due (sub) responsabili del trattamento, in conformità con le istruzioni del Titolare, quest'ultimo rimane soggetto agli obblighi derivanti dall'articolo 28(1) GDPR sulle "garanzie sufficienti", oltre a quelli previsti dall'articolo 44 GDPR, per garantire che il livello di protezione assicurato dal GDPR non venga compromesso dai trasferimenti di dati personali. A tal proposito, è il responsabile/esportatore che deve fornire al Titolare la documentazione che provi il rispetto del GDPR nei trasferimenti all'estero, come precisato anche nella Raccomandazione 01/2020 dell'EDPB. Il titolare deve valutare tutto quanto fornito dal Responsabile ed eventualmente chiederne una integrazione ai fini della *compliance*. Quanto alla possibilità per il titolare di sindacare circa le modalità e/o l'opportunità del trasferimento di dati all'estero, l'EDPB non si esprime con chiarezza, ma genericamente asserisce che tale l'estensione di tale potere cambia al variare della base giuridica utilizzata per il trasferimento e alla circostanza per cui il trasferimento sia iniziale o successivo (c.d *onward transfer*).

L'EDPB ha anche affrontato, nell'Opinione, la questione relativa alla formulazione utilizzata nei contratti tra titolari e responsabili del trattamento. A tal proposito, ha formato oggetto dei quesiti dell'Autorità danese il caso in cui il responsabile tratti i dati ai sensi del diritto di uno Stato membro cui è soggetto (articolo 28(3)(a) GDPR), ricordando il principio generale che i contratti non possono derogare alla legge.

Alla luce della libertà contrattuale concessa alle parti di adattare il contratto titolare-responsabile alle loro circostanze, entro i limiti dell'articolo 28(3) GDPR, l'EDPB ritiene che includere la frase " *salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento*" sia fortemente raccomandato ma non obbligatorio.

Tuttavia, l'EDPB chiarisce come l'inserimento di una tale clausola non esonera il responsabile dal rispettare i suoi obblighi ai sensi del GDPR.

Ad esempio, nel caso di trasferimento di dati all'estero, l'EDPB ritiene improbabile che la formulazione " *salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento* ", sia di per sé sufficiente a garantire la conformità con l'articolo 28(3)(a) GDPR in combinazione con il Capo V del GDPR. Come illustrato dalle SCC e dalle raccomandazioni BCR-C della Commissione Europea, l'articolo 28(3)(a) del GDPR non impedisce, in linea di principio, l'inclusione nel contratto di disposizioni che legittimano il trasferimento di dati all'estero sulla base di norme di legge di paesi terzi, ma ciò non consente comunque il

ISSN 2239-8570

trasferimento verso paesi che non offrano un adeguato livello di protezione ai sensi del GDPR.

A tal riguardo, l'EDPB raccomanda che nei rapporti tra titolare e responsabile o tra responsabile e sub-responsabile sia attentamente considerata anche la possibilità che il rinvio nel contratto a leggi di un paese terzo in grado di compromettere o ostacolare la conformità al GDPR.

Infine, per rispondere al Quesito 2b, l'EDPB chiarisce che far seguire all'impegno del responsabile di trattare i dati solo su istruzioni documentate del Titolare la frase "*a meno che non sia richiesto dalla legge o da un ordine vincolante di un ente governativo*" (testualmente o in termini molto simili) non possa essere interpretato come un'istruzione documentata da parte dello stesso titolare del trattamento.

Alla luce della disamina sopra proposta, appare evidente come l'Opinion 22/2024 apra più interrogativi di quanti ne risolva. Alcuni capisaldi che però si possono trarre dalle indicazioni dell'EDPB concernono il ruolo del titolare, il quale resta soggetto ad una responsabilità superiore rispetto a quella di tutti gli altri soggetti coinvolti - per suo conto - lungo la catena di trattamento.

Tale impostazione, tuttavia, è di difficile declinazione nella pratica per diversi ordini di ragioni:

i. la catena di trattamento può essere anche molto lunga e articolata;

ii. frequentemente i responsabili ovvero i sub-responsabili sono scelti tra colossi dell'informatica e tra fornitori da cui è quasi impossibile pretendere trasparenza e riuscire in concreto ad orientare le modalità di trattamento.

EMANUELA BURGIO

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_it

2024/4(25)CS

25. La dichiarazione EDPB 4/2024 del 7.10.2024 sulle modifiche alla proposta di regolamento che stabilisce ulteriori norme procedurali per l'applicazione del GDPR

Il 7 ottobre 2024 il Comitato europeo per la protezione dei dati personali (**EDPB** o **Comitato**) ha adottato la dichiarazione 4/2024 (la **Dichiarazione**) sugli emendamenti alla proposta di regolamento che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679, presentata dalla Commissione europea il 4 luglio 2023 (COM(2023) 348 final) (la **Proposta**). Più in particolare, il Comitato si esprime sulle posizioni dei due colegislatori contenute negli Emendamenti del Parlamento in prima lettura del 10 aprile 2024 e nell'Approccio generale 11214/24 del 13 giugno 2024 del Consiglio (le **Posizioni**).

ISSN 2239-8570

Il testo della Proposta, peraltro, era già stato oggetto di valutazione nel Parere congiunto dell'EDPB e dell'EDPS del 19 settembre 2023 (n. 1/2023) (il **Parere congiunto**).

La Proposta intende rimediare ad alcune complicazioni applicative del regolamento (UE) 2016/679 (**GDPR**) emerse dopo la sua entrata in vigore e derivanti dalla varietà delle norme procedimentali nazionali con le quali le singole Autorità esercitano i compiti e i poteri loro attribuiti dal GDPR. Termini e procedimenti decisori diversi sono risultati essere di ostacolo ad un'efficiente cooperazione tra le diverse Autorità nazionali. La cooperazione è indispensabile per la coerente ed uniforme applicazione del GDPR, in particolare per i «trattamenti transfrontalieri», nei quali cioè il trattamento avviene nell'ambito di attività svolte in stabilimenti collocati in più Stati membri oppure in un unico Stato ma incidendo in modo sostanziale sugli interessati di più Stati membri. La necessità di garantire decisioni uniformi e condivise tra le Autorità interessate, e contemporaneamente di consentire al titolare o al responsabile del trattamento di interloquire con un'unica Autorità in un procedimento che li riguarda, è garantita dal GDPR attraverso il meccanismo di applicazione decentrata del c.d. di «sportello unico». Esso prevede che l'Autorità dello stabilimento principale o unico assuma le funzioni di «**Autorità capofila**» competente, tra l'altro, a trattare i reclami proposti e ad esercitare i diversi poteri ispettivi, autorizzativi, sanzionatori, ecc. Essa, però, deve decidere cooperando con le altre Autorità interessate, con l'obiettivo di ottenere una posizione condivisa sulla questione (art. 60 GDPR). Nel caso di contrasto tra le posizioni, che segua la presentazione da parte di un'Autorità di un'«obiezione pertinente e motivata» al progetto di decisione di quella capofila o una disputa di competenza, la questione controversa è sottoposta al procedimento di composizione delle controversie da parte dell'EDPB, il quale adotta una decisione vincolante per l'Autorità capofila e per tutte le Autorità interessate, nell'ambito del meccanismo di coerenza (artt. 63 e 65 GDPR).

La Proposta, con l'obiettivo di uniformare i procedimenti amministrativi e disciplinare più analiticamente fasi e termini del meccanismo di coerenza e della composizione delle controversie, ha presentato integrazioni alla scarna procedura del GDPR. Sono state previste norme procedurali uniformi in tema di forma e contenuto dei reclami, di indagini delle Autorità nell'applicazione transfrontaliera del GDPR, di diritti procedurali. Sono state altresì puntualizzate le norme relative alle obiezioni pertinenti e motivate ai progetti di decisione della capofila e le fasi e i termini della procedura di cooperazione e composizione delle controversie tra Autorità dinnanzi all'EDPB.

In via generale, la Dichiarazione accoglie con favore gli emendamenti alla Proposta apportati delle suddette Posizioni di Parlamento e Consiglio. Sono però auspicate ulteriori modifiche su alcuni profili.

- Quanto agli atti del procedimento del procedimento l'EDPB apprezza l'emendamento volto a chiarire il concetto di reclamo quale segnalazione avente ad oggetto la richiesta di tutela dei propri diritti. Una particolare attenzione è dedicata all'emendamento introduttivo del «fascicolo comune» elettronico, contenente tutti i documenti pertinenti del

ISSN 2239-8570

caso, comprese tutte le informazioni interne o riservate, nonché una traduzione di tutti i documenti nella lingua di cooperazione. Lo strumento, però, pur ritenuto astrattamente utile per facilitare la condivisione di informazioni tra le Autorità, secondo il Comitato richiederebbe complesse modifiche ai sistemi di gestione dei documenti e di comunicazione utilizzati a livello nazionale ed europeo. Una particolare preoccupazione è espressa anche in relazione alla circostanza che se si dovesse consentire alle parti di accedere a tale fascicolo in qualsiasi momento, ciò potrebbe aumentare il numero dei ricorsi contro le decisioni delle Autorità e le probabilità di *data breaches*. Secondo l'EDPB, poi, il nuovo regolamento non dovrebbe imporre particolari regole per le traduzioni dei documenti, e suggerisce di eliminare l'apposita disposizione della Proposta sul punto. Al di là di tutto ciò, il Comitato ribadisce l'importanza di garantire il diritto di accesso del reclamante ai documenti non riservati, e di rendere inaccessibili alle parti le informazioni riservate o contenenti segreti commerciali.

- Alcune osservazioni sono svolte in relazione agli emendamenti relativi a fasi del procedimento. Nella fase di c.d. verifica preliminare, l'Autorità a cui è presentato il reclamo stabilisce se esso riguardi un trattamento transfrontaliero e ne verifica l'ammissibilità. L'EDPB apprezza gli emendamenti volti ad attribuire a tale Autorità il potere di decidere in via preliminare quale sia l'Autorità capofila e a chiarire che la valutazione di ammissibilità del reclamo da essa effettuata è vincolante per l'Autorità capofila. È apprezzato altresì l'emendamento volto a consentire che, prima dell'eventuale trasmissione del reclamo alla capofila, l'Autorità a cui esso è presentato possa ritenere che titolare o responsabile abbiano affrontato debitamente la presunta violazione del GDPR e che la richiesta del reclamante sia stata trattata in modo soddisfacente. Questo consentirebbe di risolve rapidamente il caso nella fase iniziale. In riferimento alla fase di «composizione amichevole del reclamo» introdotta con la Proposta, l'EDPB ritiene necessario aggiungere una previsione che renda possibile in ogni momento, ed effettuabile in ogni Stato membro con procedure uniformi, tale composizione conciliata tra le parti (interessato e soggetto che si presume abbia violato il GDPR). Alle Autorità dovrebbe essere assegnato un ruolo attivo e facilitatore a riguardo, fermo restando che l'accertamento della definizione conciliata della questione dovrebbe pur sempre essere oggetto di una decisione dell'Autorità capofila. Secondo l'EDPB, di contro, non sarebbe opportuno imporre che le parti raggiungano un accordo «esplicito», in quanto nella sua esperienza non è raro che ad un certo punto il reclamante smetta di interloquire con le Autorità: simili ipotesi renderebbero complesso accertare la definizione del procedimento, salva l'introduzione di una disciplina del silenzio- assenso del reclamante in relazione alla conclusione dell'accordo conciliativo.

- La proposta di nuove norme procedurali sulla cooperazione rafforzata prevede che l'Autorità capofila, già una volta formatasi un'opinione preliminare sulle questioni principali, rediga un documento di «sintesi delle questioni chiave» sul quale le Autorità interessate possono formulare osservazioni. L'EDPB ritiene che gli emendamenti sul punto,

ISSN 2239-8570

introduttivi di un obbligo di aggiornamento di tale sintesi all'avanzare della procedura per riflettere eventuali cambiamenti fattuali o giuridici, potrebbero generare incertezza giuridica e complicare l'attività delle Autorità. È, invece, ben accolta la modifica volta ad estendere a tutte le Autorità interessate la possibilità di attivare la procedura di urgenza davanti all'EDPB in caso di disaccordo sulle questioni chiave basate sui reclami. La nuova disciplina analitica delle «obiezioni pertinenti e motivate», pur emendata dalle Posizioni dei colegislatori, non riceve l'apprezzamento del Comitato, il quale auspica l'eliminazione della relativa disposizione. Le perplessità si appuntano, in particolare, sulla limitata possibilità di sollevare le obiezioni solo sugli elementi menzionati nel progetto di decisione e non su tutti gli elementi di fatto e di diritto del fascicolo. Peraltro, secondo l'EDPB, la possibilità di sollevare obiezioni dovrebbe essere estesa anche ai progetti di decisione *sui generis*, ossia quelli che danno atto degli accordi raggiunti in sede di composizione amichevole del reclamo.

- La cooperazione tra Autorità è analiticamente regolamentata dalla Proposta con riguardo ad attività, fasi e termini richiesti per raggiungere un consenso sulla decisione da adottare. L'EDPB accoglie con favore gli emendamenti che introducono la possibilità per la capofila di non applicare le nuove norme per la cooperazione rafforzata in determinati casi più semplici e fanno salva la possibilità per le altre Autorità interessate di opporvisi. Una tale opportunità (di c.d. «Opt-out» dall'applicazione del Capo III della Proposta) è ritenuta utile per la flessibilità delle azioni delle Autorità. Anche l'introduzione di termini procedimentali è favorevolmente accolta dall'EDPB, sebbene l'auspicio sia per una loro definizione con realismo e garanzia di flessibilità in relazione alla complessità dei casi. Di contro, sono sollevate obiezioni agli emendamenti che, a determinate condizioni, consentirebbero esplicitamente ad ogni Autorità interessata di richiedere a quella capofila di procedere d'ufficio alla valutazione di presunte violazioni del GDPR. Per il Comitato, ciò non aggiungerebbe nulla a quanto già possibile ottenere con una cooperazione «sincera ed effettiva» tra le autorità di vigilanza. Ulteriori riserve riguardano la modifica introduttiva di una disposizione che chiama l'EDPB ad adottare decisioni su questioni procedurali che vedono contrapporsi le Autorità («determinazioni procedurali»). Il Comitato esprime la preoccupazione che una tale previsione possa aumentare in numero delle procedure di urgenza e incrementare il carico di impegni dell'EDPB. A suo avviso, il ricorso a determinazioni procedurali dovrebbe essere concepito solo come ultima *ratio*, mentre si dovrebbe garantire che le Autorità si sforzino innanzitutto di trovare un accordo tra loro. Quanto alla disciplina per le procedure di urgenza, l'EDPB esprime un particolare apprezzamento della modifica che elimina le restrizioni sulla portata geografica delle misure finali e stabilisce che le decisioni vincolanti ed urgenti indirizzate alla capofila e a tutte le Autorità interessate specifichino le Autorità competenti ad adottare le misure definitive. Viene ancora ribadita la raccomandazione già espressa nel Parere congiunto affinché si preveda che l'EDPB possa ordinare ad

ISSN 2239-8570

un'Autorità di imporre misure diverse o aggiuntive rispetto a quelle richieste.

- Un particolare giudizio è espresso con riferimento a diritti relativi al procedimento. Il diritto a un ricorso giurisdizionale effettivo nei confronti di un'Autorità di controllo, previsto da un emendamento introduttivo di una nuova apposita disposizione, verrebbe riconosciuto a ciascuna parte nelle ipotesi in cui: a) l'Autorità ricevente un reclamo non eserciti i propri poteri per garantire che un'altra Autorità prosegua la procedura; b) un'Autorità capofila non rispetti i termini previsti dal GDPR o dalla nuova regolamentazione; c) un'Autorità non si conformi ad una decisione vincolante dell'EDPB. Il Comitato argomenta, però, che il diritto a un ricorso giurisdizionale effettivo è già tutelato dall'art. 78 del GDPR e che, in ogni caso, occorra chiarire adeguatamente i presupposti del diritto disciplinato con l'emendamento *de quo*. Anche un nuovo articolo su un generale diritto ad essere ascoltati nella procedura di risoluzione della controversia è ritenuto essere poco utile a soddisfare la vera esigenza di regolamentare in modo particolare tale diritto in relazione ai diversi momenti della procedura. Ancora inutile è reputato incaricare l'EDPB di valutare, prima di richiedere all'Autorità capofila di modificare il proprio progetto di decisione, se gli elementi sui quali esso intende fondare il proprio provvedimento siano stati oggetto del diritto delle parti di essere ascoltate. L'EDPB rileva che siffatta valutazione è già nella sua competenza nella fase iniziale. Anche la previsione di un suo obbligo di fornire alle parti una previa motivazione della propria decisione, nel caso in cui verifichi che esse non abbiano avuto in precedenza la possibilità di esprimersi sui punti considerati, è reputato poco utile. Un tale obbligo, oltre ad imporre all'EDPB incombenze procedimentali potenzialmente non sostenibili, risulterebbe meno efficace della previsione attuale, che richiede che le parti debbano potersi esprimere prima che la controversia giunga al Comitato. Viene suggerito, di contro, di strutturare le eventuali forme della propria interlocuzione con le parti, sostituendo l'obbligo di motivare loro l'emananda decisione con quello del loro ascolto sugli elementi sui quali il Comitato intende basarsi per decidere e sui quali esse non hanno ancora avuto la possibilità di esprimersi.

Infine, l'EDPB sottolinea l'importanza di disciplinare forme di cooperazione tra il Comitato e le Autorità di controllo nazionali anche oltre i casi transfrontalieri, invitando i colegislatori ad introdurre meccanismi in tal senso.

CARLA SOLINAS

https://www.edpb.europa.eu/system/files/2024-10/edpb_statement_20241007_additionalproceduralrulesgdprenforcement_en_0.pdf

2024/4(26)SO

ISSN 2239-8570

26. Il parere EDPB 28/2024 del 17.12.2024 su certi aspetti della protezione dei dati relativi al trattamento dei dati personali nel contesto di modelli di IA

Con parere 28/2024 adottato il 17 dicembre 2024 (il **Parere**), il Comitato europeo per la protezione dei dati (**EDPB**), rispondendo ad una richiesta dell'Autorità di controllo irlandese del 4.9.2024 (la **Richiesta**) ai sensi dell'art. 64(2) del regolamento (UE) 2016/679 (**GDPR**), ha affrontato alcune questioni inerenti al trattamento dei dati personali nel contesto di '**modelli di IA**'.

Con questa espressione ('modelli di IA'), l'EDPB ha precisato di voler riferirsi nel Parere, in conformità alla Richiesta, ad una nozione che non trova una definizione o un riscontro diretto nel regolamento (UE) 2024/1689 (**AI Act**), e di riferirsi in particolare alla nozione di cui a p. 3 della Richiesta, ossia «il prodotto risultante dai meccanismi di addestramento che sono applicati a un set di dati di addestramento, nel contesto di Intelligenza Artificiale, Machine Learning, Deep Learning o altri contesti di trattamento correlati» … «il termine si applica sia a Modelli di IA che sono destinati ad essere assoggettati ad ulteriore addestramento, perfezionamento e sviluppo che a Modelli di IA che non lo sono» ("*'the product resulting from the training mechanisms that are applied to a set of training data, in the context of Artificial Intelligence, Machine Learning, Deep Learning or other related processing contexts' and further specifies that 'The term applies to AI Models which are intended to undergo further training, fine-tuning and/or development, as well as AI Models which are not.*'") (p. 12 del Parere).

In particolare, il Parere ha affrontato i seguenti quattro quesiti contenuti nella Richiesta:

(1) in quali circostanze un modello di IA può considerarsi 'anonimo';

(2) in che modo i titolari dei trattamenti di dati personali possono dimostrare l'appropriatezza del legittimo interesse come base giuridica per la fase dello sviluppo di modelli di IA;

(3) stessa domanda sub (2) relativamente alla fase dell'uso (deployment) di modelli di IA; e

(4) quali conseguenze comporta un trattamento illecito di dati personali nella fase dello sviluppo di un modello di IA sulle conseguenti operazioni di trattamento o funzionamento del modello di IA.

Con riferimento **alla prima domanda**, il Parere che le autodichiarazioni di anonimità di modelli di IA devono essere verificate dalle competenti autorità di controllo per la protezione dei dati personali caso per caso, in quanto l'EDPB ritiene che i modelli di IA addestrati con dati personali non possono in tutti i casi considerarsi anonimi. Nel Parere si soggiunge che, affinché un modello di IA possa essere considerato anonimo deve condursi un'analisi specifica che tenga conto di tutti i mezzi ragionevolmente impiegabili da parte del titolare del trattamento o da altri e da tale analisi deve risultare come non significativa sia (1) la probabilità di una estrazione diretta (compresa una estrazione su base probabilistica) di dati personali che riguardano persone i cui dati personali sono stati usati per sviluppare il modello di IA, che (2) la probabilità di ottenere, intenzionalmente o meno,

ISSN 2239-8570

dati personali da domande. Per il concetto di probabilità non significativa il Parere rimanda in nota a due sentenze della CGUE (19 ottobre 2016, causa C-582/14, *Breyer v Bundesrepublik Deutschland*, paragrafo 46, e 7 marzo 2024, causa C-479/22 P, *OC v European Commission*, paragrafo 51). Si specifica inoltre che, nel loro accertamento, le autorità di controllo per la protezione dei dati personali devono esaminare la documentazione fornita dal titolare del trattamento al fine di dimostrare l'anonimità del modello di IA. A tal fine, nel Parere si fornisce un elenco (non esaustivo e non prescrittivo) di metodi che possono essere utilizzati dai titolari del trattamento nella loro dimostrazione dell'anonimità del modello di IA (pp. 17-19 del Parere).

Con riferimento **alla seconda e alla terza domanda**, nel Parere, dopo aver rammentato che nel GDPR non c'è una gerarchia tra le varie basi giuridiche per il trattamento dei dati personali, si ricorda il triplice test inerente alla base del legittimo interesse, ossia: *(i)* identificare il legittimo interesse perseguito dal titolare del trattamento o da un terzo; *(ii)* analizzare la necessità del trattamento ai fini del legittimo interesse (c.d. test della necessarietà); *(iii)* accertare se il legittimo interesse non sia da ritenersi recessivo rispetto ad interessi o diritti fondamentali o libertà degli interessati (c.d. test del bilanciamento).

Quanto al primo gradino del test, relativo all'identificazione del legittimo interesse, si ricorda che un interesse può ritenersi legittimo per il fine considerato solo se tutti e tre i seguenti requisiti sono soddisfatti: *a)* è lecito; *b)* è formulato in modo chiaro e preciso; *c)* è reale ed attuale (non ipotetico ed astratto).

Ad esempio, tale interesse può comprendere il miglioramento di funzioni di rilevamento di minacce ad un sistema informatico nello sviluppo di un modello di IA, nello sviluppo o nell'uso di un servizio di chatbot che conversa con gli utenti.

Quanto al secondo gradino del test (sulla necessarietà) il Parere ricorda che il relativo accertamento richiede di considerare se il trattamento consente di perseguire il legittimo interesse, e, in caso affermativo, se c'è un modo meno invadente di perseguirlo. Relativamente a questa parte del test, si ricorda che è necessario considerare la quantità dei dati personali trattati e se il trattamento possa ritenersi proporzionato al perseguimento dell'interesse anche alla luce del principio di minimizzazione.

Quanto al terzo gradino del test (bilanciamento), il Parere, dopo aver ricordato che l'accertamento va condotto sulla base dell'analisi delle circostanze del caso concreto, fornisce una rassegna degli elementi che le autorità di controllo possono prendere in considerazione ai fini del bilanciamento, evidenziando gli specifici rischi per i diritti fondamentali, che possono emergere nello sviluppo o uso di modelli di IA. Nel Parere si specifica che il trattamento dei dati personali relativo a queste fasi può avere un impatto di vario tipo sugli interessati, non solo di segno negativo ma anche eventualmente di segno positivo, e che, nel valutare tale impatto, le autorità di controllo possono considerare la natura dei dati personali, il contesto del trattamento e le possibili ulteriori conseguenze del trattamento. Si aggiunge che vanno valutate anche le ragionevoli aspettative degli

ISSN 2239-8570

interessati, e che, in relazione a questo aspetto, bisogna considerare, anche ai fini dell'informativa da fornire agli interessati, il fatto che per gli interessati – anche avuto riguardo alla complessità delle tecnologie usate nei modelli di IA - può essere difficile comprendere la varietà degli usi potenziali dei modelli di IA e le diverse attività di trattamento implicate. In relazione a questo aspetto, il Parere specifica che sia l'informativa fornita agli interessati che il contesto del trattamento possono essere tra gli elementi da considerare per valutare le ragionevoli aspettative di trattamento da parte degli interessati. L'analisi sul contesto, secondo il Parere, può comprendere domande del tipo: se i dati personali erano o non erano pubblicamente disponibili, la natura della relazione tra l'interessato e il titolare del trattamento, la natura del servizio, il contesto nel quale i dati perosnali sono stati raccolti, la fonte dai quali sono stati raccolti (ad esempio il sito web o il servizio dove i dati personali sono stati raccolti e le specifiche privacy offerte), i potenziali usi ulteriori del modello di IA, e se gli interessati sono effettivamente consapevoli che i loro dati personali sono online. Nel Parere si ricorda anche (sempre relativamente al test di bilanciamento) che quando gli interessi, i diritti fondamentali e le libertà degli interessati sembrano tali da dover prevalere sul legittimo interesse perseguito dal titolare o dai terzi, il titolare del trattamento può valutare di introdurre misure per mitigare l'impatto del trattamento dei dati personali, e che tali misure di mitigazione non vanno confuse con le misure che il titolare del trattamento è tenuto da adottare in ogni caso per assicurare la conformità del trattamento al GDPR. Le misure di mitigazione, si prosegue nel Parere, devono essere adeguate alle circostanze del caso e alle caratteristiche del modello di IA, incluso l'uso previsto, sono soggette a rapida evoluzione e rimangono comunque nella responsabilità del titolare del trattamento. Con queste specificazioni, il Parere fornisce comunque una lista esemplificativa e non-esaustiva di misure di mitigazione in relazione alla fase di sviluppo (anche con riferimento al web scraping) e a quella dell'uso (deployment).

Con riferimento **alla quarta (e ultima) domanda**, il Parere ricorda che le autorità di controllo per la protezione dei dati personali hanno poteri discrezionali nell'accertare possibili violazioni e nell'adottare appropriate, necessarie e proporzionate misure, tenuto conto delle circostanze di ciascun caso oggetto della sua valutazione.

Il Parere considera tre scenari.

Nello Scenario 1, i dati personali sono conservati nel modello di IA (nel senso che il modello non può essere considerato anonimo, come illustrato relativamente alla prima domanda) e sono successivamente trattati dallo stesso titolare del trattamento (ad esempio nel contesto dell'uso del modello). Nel Parere si dice che va accertato caso per caso, sulla base delle circostanze e del contesto specifici, se le fasi di sviluppo e di uso hanno o meno finalità separate (costituendo così separate attività di trattamento) e in che misura la mancanza di una base giuridica per il trattamento iniziale influisce sulla liceità del trattamento successivo.

Nello Scenario 2, i dati personali sono conservati nel modello di IA e sono trattati da un altro titolare nel contesto dell'uso (deployment) del modello. A questo riguardo, nel Parere si trova scritto che le autorità di

ISSN 2239-8570

controllo dovrebbero verificare se il titolare del trattamento che usa il modello abbia effettuato un esame appropriato, come parte delle sue obbligazioni di 'accountability' per dimostrare la conformità agli articoli 5(1)(a) e 6 del GDPR, per verificare che il modello di IA non è stato sviluppato trattando illecitamente dati personali. Tale esame dovrebbe riguardare, per esempio, la fonte dei dati personali ed ogni eventuale accertamento svolto in particolare da parte di un'autorità di controllo o di un'autorità giudiziaria che abbia concluso nel senso di ritenere illegittimo il trattamento nella fase dello sviluppo, e dovrebbe essere più o meno analitico a seconda dei rischi determinati dal trattamento nella fase dell'uso.

Nello Scenario 3, un titolare del trattamento tratta illecitamente dati personali per sviluppare il modello di IA, in seguito si assicura che esso sia anonimizzato, prima che lui stesso o un altro titolare cominci un altro trattamento di dati personale nel contesto dell'uso del modello di IA. A questo proposito, nel Parere si afferma che se nella seguente fase di operatività il modello di IA non vengono trattati dati personali, allora il GDPR non trova applicazione. In altre parole, l'illiceità del trattamento iniziale non dovrebbe avere un impatto sulla successiva operatività del modello. Similmente, nel Parere si trova scritto che quando titolari di trattamento trattano dati personali raccolti durante la fase dell'uso del modello di IA, dopo che esso era stato anonimizzato, il GDPR si applicherà in relazione a queste operazioni. In questi casi, secondo il Parere, la liceità dei trattamenti effettuati durante la fase dell'uso del modello di IA non dovrebbe essere inficiata dall'illiceità dei trattamenti iniziali.

SALVATORE ORLANDO

https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

2024/4(27)DML

27. Il documento informativo del Garante privacy belga del dicembre 2024 in materia di sistemi d'intelligenza artificiale e GDPR

Nella consapevolezza che la comprensione e l'osservanza di regole e principi del regolamento (UE) 679/2016 (**GDPR**) sono cruciali per uno sviluppo e un funzionamento dei sistemi di intelligenza artificiale (**IA**) non solo in linea con gli obblighi giuridici ma anche eticamente responsabile, l'Autorità garante per la protezione dei dati personali del Belgio (**Garante Privacy belga**) ha adottato, nel dicembre del 2024, una *information brochure* (il **Documento**) senz'altro meritevole di attenzione.

Il Documento, infatti, corredando l'esposizione con utili esemplificazioni, contiene un quadro informativo chiaro, ancorché essenziale, sugli obblighi imposti dal GDPR ai soggetti coinvolti nella catena che va dallo sviluppo all'uso dei sistemi di IA. In parallelo, vengono

ISSN 2239-8570

considerati i requisiti di conformità sanciti dal regolamento (UE) 2024/1689 (**AI Act**). Destinatari del Documento sono tutti gli *stakeholders*, afferenti sia al settore legale sia all'industria dell'IA (sviluppatori, data Analyst).

Assunta la definizione di sistema di IA di cui all'art. 3, n. 1 dell'AI Act, il Documento si sofferma anzitutto sui principi applicabili al trattamento dei dati personali *ex* art. 5 GDPR, da intrecciare con i requisiti stabiliti, in relazione ai differenti livelli di rischio, dall'AI Act medesimo.

Così, avuto riguardo all'art. 5(1)(a) GDPR, ed in particolare al principio di liceità, si ricorda che le basi giuridiche del trattamento rimangono, anche con riferimento a sistemi intelligenti, le sei elencate all'art. 6 GDPR, e che spetta dunque al titolare individuare quella pertinente per legittimare le proprie operazioni sui dati. **D'altronde, però, si evidenzia che il trattamento di dati personali non è in ogni caso lecito se l'AI Act proibisce un certo sistema come, ad es., un *software* per il *social scoring***.

Quanto alla correttezza (*fairness*), il documento ricorda che l'AI Act, pur non prevedendo un corpo di regole dedicate, si basa su tale principio nella misura in cui mira a contrastare *bias* e discriminazioni nello sviluppo, nell'impiego e nell'uso dei sistemi di IA.

In relazione, poi, al principio di trasparenza, si fa notare che a seconda del livello di rischio del sistema variano i relativi requisiti: per alcuni sistemi, la trasparenza è assicurata da un avviso fornito all'utente. Per i sistemi ad alto rischio, il fornitore deve dare informazioni sull'uso dei dati, sui fattori che influenzano le decisioni basate sull'IA e su come vengono mitigati i potenziali *bias*.

Brevi considerazioni vengono svolte con riferimento ai principi di limitazione della finalità e di minimizzazione dei dati. Il documento sottolinea, al riguardo, che l'AI Act rafforzerebbe il primo di essi nel contesto dei sistemi ad alto rischio, rimarcando la necessità di stabilire uno scopo preciso e documentato per il sistema medesimo.

Quanto al diverso ma connesso principio di limitazione della conservazione, invece, il Garante belga evidenzia che la normativa sull'IA non aggiunge nulla ai precetti del GDPR.

Maggiormente significativa è la notazione per cui l'AI Act si fonda sul principio di esattezza (segnatamente sotto il profilo dell'aggiornamento dei dati) di cui all'art. 5(1)(*d*) GDPR, allorquando prescrive che i sistemi ad alto rischio devono usare dati di alta qualità e privi di *bias*, di modo da evitare *output* discriminatori.

Particolare attenzione viene dedicata ai profili della sicurezza e della riservatezza dei dati, rispetto ai quali s'intrecciano le tradizionali pratiche di *data protection* e i nuovi requisiti, specialmente in punto di robustezza, sanciti dall'AI Act. Si muove dalla constatazione che i sistemi d'IA introducono rischi specifici, legati segnatamente alla qualità dei dati (di addestramento, ma anche di *input*) e a possibili interferenze illecite e manipolazioni dall'esterno. Per fronteggiarli, l'AI Act non solo impone per i sistemi ad alto rischio una valutazione iniziale del rischio, ma anche un monitoraggio e un *testing* continuo al fine di identificare falle nella sicurezza e l'emergere di eventuali *bias*. Le misure di sicurezza da implementare, legate all'autonomia del sistema, includono la sorveglianza

ISSN 2239-8570

umana durante l'uso. Sul piano pratico, il Documento suggerisce che tutto questo si dovrebbe tradurre nel prevedere, ad esempio: un riesame dei dati di addestramento e degli algoritmi per identificare potenziali *bias*; un monitoraggio delle prestazioni in funzione di valutazione della correttezza, dell'esattezza e dell'individuazione di comportamenti anomali del sistema; un intervento negli snodi decisionali più significativi, specialmente se l'*output* presenta un elevato impatto sulle persone.

Proprio la caratteristica di autonomia decisionale che connota ogni tecnologia riconducibile al paradigma dell'IA ha probabilmente suggerito al Garante Privacy belga di soffermarsi sui rischi ad essa connessi e sugli strumenti per mitigarli previsti all'interno dei due plessi normativi più volte citati. Il documento evidenzia il differente approccio che li anima. In sintesi, il GDPR consente alle persone di opporsi *ex post* a decisioni esclusivamente automatizzate ai sensi del suo art. 22, mentre, dal canto suo, l'AI Act richiede una supervisione umana proattiva per i sistemi ad alto rischio al fine di contrastare (a monte) il rischio di *bias* e di garantire uno sviluppo e un utilizzo responsabile di tali sistemi. Detto altrimenti, quegli stessi strumenti di sorveglianza umana, di cui si è detto poco sopra, dovrebbero consentire al *deployer* del sistema d'IA di anticipare l'emergere di criticità, senza attendere la reazione oppositiva dell'interessato.

Al tema dei diritti dell'interessato (*ex* artt. 15 ss. GDPR) nel contesto di un trattamento basato sull'IA il documento dedica poche notazioni soltanto. Si sottolinea, in particolare, che l'osservanza del principio di trasparenza, in relazione all'uso che dei dati viene fatto nei sistemi d'IA, è funzionale a consentire l'effettivo e consapevole esercizio di quei diritti.

Più articolata risulta per contro l'analisi dei rapporti tra il principio di *accountability* (art. 5(2) GDPR) e l'AI Act. Il Documento, infatti, dopo aver ribadito i tratti essenziali di questo pilastro della disciplina di protezione dei dati personali, sottolinea che su di esso si fonda anche l'approccio basato sul rischio che informa di sé AI Act. Pur in assenza di una sua esplicita enunciazione nell'articolato normativo, i fornitori, i *deployer* e gli utilizzatori dei sistemi intelligenti, ciascuno nell'ambito delle rispettive sfere di attività, sono tenuti ad attuare misure ispirate al principio di *accountability*, ivi incluse: la valutazione e la classificazione preliminare del sistema; la valutazione di impatto se trattasi di sistema ad alto rischio (FRIA); la chiara documentazione delle caratteristiche del sistema; la previsione di meccanismi di intervento umano; la messa in funzione di una procedura di *reporting* degli incidenti.

Nella sua seconda (e ultima) parte, il documento si ripropone di fornire indicazioni su come traslare principi e requisiti normativi in specifiche tecniche all'interno dei sistemi di IA.

Lo fa attraverso il caso, immaginato, di un sistema concepito per il calcolo del premio di un'assicurazione sulla vita che naturalmente tratta molteplici dati personali dei clienti. Per ciascuno degli aspetti sopra considerati vengono enunciate, seppur in forma sintetica, le pratiche da adottare e, comunque, consigliabili per assicurarne la conformità sia al GDPR, sia all'AI Act.

ISSN 2239-8570

Così, l'osservanza dei principi applicabili al trattamento viene perseguita attraverso la preliminare individuazione della base giuridica per una lecita raccolta e un lecito trattamento dei dati, avuto peraltro riguardo alle categorie particolari di dati. La *fairness* del trattamento, nell'esempio del documento, passa attraverso lo scrutinio delle fonti dei dati su cui il sistema è stato addestrato, l'esecuzione di test comparativi (tra *output* del sistema riferiti a clienti con caratteristiche analoghe), nonché la previsione di un meccanismo di revisione umana delle decisioni ad alto impatto (quale quella di negare la copertura assicurativa); il tutto onde identificare e mitigare potenziali *bias*.

Sul diverso fronte della trasparenza, si evidenzia che questa richiede alla compagnia di assicurazione di predisporre un documento interno (*data protection statement*) dove siano indicate con chiarezza le tipologie di dati raccolti, usati e conservati. Ciò si dovrebbe integrare con documenti informativi, facilmente comprensibili (ad es., perché strutturati in forma di FAQ) ed accessibili al cliente, al quale andrebbe inoltre garantito di poter conoscere quali dati sono stati specificamente usati nel calcolo del suo premio.

Se sui principi di limitazione della finalità e di minimizzazione non si registrano osservazioni peculiari, maggiore interesse suscitano i suggerimenti forniti in merito alla necessaria verifica circa l'esattezza e l'aggiornamento dei dati, funzionale, come detto, stante l'autonomia decisionale del sistema d'IA in questione, ad evitare *output* discriminatori o, comunque, viziati da *bias*. Il documento, al riguardo, suggerisce di mettere in atto misure improntate ad un approccio proattivo sul lato sia dell'interessato, sia dell'impresa. Si segnala, ad es., l'opportunità di stabilire procedure di periodico *data refresh*, anche mediante richieste all'interessato, di assicurare a quest'ultimo, attraverso *app* o un portale online, un agevole meccanismo di verifica e di aggiornamento. Ancora, l'impresa dovrebbe predisporre dei meccanismi di allerta circa la qualità dei dati, idonei ad identificare dati mancanti o potenzialmente inaccurati. In relazione ai rischi implicati dalla natura intelligente del sistema, poi, si consiglia alla compagnia assicurativa, tra l'altro, di effettuare una preliminare analisi delle fonti dei dati di addestramento, da accompagnare ad un regolare monitoraggio e testing, di tipo comparativo, dell'*output* del sistema volto ad identificare bias.

Analoga attenzione meritano le indicazioni relative alla sicurezza del trattamento in relazione non tanto all'esperienza maturata nell'ambito del settore della *data protection*, quanto, piuttosto, alla tecnologia con cui viene effettuato il trattamento medesimo. In sintesi, si rimarca la necessità di assicurare una validazione dei dati di addestramento e di *input*, attraverso, per es., il tracciamento della loro provenienza e misure di identificazione delle anomalie, in relazione sia a possibili *bias* sia a fenomeni di manipolazione dall'esterno. In ogni caso, la compagnia assicurativa dovrebbe stabilire un quadro per la sorveglianza umana del sistema durante l'intero suo ciclo di vita, con speciale riguardo alle operazioni e ai processi decisionali maggiormente critici sotto il profilo dei dati rilevanti ovvero dell'impatto sull'interessato.

ISSN 2239-8570

Il documento chiude il caso di studio ribadendo la necessità, per il titolare del trattamento che si serva di un sistema d'IA, di assicurare l'*accountability*. Sotto un primo profilo, si invita a istituire un registro, in forma chiara e sintetica, di tutte le basi giuridiche sulla cui scorta vengono trattati i dati degli interessati. Sotto altro profilo, specifico alla natura intelligente del sistema, si esorta a compiere e a documentare la FRIA onde identificare e mitigare in modo proattivo i potenziali rischi associati al sistema in ottica di promozione di un calcolo dei premi assicurativi equo e non discriminatorio.

A chiusura della presente sintesi, può essere utile sottolineare che l'iniziativa del Garante belga non rappresenta un *unicum* nel panorama europeo, ma che, al contrario, da tempo si registra un'attenzione crescente verso le implicazioni di *data protection* dell'IA. Già il 3 luglio 2024 l'EDPS aveva pubblicato il documento "*Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems*" con speciale riferimento all'IA generativa. Va poi fatto un cenno al documento "*Statement on the Role of Data Protection Authorities in Fostering Trustworthy AI*", adottato l'11 ottobre 2024 nell'ambito della Tavola rotonda del G7 dei Garanti privacy, il quale contiene riferimenti a numerose risoluzioni, linee guida e altri documenti di *policy* sul tema della protezione dei dati personali nel contesto dell'IA. Infine, non può mancare un richiamo al *report* della *Taskforce* istituita in seno all'EDPB in relazione alla nota vicenda "*ChatGPT*", pubblicato il 23 maggio scorso e, da ultimo, all'Opinione n. 28/2024 del 17 dicembre 2024, resa ai sensi dell'art. 64 GDPR, "*on certain data protection aspects related to the processing of personal data in the context of AI models*". Questa si sofferma (*ivi*, par. 27 ss.), tra l'altro, sul delicato problema, non affrontato dal Garante belga ma logicamente preliminare ad ogni analisi, concernente la natura personale o anonima dei dati nel contesto di un sistema d'IA.

DAVIDE M. LOCATELLO

https://www.autoriteprotectiondonnees.be/publications/artificial-intelligence-systems-and-the-gdpr---a-data-protection-perspective.pdf

2024/4(28)FP

28. Il Final Report di ESMA del 17.12.2024 contenente le Linee guida per la qualificazione delle cripto-attività come strumenti finanziari

Il regolamento (UE) 2023/114 sui mercati delle cripto-attività (**MiCAR** o il **Regolamento**) (su cui v. in questa Rubrica la notizia n. 1 nel numero 2/2023 [2023/2(1)AF] e in *Atlante*, p. 338) mira alla creazione di un quadro giuridico armonizzato relativo al mercato europeo dei c.d. cripto-assets. L'intervento normativo si giustifica con la necessità di garantire la supervisione su un settore che in larga parte sfuggiva alla regolamentazione

ISSN 2239-8570

esistente, creando così vuoti di tutela per i consumatori e disparità di condizioni fra operatori del mercato.

Il Regolamento definisce come cripto-attività una rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga (art. 3, n. 5 MiCAR). L'ambito di applicazione del MiCAR non copre però ogni cripto-attività che rientri all'interno di questa definizione, bensì solo quelle che non siano già coperte da altre normative UE. In particolare, l'art. 2, par. 4 lett. a) MiCAR stabilisce che il Regolamento non trovi applicazioni per le cripto-attività che rientrano nella definizione di «strumento finanziario» di cui alla direttiva 2014/65/UE (**MiFID II**). Quest'ultima non provvede, tuttavia, a enucleare condizioni e criteri per una definizione generale di «strumento finanziario», ma si limita a rimandare ad un elenco di strumenti tassativamente individuati all'interno dell'Allegato 1, Sezione C. La nozione di strumento finanziario non è di conseguenza armonizzata fra gli Stati Membri: la sua applicazione a livello nazionale è, pertanto, suscettibile di dar luogo a disparità regolamentari e applicazioni difformi del MiCAR e della MiFID II.

Al fine di garantire alcune coordinate di riferimento per le autorità nazionali competenti nell'applicazione delle norme del MiCAR e per gli operatori di mercato, la European Securities and Markets Authority (**ESMA**) è stata incaricata di elaborare linee guida per chiarire le condizioni e i criteri utili a determinare quando una cripto-attività possa essere considerata uno strumento finanziario (art. 2, par. 5 MiCAR). Le linee guida non hanno l'obiettivo di delineare le condizioni per una definizione generale di «strumento finanziario», bensì quello di chiarire le intersezioni fra i diversi comparti di disciplina.

La prima versione delle linee guida è stata sottoposta a consultazione pubblica in data 29 gennaio 2024, che si è poi conclusa con la pubblicazione del Final Report il 17 dicembre 2024 (ESMA75453128700-1323) (di seguito il **Final Report**). Il Final Report riassume e analizza le risposte alla consultazione e spiega come siano state prese in considerazione per lo sviluppo della versione finale delle linee guida ad esso allegate (le **Linee guida**).

Le linee guida, in numero di nove, mirano a un complicato equilibrio tra l'esigenza di evitare un approccio olistico e quella di imbrigliare l'applicazione del MiCAR fornendo criteri eccessivamente analitici e di dettaglio. A livello generale, gli stakeholders coinvolti nella consultazione hanno manifestato apprezzamento per il documento sviluppato dall'ESMA, sottolineando però la necessità di fornire un maggior numero di esempi concreti di applicazione, oltre a formulare talune preoccupazioni relative all'incremento dei costi derivanti dalla sua implementazione. In particolare, si sottolinea che le autorità nazionali dovranno sostenere costi legati all'implementazione e alla supervisione delle linee guida, mentre i partecipanti potrebbero dover rivedere la classificazione delle loro cripto-attività e adattare i processi interni.

La Linea Guida 1 è dedicata al principio di neutralità tecnologica e all'approccio basato sulla sostanza. I partecipanti hanno accolto con favore

ISSN 2239-8570

la preminenza loro assegnatagli, tuttavia, alcuni hanno chiesto maggiori dettagli sulla loro applicare, specialmente in un contesto di tecnologie emergenti. L'ESMA sottolinea che il formato tecnologico di una cripto-attività non deve essere un fattore determinante nella sua classificazione come strumento finanziario. Ad esempio, la tokenizzazione di strumenti finanziari tradizionali non modifica la loro natura regolamentare. Questo principio è essenziale per garantire che attività simili siano soggette alle stesse regole, indipendentemente dal supporto tecnologico utilizzato.

Le Linee Guida 2-6 si occupano di delineare alcune distinzioni fra le cripto-attività e specifiche tipologie di strumenti regolati da altre normative europee.

La Linea Guida 2 è relativa alla classificazione di uno strumento come «titolo trasferibile» (*transferable security*). Alcuni partecipanti hanno espresso dubbi sull'interpretazione dei criteri di "negoziabilità" e "trasferibilità", sottolineando l'opportunità di individuare ulteriori sotto-criteri per chiarire la distinzione fra cripto-attività e titoli tradizionali. In risposta alla richiesta formulata dai partecipanti, ESMA precisa che l'interpretazione di questi termini debba essere allineata con MiFID II, in particolare al fine di considerare la capacità del bene di essere scambiato sul mercato dei capitali, anche in presenza di alcune restrizioni. Il Report chiarisce che le cripto-attività possano essere classificate come titoli trasferibili se soddisfano tre criteri cumulativi: *i*) non essere classificabili come strumenti di pagamento (una cripto-attività utilizzata principalmente come mezzo di scambio non può qualificarsi come titolo trasferibile); *ii*) appartenere ad una "classe di titoli" (la cripto-attività deve conferire diritti analoghi a quelli delle azioni, obbligazioni o altri titoli non azionari); infine *iii*) essere negoziabile sul mercato dei capitali (bastando l'astratta negoziabilità, quindi anche in ipotesi in cui non vi sia uno specifico mercato per il prodotto o tale mercato sia temporaneamente sospeso).

La Linea Guida 3 è dedicata agli strumenti del mercato monetario. Alcuni partecipanti hanno chiesto una maggiore chiarezza per distinguere tra depositi tokenizzati e strumenti del mercato monetario, poiché talvolta presentano caratteristiche simili. Il Report precisa che una cripto-attività possa essere classificate come strumenti del mercato monetario se abbiano una scadenza definita e breve e conferiscano obblighi chiari per il rimborso del capitale o il pagamento degli interessi. Una piattaforma potrebbe, ad esempio, offrire un token legato a un saldo di credito a breve termine, con un valore stabile ancorato a valute fiat come l'euro. Questo potrebbe essere considerato un equivalente digitale di un certificato di deposito.

La Linea Guida 4 si occupa invece della distinzione fra utility tokens e quote di organismi di investimento collettivo. I partecipanti alla consultazione hanno sollevato preoccupazioni che alcune attività, come lo staking (ad esempio, la Proof of Stake, funzionale ad assicurare la sicurezza e operatività della blockchain) possano essere qualificate come attività di investimento collettivo. ESMA ribadisce che la classificazione debba basarsi sui diritti conferiti dal token, piuttosto che sulla forma. In conformità alle linee guida una cripto-attività è considerata una quota di un organismo di investimento collettivo se implica una raccolta di capitali fra più

ISSN 2239-8570

investitori ed il loro impiego secondo una politica comune, al fine di generare un rendimento collettivo per gli investitori. A tal proposito, ESMA ribadisce che il progetto associato alla cripto-attività debba avere uno scopo di investimento ben definito e non un generico obiettivo commerciale o industriale.

La Linea Guida 5 concerne la distinzione con i contratti derivati. Dalla consultazione pubblica sono emerse preoccupazioni sull'applicazione dei criteri MiFID II a strumenti derivati cripto-nativi, come i futures perpetui, e sui processi di regolamento. Anche per queste ipotesi, ESMA ha ribadito che il metodo di regolamentazione dei flussi finanziari non altera, di regola, la natura del prodotto, salvo la necessità di una valutazione caso per caso (ad esempio, a seconda che la regolamentazione avvenga in cash o mediante scambio di cripto-attività). Una cripto-attività può dunque essere classificata come un derivato se serva come attività sottostante per contratti derivati (es. futures, opzioni) e possegga caratteristiche intrinseche di un contratto derivato, come il riferimento al valore di un'attività sottostante. I futures perpetui, che non hanno una data di scadenza, sono considerati derivati poiché coinvolgono lo scambio continuo della performance di un'attività sottostante.

La Linea Guida 6 riguarda il distinguo fra le cripto-attività e gli strumenti di allocazione delle emissioni (come i carbon credits). Il Report chiarisce che solo le cripto-attività conformi al sistema di EU Emissions Trading Scheme (ETS) e che rappresentino un diritto del detentore di emettere una certa quantità di carbonio possano venir qualificate come strumenti di allocazione delle emissioni.

La Linea Guida 7 fornisce invece ulteriori chiarimenti in ordine all'appartenenza di una cripto-attività all'ambito di applicazione del MiCAR. L'ESMA ha ribadito che le cripto-attività non possono essere classificate simultaneamente sotto MiCAR e MiFID II. Laddove la cripto-attività attribuisca diritti di governance corrispondenti a quelli previsti da uno strumento finanziario, essa andrà ricondotta sotto l'applicazione della MiFID II. Può essere, ad esempio, il caso di un utility token che attribuisca diritti corrispondenti a quelli di una partecipazione azionaria, come il diritto di voto su decisioni societarie o di beneficiare dei profitti o del surplus prodotti da una società. Per converso, la sola prospettiva di un guadagno futuro non è da sola in grado di attrarre la qualificazione come strumento finanziario.

Sono altresì esclusi dall'ambito di applicazione del MiCAR i token non fungibili (NFT). Molti partecipanti hanno richiesto chiarimenti aggiuntivi sulla definizione di "unicità" e "non fungibilità" specificata dalla Linea Guida 8, temendo un'eccessiva regolamentazione del mercato NFT. ESMA ha pertanto chiarito che la caratteristica di unicità di un token risieda nella sua non sostituibilità, in quanto presenti delle caratteristiche o assegni diritti che la distinguano in modo univoco rispetto ad assets prodotti dallo stesso o da altri emittenti. Nella valutazione casistica, le autorità nazionali competenti possono avvalersi di una serie di indicatori quali, ad esempio, il possesso di attributi unici che contribuiscono al suo valore intrinseco e alla

ISSN 2239-8570

sua rarità, funzionalità specifiche, o diritti esclusivi di accesso e di utilizzo unici per il titolare.

Infine, la Linea Guida 9 si occupa del problema dei token ibridi, che combinano caratteristiche di vari tipi di cripto-attività (es. utilità, investimento, pagamento). L'ESMA adotta un approccio gerarchico per classificare i token ibridi, garantendo coerenza regolamentare: se un token ibrido presenta caratteristiche di uno strumento finanziario, questa classificazione prevale.

Trattandosi di una fonte di *soft law*, le autorità nazionali competenti saranno tenute, entro tre mesi dalla pubblicazione delle linee guida, a comunicare ad ESMA se già le abbiano adottate, se siano in procinto di adottarle o se non intendano farlo.

FEDERICO PISTELLI

https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf

2024/4(29)CAT

29. I risultati del G7 Privacy di Roma del 9-11 ottobre 2024: verso un futuro digitale a prova di privacy

Dal 9 all'11 ottobre 2024, Roma è stata il centro del dibattito globale sulla privacy e sulla protezione dei dati personali. Il *G7 Data Protection and Privacy Authorities Roundtable*, giunto alla sua quarta edizione, ospitato dal Garante italiano ha visto la partecipazione delle Autorità di **Canada**, **Francia**, **Germania**, **Giappone**, **Italia**, **Regno Unito** e **Stati Uniti d'America**, insieme al Comitato europeo della protezione dei dati (**EDPB**) e al Garante europeo della protezione dei dati (**EDPS**).

Le discussioni si sono articolate attorno ai risultati di tre gruppi tematici, ciascuno dedicato a un aspetto cruciale della governance dei dati:

Data Free Flow with Trust (DFFT)

In un contesto globale sempre più dipendente dai flussi di dati transfrontalieri, è emersa la necessità di creare strumenti normativi che consentano la libera circolazione delle informazioni, garantendo al contempo elevati standard di protezione e sicurezza. Pertanto, il DFFT ha presentato il documento **"Comparative Analysis of Core Elements of GDPR Certification as a Tool for Transfers and the Global CBPR System"**. Questo studio ha esaminato le differenze e i punti di convergenza tra il sistema europeo di certificazione GDPR e il sistema CBPR (Cross-Border Privacy Rules) adottato in diversi Paesi extra-UE. L'obiettivo è stato quello di promuovere, laddove possibile, un approccio interoperabile tra i due strumenti.

Enforcement Cooperation Working Group (ECWG)

ISSN 2239-8570

Vista la crescente necessità di coordinamento per condurre istruttorie su titolari del trattamento che operano in tutto il mondo e per affrontare violazioni della privacy in un contesto senza confini fisici, è stato sviluppato un quadro di riferimento per la cooperazione tra le autorità di protezione dati. In tal senso, i lavori del secondo gruppo hanno portato all'approvazione del documento **"Enforcement Cooperation Framework"**, volto a rafforzare la cooperazione tra le autorità di protezione dei dati, evidenziandone le principali convergenze tematiche nelle relative pronunce.

Emerging Technologies Working Group (ETWG)

Il terzo gruppo si è concentrato sulle nuove tecnologie mirate alla protezione della privacy. In questo ambito, sono stati adottati tre documenti principali:

- **"Privacy-Enhancing Technologies and AI Governance for Minors"**: un rapporto che esplora come minimizzare i rischi per i minori nell'uso dell'intelligenza artificiale, attraverso l'impiego di tecnologie di protezione della privacy (PETs).
- **"Terminology and Definitions for AI and Emerging Technologies"**: un documento che stabilisce un vocabolario condiviso per concetti chiave come anonimizzazione, pseudonimizzazione e de-identificazione, al fine di armonizzare le normative e facilitare il dialogo tra le parti.
- **"Case Study on Synthetic Data and Privacy Risks"**: uno use case sull'utilizzo dei dati sintetici in ambito sanitario che analizza il loro potenziale di minimizzazione identificativa al dine di proteggere la privacy degli interessati.

Governance dell'IA: Un Ruolo Centrale per le Autorità Privacy

Inoltre, uno dei documenti più rilevanti adottati durante il G7 è stato lo **Statement on "The Role of Data Protection Authorities in Fostering Trustworthy AI"**. Il testo sottolinea la necessità di riconoscere alle Autorità di protezione dei dati personali un ruolo centrale nella supervisione e nella regolamentazione dell'IA. Grazie alla loro indipendenza e competenza, le Autorità possono infatti garantire che i sistemi di IA siano progettati by design per rispettare i diritti fondamentali, prevenendo discriminazioni e opacità algoritmiche. Le criticità evidenziate nell'approccio normativo in tema di Intelligenza Artificiale di alcuni Stati, tra cui l'Italia, sono state peraltro richiamate dalla comunicazione del 5 novembre 2024 della Commissione Ue al nostro Governo, con la quale viene suggerita una profonda opera di modifica dell'impianto legislativo proposto e una garanzia in merito all'indipendenza delle Autorità designate ai sensi dell'AI Act.

Il Communiqué e l'Action Plan: Obiettivi Concreti per il Futuro

Infine, Il G7 si è concluso con l'adozione del Communiqué e dell'Action Plan, documenti che riassumono i risultati e delineano le priorità future. Il Communiqué fornisce una panoramica delle attività svolte durante il vertice, mentre l'Action Plan identifica gli obiettivi futuri chiave, tra cui: continuare un monitoraggio fino al G7 del 2025 per valutare gli sviluppi normativi e consolidare una governance affidabile per l'intelligenza artificiale;

ISSN 2239-8570

promuovere l'interoperabilità dei regimi di protezione dei dati, come delineato nel documento "Comparative Analysis of GDPR Certification and CBPR"; sviluppare standard tecnici a protezione dei minori per l'IA, secondo i principi descritti nei documenti "Privacy-Enhancing Technologies and AI Governance for Minors; portare i documenti adottati ai più importanti tavoli internazionali e promuovere pratiche standardizzazate.

In conclusione, per la prima volta da quando, nel 2020, il G7 Privacy è nato, si è arrivati all'adozione di un numero elevato di documenti tecnici (sui quali v. *infra* in questa Rubrica in questo numero le notizie [2024/4(30)AB], [2024/4(31)IG], [2024/4(32)PG] [2024/4(33)CS]) che hanno gettato le basi per una maggiore collaborazione e uniformazione delle prassi a livello internazionale.

CARMINE ANDREA TROVATO

https://www.gpdp.it/home/docweb/-/docweb-display/docweb/10062575

2024/4(30)AB

30. Il rapporto dell'11 ottobre 2024 pubblicato durante il G7 dei Garanti privacy su anonimizzazione, pseudonimizzazione e deidentificazione

L'11 ottobre 2024 è stato pubblicato sul sito del Garante per la protezione dei dati personali il documento intitolato "*Reducing identifiability in cross-national perspective: Statutory and policy definitions for anonymization, pseudonymization, and deidentification in G7 jurisdictions*" (di seguito, il **Rapporto**). Il Rapporto è stato elaborato nell'ambito dell'evento annuale *G7 Data Protection and Privacy Authorities Roundtable* (v. notizia precedente in questa Rubrica [2024/4(29)CAT]).

Nelle giornate della conferenza, dedicata a "La privacy nell'era dei dati", sono stati affrontati numerosi temi legati alle sfide per la *privacy* e la protezione dei dati personali dinanzi ai cambiamenti digitali.

Come negli anni precedenti, le DPA hanno suddiviso i lavori in base a tre diverse Aree/Pilastri:

- Sicura e responsabile circolazione dei dati personali (*Data Free Flow with Trust*);
- Tecnologie emergenti;
- Cooperazione per l'applicazione della normativa in materia di protezione dei dati personali.

Allo scopo di contribuire alla comprensione comune dei termini e dei concetti chiave in uso nel settore delle tecnologie emergenti (c.d. Secondo Pilastro), è stato prodotto il Rapporto, elaborato dalle DPA anche in qualità di parti del *G7 Emerging Technologies Working Group*. La redazione del documento è stata coordinata dallo *Office of the Privacy Commissioner* (**OPC**) del Canada.

ISSN 2239-8570

Il Rapporto è stato definito dagli stessi compilatori come un *terminology paper*, avente come obiettivo principale quello di allineare, in particolare, le definizioni di anonimizzazione, psuedonimizzazione e de-identificazione. Appurato l'interesse sempre maggiore per l'utilizzo di procedure e tecnologie che possano ridurre le possibilità di identificare gli individui, infatti, il rapporto si sofferma sulle definizioni legislative e non di tali tecniche nei diversi Paesi del G7, individuando brevemente le caratteristiche comuni e sottolineando le differenze presenti nei vari sistemi giuridici, tenuto conto anche del livello sovranazionale, nonché di quello regionale e/o sub-statuale in cui si rinvengono le espressioni medesime.

In generale, le definizioni stabiliscono significati normativi specifici, comprese le condizioni in forza delle quali le informazioni sono considerate o meno rientranti nell'ambito di applicazione di una determinata formulazione. In alcuni casi, le definizioni includono o implicano anche processi specifici o requisiti aggiuntivi che devono essere soddisfatti. A seconda dei casi, le informazioni che rientrano in una definizione o nell'altra possono essere soggette o meno a minori restrizioni circa il relativo utilizzo e, in alcuni casi, possono cadere all'infuori dell'ambito di applicazione della normativa sulla protezione dei dati personali.

Il rapporto individua le aree di sovrapposizione e le differenze in base ai seguenti profili:

- Il grado o la misura in cui l'identificabilità deve essere ridotta;
- Il grado o la misura in cui le informazioni possono essere utilizzate per identificare una persona;
- I processi e le tecniche richieste per ridurre l'identificabilità;
- Se le informazioni risultanti sono considerate informazioni personali.

Va sottolineato però come il significato e l'interpretazione delle definizioni si basano comunque sulla definizione di "dato personale" presente nel sistema giuridico preso a riferimento.

Per quanto riguarda la **de-identificazione**, le definizioni variano, anzitutto, a seconda del grado in virtù del quale è possibile identificare una persona. Così, ad esempio, il *Section* 2(1) della proposta *Consumer Privacy Protection Act* del Canada (**CPPA**) e il *Section* 12 del *Quebec's Act respecting the protection of personal information in the private sector* richiedono che le persone non possano essere identificate *direttamente* dalle informazioni. Diversamente, il *US Health Insurance Portability and Accountability Act* (**HIPAA**) *Privacy Rule*, il *California Consumer Privacy Act* (**CCPA**) e il *Ontario's Personal Health Information Protection Act* (**PHIPA**) stabiliscono soglie più elevate per considerare le informazioni de-identificate, richiedendo sostanzialmente la "minimizzazione", entro una "misura ragionevole", della possibilità di identificazione. Ancora, le definizioni di de-identificazione possono divergere in base al fatto che l'informazione de-identificata possa o meno essere qualificata alla stregua di un dato personale (nella seconda ipotesi, le soglie per considerare le informazioni de-identificate sono in genere più elevate). In ogni caso, nella maggior parte degli Stati la de-identificazione è considerata come un

ISSN 2239-8570

processo tendenzialmente reversibile, ancorché non sempre lecitamente ammissibile (vedi, ad esempio, *Ontario's* PHIPA).

Per quanto concerna la **pseudonimizzazione**, alcune definizioni sono presenti, ad esempio, nel Regolamento (UE) 2016/679 (**GDPR**) per l'Unione Europea e nello *Japan's Act on the Protection of Personal Information* (**APPI**). In generale, si richiede che i dati personali non possano più essere attribuiti ad uno specifico interessato senza l'utilizzo di informazioni aggiuntive. Inoltre, la soglia di identificabilità tiene conto di tutti i mezzi ragionevolmente utilizzabili, da parte del titolare del trattamento o altro soggetto, per identificare direttamente o indirettamente la persona fisica. Per il Giappone viene specificato (art. 2 APPI) che la pseudonimizzazione avviene attraverso la rimozione di identificatori o la loro sostituzione con altri identificatori senza seguire schemi che consentano di ripristinare il loro stato originale. In ogni caso, stante la (tendenziale) reversibilità della procedura, le informazioni pseudonimizzate sono ancora considerate dati personali; tanto che devono essere messe in atto specifiche misure tecniche, organizzative e di sicurezza in modo tale da prevenire, appunto, la possibilità di re-identificazione (vedi, ad esempio, l'art. 4(5), GDPR).

Per quanto riguarda l'**anonimizzazione**, è generalmente richiesto che, all'esito della procedura, le informazioni non consentano di identificare la persona né direttamente, né indirettamente. Tuttavia, la soglia per determinare l'identificabilità può variare anche in maniera significativa nei diversi sistemi. Guardando alla legislazione del Quebec, occorre valutare se è ragionevolmente prevedibile dalle circostanze concrete che le informazioni possano identificare un individuo direttamente o indirettamente; il processo utilizzato per l'anonimizzazione deve inoltre seguire i criteri e i termini stabiliti dalla normativa, nonché le "*generally accepted best practices*". Analogamente, in Giappone il processo deve essere eseguito, in determinate casi, in conformità a specifici *standard* stabiliti dalla *Personal Information Protection Commission* (art. 43 APPI). In entrambe le giurisdizioni, peraltro, la procedura di anonimizzazione è considerata come irreversibile. Al contrario, per il GDPR non è richiesta né l'irreversibilità della anonimizzazione, né il raggiungimento di una soglia specifica definita *a priori*, essendo solamente previsto di valutare «la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica», prendendo in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici (Considerando 26 GDPR).

Preme sottolineare come per le DPA sia pressoché assodato il fatto che nella pratica è molto difficile, se non impossibile, eliminare qualsiasi possibilità di re-identificazione. Per tale ragione, i requisiti di "irreversibilità" della procedura di anonimizzazione devono essere intesi ai soli fini dell'applicazione della normativa sulla protezione dei dati, piuttosto che come uno stato necessariamente assoluto (elemento, questo, confermato tra l'altro da numerose linee guida emanate, specificamente richiamate nel rapporto).

ISSN 2239-8570

Va da sé che le informazioni anonime non sono considerate informazioni personali e pertanto ad esse non si applicano le norme previste dalla legge per tali informazioni. In alcuni sistemi giuridici, tuttavia, alcuni vincoli possono applicarsi anche alle informazioni anonime come, ad esempio, il divieto di procedere o tentare la re-identificazione.

Il rapporto è poi seguito da un allegato (*Annex*) che riproduce nel dettaglio le diverse definizioni di de-identificazione, pseudonimizzazione e anonimizzazione nelle diverse legislazioni applicabili ai Paesi del G7 partecipanti alla conferenza, non solo a livello nazionale, bensì anche di fonti sub-statuali ovvero para-normative.

Come è possibile osservare dalla lettura attenta del rapporto, le varie aree di sovrapposizione creano delle sicure opportunità per una maggiore armonizzazione a livello transnazionale, mentre le differenze più marcate riguardano non tanto le circostanze in base alle quali un'informazione personale può essere astrattamente sussunta entro una determinazione definizione, quanto piuttosto i requisiti normativi richiesti per potere in concreto parlare di dati anonimi, psudonimizzati ovvero de-identificati. Infine, sembra che i termini "pseudonimizzazione" e "anonimizzazione" siano generalmente riferibili a concetti meno sovrapponibili tra di loro, mentre così non pare per l'espressione "de-identificazione".

Auspicando nella prosecuzione del dialogo, va rammentato come le DPA hanno approvato un Action Plan per il 2024/2025. Il rapporto relativo alla anonimizzazione, pseudonimizzazione e de-identificazione è esplicitamente richiamato nella sezione intitolata "*strategic support*" delle azioni relative al Secondo Pilastro. Le Autorità, quindi, si sono date appuntamento al prossimo *G7 DPA Roundtable*, incontro che si terrà in Canada e sarà ospitato dal OPC canadese.

ALESSANDRO BERNES

Report G7 Garanti privacy 11.10.2024 su anonimizzazione, pseudonomizzazione e de-identificazione

2024/4(31)IG

31. La dichiarazione dell'11.10.2024 del G7 dei Garanti Privacy su IA e bambini

Fra i principali temi di confronto discussi nell'incontro del G7 dei Garanti Privacy (su cui v. in questa Rubrica la notizia numero 29 in questo numero [2024/4(29)CAT]) figura quello della salvaguardia dei dati personali dei minori di età nell'impiego dell'IA, che ha formato oggetto dello *Statement on AI and Children* dell'11 ottobre 2024.

Le autorità hanno al riguardo espresso significative preoccupazioni, sottolineando che i minori, a causa della loro vulnerabilità (dovuta alla loro ridotta capacità di comprendere i concetti di privacy digitale e alla loro limitata esperienza di vita) sono maggiormente esposti ai rischi legati

ISSN 2239-8570

all'impiego dei sistemi di intelligenza artificiale, fra i quali il rischio di manipolazione, di discriminazione per effetto di decisioni automatizzate, di sfruttamento commerciale e di essere esposti a contenuti inappropriati. Le autorità hanno, pertanto, sottolineato la necessità di adottare misure preventive per garantire che i dati personali dei minori siano trattati in modo responsabile e conforme ai principi di protezione dei dati. Tra queste misure figurano l'implementazione del principio di "privacy by design e by default", in modo da ridurre i rischi di dipendenza, manipolazione e discriminazione, oltre che l'adozione di modelli trasparenti e spiegabili e l'applicazione di rigorosi limiti alla raccolta e all'utilizzo dei dati personali dei minori.

In quest'ottica, si è infine segnalata l'importanza di promuovere l'alfabetizzazione digitale nell'ambito delle politiche di innovazione digitale, per accrescere la consapevolezza sia tra i bambini e i giovani sia tra gli educatori, riguardo alle opportunità e ai rischi associati all'uso dell'intelligenza artificiale. L'obiettivo è garantire che l'IA sia utilizzata nei contesti educativi non solo con adeguate capacità tecniche, ma anche con consapevolezza e adesione ai diritti e ai doveri connessi alla tutela dei dati personali.

Nel piano d'azione 2024-2025, presentato in chiusura del vertice, si è concordato sulla necessità di rafforzare la collaborazione internazionale per monitorare l'utilizzo della IA e di sviluppare linee guida comuni, finalizzate a garantire un uso etico e responsabile delle tecnologie emergenti, che, con specifico riguardo ai minori di età, si traduce nella salvaguardia della loro autonomia in uno spazio sicuro, al contempo capace di promuoverne il benessere.

ILARIA GARACI

https://www.garanteprivacy.it/documents/10160/0/Roundtable+of+G7+Data+Protection+and+Privacy+Authorities+2024+-+Statement+on+AI+and+Children.pdf/d9222969-ba18-1f7a-e51f-233527eb0bfe?version=1.1

2024/4(32)PG

32. Adottato l'11.10.2024 durante il G7 dei Garanti Privacy un documento di analisi comparativa tra il GDPR ed il sistema CBPR globale di trasferimento dei dati personali con riferimento al sistema delle certificazioni

In data 11 ottobre 2024 è stata pubblicata, come parte dell'attività del gruppo di lavoro Data Free Flow with Trust (**DFFT**) nell'ambito dell'incontro dei G7 dei Garanti Privacy (su cui v. in questa Rubrica la notizia numero 29 in questo numero [2024/4(29)CAT]), un'analisi comparativa volta a valutare differenze e somiglianze tra i criteri di certificazione dell'Unione europea da utilizzare come strumento per i

ISSN 2239-8570

trasferimenti di dati da titolare a titolare del trattamento (la **Certificazione GDPR**, basata sulle Linee guida EDPB (Linee guida EDPB 1/2018 versione 3.0 adottate il 4 giugno 2019 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del GDPR e Linee guida 07/2022 versione 2.0 adottate il 14 febbraio 2023 sulla certificazione come strumento per i trasferimenti) e il Global Cross-Border Privacy Rules System (**Global CBPR System**). L'obiettivo del documento è contribuire al dialogo sugli elementi di convergenza e sulla futura interoperabilità degli strumenti globali e regionali per i trasferimenti transfrontalieri di dati in vari forum internazionali.

Questa analisi comparativa non pregiudica l'approvazione dei singoli meccanismi di Certificazione GDPR da parte di organismi di certificazione accreditati o di Autorità garanti nazionali in linea con la disciplina sulla protezione dei dati europea o la certificazione di organizzazioni da parte di "Accountability Agents" riconosciuti dal **Global CBPR Forum**.

L'obiettivo generale delle norme sui trasferimenti è garantire che gli standard di protezione dei dati continuino a essere rispettati quando i dati vengono trasferiti oltre confine. In questo contesto, sia il GDPR che il Global CBPR System prevedono schemi di certificazione come strumento per i trasferimenti transfrontalieri di dati personali. Questi stabiliscono principi chiave simili (liceità, limitazione delle finalità, sicurezza dell'elaborazione dei dati e trasparenza). Si segnalano, però, anche rilevanti differenze con riferimento al loro fondamento giuridico, struttura e finalità, nonché disposizioni con regole specifiche (tra cui esecutività e ricorso legale, norme relative alla supervisione indipendente e all'accesso governativo).

Con riferimento al *fondamento giuridico*, è necessario sottolineare che gli schemi di certificazione GDPR saranno sviluppati sulla base e in conformità con il GDPR, che rappresenta una disciplina giuridicamente vincolate e direttamente applicabile ai Paesi membri e allo Spazio Economico Europeo (**SEE**); il Regolamento stabilisce le condizioni in base alle quali possono essere effettuati trasferimenti internazionali di dati personali (Capo V, artt. 44-50). I trasferimenti di dati sono soggetti a garanzie adeguate, che possono, tra gli altri meccanismi di tutela, essere fornite da una certificazione GDPR approvata. Il Global CBPR System rappresenta, invece, un quadro di regole a carattere volontario e multilaterale con principi, requisiti e una struttura di governance concordati tra i Membri del Global CBPR Forum e applicati in base alla legge nazionale dei Membri.

Per quanto concerne, inoltre, *struttura e scopo degli schemi*, ai sensi del GDPR, coloro che operano nell'ambito di attività soggette al GDPR (esportatore GDPR) non possono trasferire dati personali a un altro titolare o responsabile del trattamento al di fuori dello SEE (importatore di dati) senza garantire un livello equivalente di protezione degli individui. L'importatore di dati (titolare o responsabile del trattamento non SEE non soggetto/a al GDPR) può, quindi, essere certificato in relazione alle sue attività di elaborazione dei dati personali ricevuti dall'esportatore GDPR. Lo schema di certificazione GDPR deve garantire un livello di protezione "sostanzialmente equivalente" a quello offerto dalla disciplina europea. Ciò

ISSN 2239-8570

include il rispetto dei principi fondamentali di protezione dei dati, la garanzia di una supervisione indipendente e che gli interessati possano far valere efficacemente i propri diritti, nonché una serie di obblighi per l'importatore e l'esportatore GDPR di monitorare e intervenire quando la legislazione nazionale o la prassi nel paese dell'importatore di dati impediscano il rispetto degli impegni della certificazione. Il Global CBPR System, invece, non è istituito esclusivamente come strumento di trasferimento di dati, ma rappresenta una certificazione dei principi fondamentali di privacy e protezione dei dati applicabili in tutte le giurisdizioni interessate. I requisiti del Global CBPR Program che supportano una certificazione sono comuni a tutti i membri e, pertanto, condivisi anche dalle organizzazioni certificate che operano in qualsiasi giurisdizione partecipante. Le certificazioni possono essere rilasciate solo da terze parti indipendenti approvate da tutti i membri (Accountability Agent). Per diventare un membro del Global CBPR Forum, e quindi partecipare al Global CBPR System, una giurisdizione deve dimostrare che i requisiti del Global CBPR Program sono applicabili in base alle proprie leggi nazionali. Il Global CBPR System, infine, consente vari modelli di applicazione (anche tramite le Privacy Enforcement Authorities (PEA), gli organismi di applicazione multi-agenzia, una rete di organismi di settore designati, corti e tribunali o una combinazione di quanto sopra, come i Membri ritengono appropriato), in modo che le certificazioni Global CBPR siano vincolanti e applicabili all'interno della giurisdizione in cui un'organizzazione è certificata.

La certificazione Global CBPR e GDPR presentano, però, anche alcune differenze chiave:

– *Esecutività dei diritti degli interessati e ricorso legale*: uno degli obiettivi della certificazione GDPR è garantire diritti esercitabili e rimedi legali efficaci per gli interessati quando i dati personali vengono trasferiti al di fuori dello SEE. A tal fine, la certificazione GDPR consente agli interessati di presentare reclami contro l'importatore di dati presso un'Autorità Garante e di far valere i propri diritti in qualità di beneficiari terzi dinanzi al tribunale della loro residenza abituale o, se del caso, dello stabilimento dell'esportatore GDPR. L'importatore di dati deve assumere impegni vincolanti aggiuntivi (ad esempio tramite contratto tra l'esportatore GDPR e l'importatore di dati) per dare effetto a queste disposizioni. Ai sensi del sistema CBPR globale, invece, la disponibilità di rimedi si basa sulle leggi nazionali dei membri; tutte le organizzazioni certificate sono comunque tenute a stabilire procedure per ricevere e rispondere ai reclami individuali e gli "Accountability Agent" devono prevedere sistemi di risoluzione delle controversie per i reclami dei consumatori e al fine di far rispettare i requisiti di certificazione nei confronti delle organizzazioni certificate. Tutte le giurisdizioni partecipanti devono avere un'autorità di controllo per i requisiti del programma CBPR globale, che devono aderire al CAPE globale, un accordo tra i regolatori per cooperare in materia di controllo.

ISSN 2239-8570

– *Supervisione indipendente:* il GDPR stabilisce che vengano istituite autorità garanti pubbliche indipendenti; la certificazione GDPR richiede quindi esplicitamente all'importatore di dati nel paese terzo di collaborare con l'autorità competente, di accettare di essere sottoposto a verifica e ispezione, di tenere conto delle indicazioni e di conformarsi alle decisioni dell'autorità di protezione dei dati. Il sistema CBPR globale richiede alle giurisdizioni di dimostrare l'esistenza di una PEA e il modo in cui la PEA può far rispettare i requisiti del programma CBPR globale nei confronti di organizzazioni certificate e Accountability Agents per attività correlate alla certificazione ai sensi del diritto nazionale.

– *Accesso governativo e misure supplementari*: i due sistemi seguono approcci diversi per quanto riguarda l'accesso governativo ai dati personali detenuti da organizzazioni private certificate. La certificazione GDPR impone obblighi distinti all'importatore di dati certificato in caso di richieste di accesso da parte di autorità di paesi terzi: l'importatore di dati deve informare tempestivamente l'esportatore GDPR, esaminare la richiesta e, quando necessario, contestarne la legittimità e ridurre al minimo le informazioni divulgate. Il sistema CBPR globale richiede che le organizzazioni certificate adottino procedure per rispondere a citazioni, mandati o ordini giudiziari o governativi, compresi quelli che richiedono la divulgazione di informazioni personali, nonché di garantire la necessaria formazione ai propri in merito a questo aspetto, ma non prevede come un'organizzazione debba rispondere o che l'esportatore di dati debba necessariamente essere informato.

– *Limitazioni della conservazione*: da un lato, ai sensi della certificazione GDPR, gli importatori di dati devono rispettare il principio di limitazione della conservazione (art. 5, par. 1, lett. e) e non conservare i dati personali più a lungo del necessario per gli scopi del trasferimento, dall'altro, per quel che concerne il sistema CBPR globale, questo non prescrive la determinazione di criteri atti ad individuare quanto i dati debbano essere cancellati.

– *Notifica di violazione dei dati*: ai sensi della certificazione GDPR, gli importatori di dati che agiscono come titolari del trattamento devono essere soggetti all'obbligo di notificare la violazione di dati personali (data breach) alle autorità di protezione dei dati e, qualora necessario, agli interessati al trattamento. Il sistema CBPR globale non richiede espressamente tale notifica, ma incoraggia i suoi membri ad implementare simili disposizioni nelle leggi nazionali.

– *Decisioni automatizzate (inclusa la profilazione)*: il GDPR prevede regole appositamente stabilite per i processi unicamente automatizzati di dati (art. 22) e l'adozione di specifiche misure di salvaguardia (come il diritto degli individui a ottenere l'intervento umano); tale disciplina non esiste nel sistema CBPR globale.

Infine, si registrano alcune chiare convergenze tra le regole previste dai due sistemi:

ISSN 2239-8570

– *Sicurezza del trattamento*: sia il Global CBPR System che la certificazione GDPR adottano un approccio basato sul rischio per quanto riguarda la sicurezza del trattamento, il che significa che le organizzazioni certificate sono tenute a implementare misure tecniche e organizzative per garantire un livello di sicurezza adeguato ai rischi che il trattamento presenta per gli individui.

– *Trasparenza e diritto all'informazione*: entrambi i sistemi richiedono alle organizzazioni certificate che agiscono come titolari di fornire agli individui determinate informazioni relative alle attività di trattamento prima o al momento della raccolta dei dati. Questo obbligo può essere soggetto a esenzioni che differiscono nei due sistemi. Le organizzazioni certificate sono anche tenute a fornire informazioni sulla certificazione ottenuta.

– *Procedure interne di gestione dei reclami e supervisione interna*: in entrambi i sistemi, le organizzazioni certificate sono tenute a stabilire procedure interne per ricevere e rispondere ai reclami degli interessati ed a dar eventualmente prova, anche in via documentale, della conformità agli obblighi previsti dallo schema di certificazione.

PAOLO GUARDA

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165
https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/g7-roundtable-2024-data-protection-authorities-collaborate-shape-future-ai-and-privacy_en

2024/4(33)CS

33. Il documento *Promoting enforcement Cooperation* del G7 dei Garanti Privacy dell'11.102024

Tra le dichiarazioni approvate l'11 ottobre 2024 durante l'incontro del G7 dei Garamti Privacy (su cui v. *supra* in questo numero di questa Rubrica la notizia n. 29 [2024/4(29)CAT]), i partecipanti hanno adottato la *Promoting enforcement Cooperation*, un documento contenente il reciproco impegno a consolidare le attività di cooperazione multilaterale – tramite la partecipazione a *network* già esistenti o futuri - e bilaterale -tramite protocolli di intesa o azioni congiunte-. Il fine è la promozione della cooperazione tra le Autorità di protezione dei dati anche tramite la condivisione delle rispettive conoscenze ed esperienze a beneficio di una più efficace applicazione della normativa e di controlli più efficienti.

Il documento, dunque, attraverso un sintetico elenco di attività più significative svolte dalle varie Autorità, offre già una prima occasione di condivisione delle loro recenti esperienze di vigilanza in sei aree, individuate come prioritarie per la protezione dei dati: il contesto

ISSN 2239-8570

dell'intelligenza artificiale (AI) e delle tecnologie emergenti; la privacy dei bambini; le tecnologie di geolocalizzazione; la privacy sanitaria; la sicurezza dei dati; la pubblicità *online*.

Tutte le Autorità hanno prestato un crescente impegno per assicurare la protezione dei dati personali nel contesto delle tecnologie emergenti e dell'AI. Le iniziative esemplari segnalate concernono:

- le misure adottate con riguardo ai problemi posti da **ChatGPT**. Sono segnalati, oltre ad un'indagine avviata il 4 aprile 2024 dall'OPC canadese, anche i provvedimenti del GPDP italiano (v. ora il provvedimento n. 755 del 2 novembre 2024, su cui v. in questa Rubrica in questo numero *infra* la notizia n. 44 [2024/4(44)EB] e i due provvedimenti del 30 marzo 2023 e dell'11 aprile 2023, sui quali v. in questa Rubrica la notizia n. 5 nel numero 1/2023 [2023/1(5)SO], e in *Atlante*, p. 303). Vien dato conto, inoltre, della *task force* per intraprendere approcci comuni istituita dall'EDPB con il *Report of the work undertaken by the ChatGPT Taskforce*, del 23 maggio 2024 (su cui v. in questa Rubrica la notizia n. 13 nel numero 2/2024 [2024/2(13)AN]).
- le questioni sollevate dal **riconoscimento facciale**. Si evidenziano l'ordine di cessazione di tale attività nei confronti dei lavoratori impartito nel febbraio 2024 dall'Autorità del Regno Unito (ICO) alla società Serco Leisure, e le indagini avviate dalla CNIL francese nel febbraio 2024 riguardo l'utilizzo di telecamere intelligenti da parte di autorità locali e nei giochi olimpici. Vien dato conto, inoltre, delle Istruzioni sull'uso di sistemi di telecamere con funzioni di riconoscimento facciale per prevenire la criminalità e garantire la sicurezza adottate dalla PPC giapponese nel marzo 2023.
- la protezione dei dati in relazione all'**AI generativa**. Sono richiamati sul punto gli atti adottati dall'Autorità giapponese nel 2023 (PPC: Avvertenze sull'uso dell'Intelligenza artificiale generativa) e dall'EDPS il 3 giugno 2024: il documento *Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems* (sul quale v. in questa Rubrica la notizia n. 14 sul numero 2/2024 [2024/2(14)BG]).
- il **rapporto tra algoritmi, intelligenze artificiali e principî del trattamento dei dati**. Sul punto viene condivisa l'esperienza della denuncia del 31.5.2023 della Federal Trade Commission (FTC) statunitense contro Amazon per l'assistente vocale 'Alexa' in relazione alle normative a protezione dei minori e dei consumatori per la conservazione a tempo indeterminato delle registrazioni vocali di bambini (su cui v. in questa Rubrica la notizia n. 11 nel numero 2/2023 [2023/2(11)LV] e in *Atlante*, p. 359), e contro Rite Aid nel dicembre 2023 ed Everalbum nel 2021 in relazione al trattamento illecito e discriminatorio dei dati con algoritmi.

Le Autorità hanno inoltre condiviso le loro esperienze sul monitoraggio della corretta tutela dei dati personali dei bambini, destinatari di forme di garanzia più intense. Vien dato atto della storica sanzione di 275 milioni di dollari ad Epic Games, creatore del videogioco **Fortnite**, conseguente all'indagine della FTC statunitense per violazioni della *Children's Online*

ISSN 2239-8570

Privacy Protection Rule in ragione, tra l'altro, della raccolta dei dati di minori di tredici anni senza consenso dei genitori. Sono riferite diverse azioni delle varie Autorità contro il Social Network **TikTok** (tra esse delle Autorità canadese OPC e dell'Autorità del Regno Unito ICO, e della FTC statunitense). Il tema dell'implementazione dei meccanismi di controllo dell'età è stata oggetto dell'attenzione della CNIL francese nel quadro delle sue più ampie indagini dell'anno 2024 sulla raccolta *online* dei dati dei minori. Viene dato conto, infine, dell'impegno dell'EDPS nella valutazione del rispetto dei principi di necessità e proporzionalità del trattamento dei dati personali dei minori di 15 anni da parte delle forze dell'ordine.

Anche quello dei rischi derivanti dal tracciamento delle persone tramite dati di **geolocalizzazione** è stato oggetto di condivisione di esperienze di vigilanza delle Autorità. L'ICO del Regno Unito riporta il caso delle sanzioni irrogate nel marzo 2024 al Ministero dell'Interno per violazioni della legge sulla protezione dei dati dal progetto pilota per il **monitoraggio elettronico GPS dei migranti**; l'FTC americana quello delle contestazioni alla **vendita dei dati di geolocalizzazione effettuata senza consenso informato degli utenti** da parte di un broker di dati, **Kochava Inc.**; la CNIL francese quelli delle sanzioni irrogate, tra l'ottobre e il novembre 2023, per le illegittime attività **di geolocalizzazione dei veicoli utilizzati da lavoratori dipendenti**, e quello del sanzionamento, il 16 marzo del 2023, di una **società di scooter-noleggio** per aver strutturato il trattamento dei dati di geolocalizzazione degli utenti in modo quasi permanente in violazione del principio di minimizzazione. L'esperienza riferita dall'OPC Canadese riguarda le contestazioni mosse nel 2022 alla società titolare della nota **catena di caffè e fast-food canadesi, Tim Hortons**, per aver tracciato costantemente i clienti con la propria app, senza uno scopo appropriato e senza valido consenso, trattando i loro dati di geolocalizzazione anche quando l'app era chiusa.

Con riferimento alle azioni in materia di c.d. privacy sanitaria sono state condivise le esperienze della FTC statunitense, che ha emesso provvedimenti contro fornitori di piattaforme per servizi sanitari per la **condivisione di dati sanitari con altre società a scopo pubblicitario** (provvedimenti contro BetterHelp e contro GoodRx); della BfDI tedesca, che ha imposto alle compagnie di assicurazione sanitaria di fornire **cartelle cliniche elettroniche conformi al GDPR** e non solo al diritto nazionale in materia; della CNIL francese, che ha sanzionato il titolare di un sito web, **Doctissimo**, su temi della salute per diverse inosservanze del GDPR, in particolare in relazione a cookies e al requisito del **consenso al trattamento dei dati sanitari**. Viene inoltre dato conto di più ampie iniziative della CNIL, che nel 2022 e nel 2023 ha avviato indagini in tema di cartella clinica elettronica, e della pubblicazione da parte del PPC giapponese nel 2022 di una Guida sulla fuga di dati.

La **sicurezza dei dati** è stata riconosciuta come tema di rilevante interesse sul quale la cooperazione tra le Autorità potrebbe risultare particolarmente fruttuosa, vista la somiglianza dei quadri giuridici in questo ambito. Anche per tale aspetto sono state segnalate le misure adottate da alcune Autorità in relazione a violazioni della normativa sulla protezione dei

ISSN 2239-8570

dati personali (PPC giapponese, BfDI tedesca, l'ICO britannica). In questo quadro si segnala la posizione della FTC statunitense, che, nel procedimento a carico della società **Blackbaud** del 2024, ha riconosciuto le misure di minimizzazione dei dati come un pilastro per garantire la sicurezza dei dati.

Infine, la condivisione di esempi di azioni svolte in tema di **pubblicità online**, oltre a riferire di una sanzione dell'Autorità francese ad una **società di retargeting comportamentale** per violazione della normativa in tema di consenso e trasparenza (cfr. il provvedimento della CNIL contro **Criteo** del 15 giugno 2023), e degli inviti della ICO del Regno Unito rivolti alla maggioranza dei siti web più importanti del Regno Unito a conformarsi alla normativa in tema di consenso ai cookie pubblicitari, ha dato conto dell'avvio dell'*iter* per la definizione di una proposta di regolamento in materia di sorveglianza commerciale da parte della FTC statunitense.

CARLA SOLINAS

https://www.garanteprivacy.it/documents/10160/0/Roundtable+of+G7+Data+Protection+and+Privacy+Authorities+2024+-+Promoting+Enforcement+Cooperation.pdf/8d3aebb6-d50e-c553-5d69-9aa4f6a19c0b?version=1.1

2024/4(34)ST

34. Le Linee Guida in materia di intelligenza artificiale della Pontificia Commissione dello Stato di Città del Vaticano del 16.12.2024

Con il decreto numero DCCII della Pontificia Commissione dello Stato Città del Vaticano del 16 dicembre 2024 - entrato in vigore il 1 gennaio 2025 - sono state promulgate le Linee guida in materia di intelligenza artificiale (di seguito **Linee Guida**).

Un ruolo centrale delle Linee guida è attribuito all'esigenza di garantire eticità nell'orientamento delle scelte che riguardano la diffusione e l'uso dei sistemi di intelligenza artificiale.

Le Linee guida, che si compongono di 15 articoli, accolgono l'invito, fatto in più occasioni da Papa Francesco, di considerare che l'IA influenza in modo dirompente l'economia, la società, la qualità della vita, le relazioni tra persone e tra Paesi e la stabilità internazionale. Pertanto occorre che l'IA come altri "utensili" creati dall'uomo rimanga "uno strumento" nelle sue mani.

In particolare, le Linee Guida recano principi generali tesi a valorizzare e promuovere l'utilizzo etico e trasparente dell'intelligenza artificiale, in una dimensione antropocentrica e affidabile, nel rispetto della dignità umana e del bene comune.

La struttura delle Linee Guida è molto più semplice rispetto all'articolato e complesso Regolamento (UE) 2024/1689 sull'intelligenza artificiale, ma non rinuncia alle definizioni che troviamo nell'art. 2 dove leggiamo che si

ISSN 2239-8570

intende per: «intelligenza artificiale»: l'insieme di sistemi e modelli computazionali che, attraverso processi automatizzati, sono in grado di analizzare dati, apprendere da essi, prendere decisioni ed eseguire compiti che di norma richiederebbero l'intelligenza umana; per «sistema di intelligenza artificiale»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dai dati analizzati che riceve come generare risposte quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali; per «modelli di intelligenza artificiale»: sistemi di software e hardware che, attraverso l'utilizzo di tecniche di apprendimento automatico e la capacità di identificare strutture ricorrenti in collezione di dati, sono in grado di eseguire compiti e attività tipicamente associati all'intelligenza umana; per «dato»: qualsiasi informazione, atto o fatto rappresentati in forma digitale; per «dati biometrici»: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici; per «rischio»: l'utilizzo del dato nell'ambito del sistema di intelligenza artificiale e dei modelli di intelligenza artificiale che esponga ad un'elevata probabilità del verificarsi di un danno.

La struttura più semplice delle Linee Guida è legata anche al riferimento ai Principi fondamentali dell'art.3, il cui rispetto deve essere assicurato nello svolgimento delle attività nell'ambito della sperimentazione, dello sviluppo, dell'adozione e dell'utilizzo di sistemi e modelli di intelligenza artificiale. Lo svolgimento di dette attività deve essere conforme al rispetto della dignità umana, del bene comune e ispirato ai principi di responsabilità etica, trasparenza e proporzionalità dell'azione amministrativa.

I sistemi e i modelli di intelligenza artificiale devono essere sviluppati e applicati garantendo la sicurezza dello Stato della Città del Vaticano, la protezione e la riservatezza dei dati personali, la non discriminazione dell'essere umano, la sostenibilità economica e la cura del Creato.

Non meno importanza è attribuita alla verifica e vigilanza sui processi di trattamento e gestione del dato nell'ambito dello sviluppo e applicazione di sistemi e modelli di intelligenza artificiale, affinché i risultati siano corretti, attendibili, appropriati ed ottenuti secondo i principi di trasparenza e proporzionalità.

Gli Organismi operativi, scientifici e gli Organi giudiziari, nel rispetto della dimensione antropocentrica nell'utilizzo dei sistemi e dei modelli di intelligenza artificiale, devono garantire la vocazione dell'intelligenza artificiale al servizio dell'uomo, preservando il rispetto dell'autonomia e del potere decisionale dell'umano.

In linea con i principi fondamentali dell'art. 3 delle Linee Guida sono i divieti di utilizzo dell'intelligenza artificiale di cui all'articolo 4. Sono vietate, infatti, le seguenti pratiche: a) l'uso di un sistema di intelligenza artificiale per trarre deduzioni generali di ordine antropologico con effetti discriminatori sulla persona; b) l'uso di un sistema di intelligenza artificiale che utilizzi tecniche di manipolazione subliminale idonee a provocare alla persona o a un gruppo di persone un danno fisico o psicologico; c) l'uso di

ISSN 2239-8570

un sistema di intelligenza artificiale che precluda alle persone con disabilità di accedere all'intelligenza artificiale e alle relative funzionalità ed applicazioni; d) l'uso di un sistema di intelligenza artificiale che, attraverso il trattamento del dato, crei disuguaglianze sociali, degradando la dignità umana e violando i principi fondamentali dell'uomo; e) l'uso di un sistema di intelligenza artificiale atto a compromettere la sicurezza dello Stato della Città del Vaticano e delle aree di cui agli articoli 15 e 16 del Trattato Lateranense

e il mantenimento dell'ordine pubblico e ad incentivare la proliferazione di condotte delittuose; f) l'uso di un sistema di intelligenza artificiale le cui finalità si pongano in contrasto con la missione del Sommo Pontefice, l'integrità della Chiesa cattolica e il corretto svolgimento delle attività istituzionali del Governatorato dello Stato della Città del Vaticano; g) l'uso di un sistema di intelligenza artificiale che si ponga in contrasto con le Linee Guida.

L'attenzione alla persona, alla sua dignità, alla non discriminazione e alla non diseguaglianza sociale, sono posti come principi cardine. Quanto detto pare confermato anche dall'art. 5 che delinea i principi in materia di informazione e trattamento dei dati e prevede, non solo che la circolazione delle informazioni, l'elaborazione del dato e il trattamento dei dati personali mediante utilizzo dell'intelligenza artificiale, non debba arrecare pregiudizio alla veridicità, alla libertà di espressione, all'imparzialità e alla completezza, ma anche che la circolazione delle informazioni, l'elaborazione del dato e il trattamento dei dati personali mediante sistemi e modelli di intelligenza artificiale non debba essere finalizzato a produrre effetti discriminatori, a ledere la dignità umana e a danneggiare l'immagine dello Stato della Città del Vaticano e della Chiesa cattolica.

Il Capo II delle Linee Guida si affida a Principi generali per materia e, dopo aver delineato i principi in materia di informazione e trattamento dei dati, si occupa dei Principi in materia di ricerca scientifica e sanità; protezione del diritto di autore; beni culturali; infrastrutture e servizi; procedure amministrative; lavoro; attività giudiziaria e di sicurezza.

Quanto ai Principi in materia di ricerca scientifica e sanità, si prevede che si possa

favorire l'introduzione di sistemi e modelli di intelligenza artificiale che contribuiscano al miglioramento della cura della salute della persona e della tutela della sanità e igiene pubblica, a condizione che ciò avvenga nel rispetto dei diritti umani, delle libertà fondamentali e della protezione nel trattamento dei dati personali.

Occorre garantire, da una parte, che chi usufruisce delle prestazioni sanitarie sia informato sull'utilizzo dei sistemi di intelligenza artificiale applicati. Da altra parte, si richiede che i sistemi di intelligenza artificiale sviluppati ed applicati nell'ambito della ricerca scientifica e della sanità, non arrechino pregiudizio o limitazioni alla valutazione decisionale degli esercenti la professione medica.

Quanto ai Principi in materia di protezione del diritto di autore, si richiede il rispetto della Legge sulla protezione

ISSN 2239-8570

del diritto di autore sulle opere di ingegno e dei diritti connessi (n. CXCVII, 1° settembre 2017) e la identificazione dei contenuti mediante l'acronimo "IA".

Con riferimento ai Principi in materia di beni culturali, le Linee Guida, all'articolo 8, prevedono che si possa favorire l'introduzione di sistemi e modelli di intelligenza artificiale purché contribuiscano al miglioramento della conservazione, gestione, valorizzazione e fruizione del patrimonio artistico – museale. Con riferimento all'utilizzo dell'intelligenza artificiale nell'ambito dell'attività di restauro dei beni culturali, si richiede che ciò avvenga nel rispetto dei principi di metodo riconosciuti a livello internazionale.

In materia di infrastrutture e servizi, i principi delineati dalle Linee Guida prevedono che il Governatorato dello Stato della Città del Vaticano possa avvalersi di sistemi e modelli di intelligenza artificiale al fine di incentivare la sostenibilità economica ed ambientale nell'ambito dell'esecuzione degli interventi infrastrutturali e dell'erogazione dei servizi. Detti sistemi, però, non devono arrecare pregiudizio o limitazioni alle valutazioni decisionali dei soggetti individuati dall'Amministrazione quali responsabili dell'esecuzione delle attività.

Di particolare interesse anche l'art. 10 delle Linee Guida che detta i Principi in materia di procedure amministrative prevedendo espressamente la possibilità di avvalersi dell'intelligenza artificiale al fine di favorire il processo di semplificazione dei procedimenti, di ridurre i tempi di definizione dei procedimenti medesimi, di innalzare i livelli prestazionali dell'azione amministrativa, garantendo agli interessati la conoscibilità degli interventi regolatori. L'utilizzo dell'intelligenza artificiale nella materia delle procedure amministrative, deve conformarsi, oltre al rispetto dei principi fondamentali generali delineati dallo stesso Decreto, anche ai seguenti principi: a) eticità nell'orientamento delle scelte amministrative; b) trasparenza, economicità, efficacia, efficienza e risultato; c) segregazione delle funzioni e buon andamento dell'azione amministrativa. Si introduce un importante principio di responsabilità ai sensi del quale l'uso dell'intelligenza artificiale nella materia delle procedure amministrative, deve avvenire nel rispetto dell'autonomia e del potere decisionale della persona che resta l'unica responsabile dei provvedimenti e dei procedimenti in cui sia stata utilizzata l'intelligenza artificiale. L'utilizzo dell'intelligenza artificiale deve cioè svolgere una funzione strumentale e di supporto nelle attività amministrative, al fine di valorizzare competenze ed attitudini delle risorse umane. Principi analoghi regolano la materia del lavoro, ove si specifica altresì, all'art. 11 delle Linee Guida, che nell'ambito delle procedure di selezione del personale, la sperimentazione e applicazione dei sistemi e modelli di intelligenza artificiale deve avvenire nel rispetto del principio di trasparenza, prevenendo ogni violazione della dignità umana e potenziali effetti discriminatori tra i partecipanti alla procedura di selezione.

La centralità della persona umana è ribadita anche dall'articolo 12, Principi in materia di attività giudiziaria, ove si prevede che i sistemi di intelligenza artificiale possano essere utilizzati esclusivamente per l'organizzazione e semplificazione del lavoro giudiziario, nonché per la

ISSN 2239-8570

ricerca giurisprudenziale e dottrinale. Ne consegue che è riservata esclusivamente al magistrato la decisione sulla interpretazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione di ogni provvedimento.

Le Linee Guida sembrano perseguire, con un approccio semplice ma efficace, un utilizzo responsabile dell'Intelligenza artificiale, con attenzione alle opportunità, ma anche nella consapevolezza dei rischi.

SARA TOMMASI

https://www.vaticanstate.va/images/N.%20DCCII.pdf

2024/4(35)LS

35. Lo studio del World Economic Forum sulla governance della IA generativa dell'ottobre 2024: la necessità di un quadro normativo a 360°

L'8 ottobre 2024, il World Economic Forum ha pubblicato uno studio che propone un approccio a 360° per costruire una governance capace, da un lato, di mitigare i rischi posti dalle nuove tecnologie e, dall'altro lato, di supportare e incentivare lo sviluppo di un'IA generativa rispettosa dei diritti umani (lo **Studio**). Nello specifico, lo Studio ha l'obiettivo di fornire ai responsabili politici e ai regolatori un quadro di governance pratico, dettagliato e attuabile per tale tecnologia basato su tre pilastri fondamentali e rispettivamente: "**imbrigliare il passato**" (*to harness the past*); "**costruire il presente**" (*to build the present*) e "**pianificare il futuro**" (*to plan the future*).

Il primo richiede di esaminare le regolamentazioni nazionali già esistenti per verificarne l'adeguatezza rispetto ai rischi posti dall'IA generativa sotto tre diversi punti di vista.

Innanzitutto, si afferma la necessità di studiare l'impatto che quest'ultima ha sulle legislazioni per capire se esse possano ancora trovare applicazione – e se debbano essere adattate di conseguenza – ovvero direttamente superate perché non più idonee ad affrontare adeguatamente le sfide dell'IA generativa. Tra queste, il World Economic Forum fa specifico riferimento alla **protezione della privacy e dei dati personali**; ai **diritti di proprietà intellettuale**; ai **consumatori**, alla **responsabilità da prodotto** e, infine, alla **concorrenza**.

Per mitigare le criticità di ciascuna, vengono poi elencate, a mero titolo esemplificativo, alcune strategie. Ad esempio, rispetto al problema della mancanza di una base giuridica per la raccolta e il conseguente trattamento dei dati personali – utilizzati come dataset per allenare l'IA generativa – si propone quale possibile soluzione l'**adozione di meccanismi di opt-in/out e la concessione di licenze** che potrebbero contribuire alla formazione di standard che i produttori e i fornitori di sistemi di IA sarebbero obbligati a rispettare. Un altro caso particolarmente problematico è anche la capacità di

ISSN 2239-8570

tali sistemi di aumentare le economie di scala e, conseguentemente, di rafforzare la concentrazione dei mercati. Al riguardo, gli autori ritengono utile incentivare studi settoriali e consultazioni con gli stakeholders per fornire loro una conoscenza mirata sulle dinamiche competitive dei mercati e sull'impatto della tecnologia su di esse.

Inoltre, questo primo pilastro considera anche che la natura multidisciplinare dell'IA comporti inevitabilmente l'**applicazione contestuale di diverse regolamentazioni** che possono sovrapporsi ed entrare in conflitto tra loro. Ciò può determinare il rischio di un quadro normativo poco chiaro per tutti gli attori coinvolti. Dunque, il report sottolinea come i legislatori debbano individuare e **risolvere le eventuali tensioni tra i diversi sistemi regolatori** come elemento fondamentale per garantire un quadro giuridico ben definito.

Tuttavia, per poter raggiungere tale scopo è necessario che vengano sviluppate tecnologie realmente affidabili. Perciò, **occorre che siano correttamente allocate le responsabilità legali dei partecipanti la catena di distribuzione** di tali sistemi. Al riguardo, il gruppo di esperti incentiva l'adozione di linee guida per chiarire i gradi di responsabilità per i diversi ruoli lungo l'intero ciclo di vita dell'IA generativa, pena la perdita di fiducia degli investitori e degli utilizzatori. Tra i vari approcci che possono essere utilizzati sul tema lo studio richiama, a titolo puramente esemplificativo, il c.d. **"case-based review"**. Quest'ultimo, con l'intento di assicurare la prevedibilità, dispone che vengano fornite indicazioni generali circa le modalità di attribuzione in astratto delle responsabilità e, al contempo, incentiva l'adozione di meccanismi capaci, in concreto, di far fronte alla complessità delle diverse situazioni. Inoltre, come ulteriore strategia, si sottolinea l'importanza di dotarsi di una **terminologia comune** in materia. Per evitare, poi, la **disparità di trattamento tra i vari partecipanti la catena di distribuzione dell'IA**, si propone ai legislatori di capire il tipo di controllo, l'influenza e le risorse che ciascuno di essi ha avuto nonché considerare se possa essere funzionale utilizzare terze parti per certificare l'affidabilità dell'IA. Non solo, un altro aspetto fondamentale è assicurare la **trasparenza dei sistemi**, che è possibile realizzare attraverso documentazione e meccanismi di tracciabilità (così da risalire all'origine dei risultati), standard tecnici per l'ingresso nel mercato nonché la creazione di comitati settoriali di revisione e di audit indipendenti.

Una volta risolti eventuali divari e sovrapposizioni tra le regolamentazioni in materia, occorre poi che esse siano efficacemente applicate. Nel merito, due sono le opzioni possibili: attribuire nuove competenze settoriali ad **autorità pubbliche già esistenti oppure** costituirne direttamente di **nuove** specificamente dedicate. Tuttavia, sebbene quest'ultima soluzione venga sostenuta da chi ritiene che la creazione di un'agenzia centralizzata sull'IA sia l'unico modo possibile per affrontare il fenomeno digitale, altri la criticano perché meno efficace. Piuttosto, molti preferirebbero un organismo con competenze simili a un **consiglio per coordinare e coadiuvare le autorità nazionali già esistenti**.

Il secondo pilastro verte, invece, sulla necessità di adottare un approccio multidisciplinare che consenta di costruire e **condividere un patrimonio di**

ISSN 2239-8570

conoscenze comuni sull'IA generativa grazie alla **collaborazione tra l'industria** (in quanto più prossima alla tecnologia)**, l'accademia e le organizzazioni della società civile** (OSC).

Per raggiungere tale obiettivo, gli autori suggeriscono ai governi alcune strategie per incoraggiare le imprese a adottare **pratiche di IA sostenibili e responsabili**.

Tra queste, si propone di riconoscere **incentivi finanziari** come agevolazioni fiscali e sovvenzioni per la ricerca, lo sviluppo e la formazione su tale tecnologia. Inoltre, si invitano i legislatori a fissare chiaramente gli **obiettivi** in materia in modo da ridurre l'ambiguità sul quadro giuridico applicabile e predisporre delle **linee guida** per aiutare gli operatori a sviluppare sistemi tecnologici rispettosi delle politiche statali. Ad esempio, particolarmente utile risulterebbe la creazione di **standard tecnici** per stabilire metodologie e parametri di riferimento comuni **per valutare le prestazioni**, **la sicurezza e la conformità etica** dei sistemi di IA. A tal fine, il report ritiene essenziale assicurare la coordinazione e incentivare il lavoro e la ricerca multidisciplinari così da **creare un patrimonio di conoscenze open-source**. Al riguardo, gli autori richiedono, ad esempio, di **consentire agli studenti e ai ricercatori l'accesso alle infrastrutture (fisiche e digitali) e ai dati** nonché di fornire loro regolarmente materiale di studio aggiornato alle evoluzioni dell'IA. In più, si sottolinea come le attuali **differenze salariali tra chi lavora in accademia e chi in industria** spingano sempre più ad abbandonare la ricerca. Per contrastare detto fenomeno, sarebbe utile altresì prevedere **sussidi** per progetti volti ad affrontare le sfide delle tecnologie avanzate e a finanziare corsi di formazione specifici sull'IA.

Infine, il World Economic Forum reputa che anche le **OSC** possano offrire un valido aiuto in quanto capaci di fornire delle valutazioni indipendenti sull'impatto sociale dell'IA. Perciò, si spingono, da un lato, i regolatori a fornire a questi organismi ingenti finanziamenti e, dall'altro lato, l'industria a condividere con essi i dati raccolti.

Il terzo pilastro offre invece una prospettiva sul futuro dell'IA e analizza alcune delle principali sfide che i governi saranno chiamati ad affrontare per arginare i rischi di tale tecnologia per la società.

Innanzitutto, nello Studio **si invitano i regolatori ad assumere specialisti di IA** e, al contempo, a dotare di competenze specifiche coloro che già lavorano in tale settore.

Inoltre, essi dovrebbero anche **monitorare lo sviluppo delle nuove tecnologie e le loro interazioni con la società in modo da prevedere i potenziali rischi rispetto alle libertà fondamentali**. Sul punto, particolarmente **preoccupante è il fenomeno dell'IA emozionale**, che comprende sistemi sviluppati per riconoscere, interpretare e adattare le risposte alle emozioni umane. Questa tipologia di IA solleva diverse preoccupazioni, perché **capace di manipolare e creare un senso di dipendenza affettiva nell'utilizzatore**. Pertanto, i regolatori dovrebbero elaborare strategie efficaci per contrastare tali pericoli, lavorando anche in collaborazione con l'accademia e l'industria. Tra le soluzioni più efficaci a tal fine, gli autori dello Studio suggeriscono la predisposizione di

ISSN 2239-8570

valutazioni di impatto, l'adozione di regolamentazioni più snelle nonché una politica di previsione strategica per affrontare con metodo più scientifico e rigoroso le sfide future.

Il report ricorda poi come il carattere transnazionale dell'IA richieda necessariamente che tale fenomeno venga affrontato con approccio olistico.

In quest'ottica, l'ultimo punto che viene analizzato sottolinea l'importanza della **cooperazione internazionale** senza la quale il rischio è quello di un quadro giuridico frammentato e di un diverso grado di sviluppo dell'IA tra i vari Stati. In particolare, la cooperazione internazionale è particolarmente essenziale **in sei settori**, ossia: **i)** nell'elaborazione di standards che possano essere azionati facilmente; **ii)** nell'implementazione di misure di sicurezza tecniche e nel coordinamento tra i diversi organismi preposti a tal fine; **iii)** nell'identificazione proattiva di rischi e opportunità da attuare, ad esempio, attraverso la costituzione di un osservatorio internazionale appositamente dedicato; **iv)** nella collaborazione per la predisposizione di trattati e altri strumenti per costruire norme che stabiliscano precisamente divieti nella ricerca, sviluppo e utilizzo dell'IA in quanto la mancanza di un chiaro allineamento giuridico aumenta la probabilità che tali tecnologie vengano utilizzate impropriamente; **v)** nella condivisione di competenze specifiche sull'IA da realizzarsi attraverso, ad esempio, la costituzione di una piattaforma globale che permetta di condividere con gli stakeholders le best practices e i casi studio per attuare una governance dell'IA responsabile e consapevole; **vi)** nella condivisione da parte dei paesi sviluppati di infrastrutture e risorse per consentire ad ogni nazione di costruire un bagaglio di conoscenze sull'IA e di partecipare proattivamente ai forum internazionali. A tal fine, si propone ai regolatori di considerare meccanismi di condivisione multilaterale, di proprietà condivisa, di calcolo e di dati.

In conclusione, lo Studio afferma l'esigenza, prima di introdurre nuove regolamentazioni sull'IA, di valutare l'attuale quadro normativo e di migliorare il coordinamento tra le varie normative di settore per ridurre i rischi causati dall'IA generativa. A detta degli autori dello Studio, le autorità regolatorie esistenti dovrebbero essere valutate rispetto alle loro capacità di rispondere alle sfide legate a tale tecnologia e dovrebbe essere considerata attentamente la possibilità di addivenire a un compromesso tra una governance distribuita e una fondata sulla creazione di un'agenzia appositamente nominata.

In ogni caso, si afferma chiaramente la necessità di un approccio olistico, vale a dire che coinvolga tutta la società, che promuova la collaborazione tra l'industria, la società civile e l'accademia e che fornisca soluzioni interdisciplinari. In altri termini, solo attraverso una politica armonizzata, basata sulla condivisione di conoscenze comuni, sulla cooperazione internazionale e su pratiche standardizzate sarà possibile affrontare le preoccupazioni poste dall'IA generativa in modo più efficace a livello globale.

LUDOVICA SPOSINI

ISSN 2239-8570

https://www3.weforum.org/docs/WEF_Governance_in_the_Age_of_Generative_AI_2024.pdf

2024/4(36)FP

36. Lo studio del Financial Stability Board del 14.11.2024 sulle implicazioni di stabilità finanziaria dell'intelligenza artificiale

Il 14 novembre 2024 il Financial Stability Board (**FSB**) ha pubblicato un report relativo al crescente utilizzo dell'intelligenza artificiale nel settore finanziario e alle sue potenziali ripercussioni sulla stabilità del sistema: "*The Financial Stability Implications of Artificial Intelligence*" (lo **Studio**). Lo Studio aggiorna il precedente report del 1 novembre 2017 sull'utilizzo dell'IA e del machine learning nel settore finanziario, al fine di dar conto delle nuove prassi e delle iniziative sviluppatesi, nel tempo, a livello nazionale.

Il settore finanziario si è da sempre contraddistinto come un ambito particolarmente adatto alla sperimentazione nell'uso delle nuove tecnologie e questa tendenza è stata confermata anche dalla rapidissima diffusione dei sistemi di intelligenza artificiale. Lo Studio segue la definizione adottata dall'OECD (OCSE) di IA come "machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (OECD, AI Principles, 2024).

Negli ultimi anni, l'IA, in particolare quella generativa (**GenAI**) e quella che fa uso di modelli linguistici di grandi dimensioni (**LLM**), ha registrato un picco di incremento nel suo utilizzo in ambito finanziario, così come una progressiva diversificazione dei suoi impieghi. Questo fenomeno è stato alimentato da progressi nel deep learning, dalla disponibilità di big data e dall'aumento della potenza computazionale, insieme a miglioramenti significativi di software e hardware. La raccolta di grandi quantità di dati non strutturati, i progressi nel cloud computing e l'uso diffuso di modelli di IA pre-addestrati rendono particolarmente complessa l'analisi di questo fenomeno.

L'adozione dell'IA nel settore finanziario è influenzata da una combinazione di fattori che riguardano tanto il lato dell'offerta, quanto quello della domanda. Con riferimento ai primi, i progressi nel deep learning e le tecniche che si avvalgono di reti neurali profonde hanno migliorato le capacità dell'IA, consentendo applicazioni più sofisticate. La disponibilità di grandi volumi di dati ha permesso l'addestramento di modelli di IA più accurati e complessi. L'aumento della potenza di calcolo, in particolare attraverso l'uso di unità di elaborazione grafica (**GPU**) e unità di elaborazione tensoriale (**TPU**), ha accelerato l'addestramento e l'implementazione dei modelli di IA. Innovazioni come il Transformer – un'architettura di deep learning in grado di differenziare il significato delle parole a seconda del contesto di riferimento e di predire lo sviluppo di un testo – hanno migliorato le prestazioni dei modelli di IA, mentre i progressi

ISSN 2239-8570

nell'hardware hanno reso più efficienti i processi di calcolo. L'accesso al cloud ha reso inoltre più economico e scalabile l'uso dell'IA, permettendo alle istituzioni finanziarie di sfruttare risorse computazionali senza investimenti significativi in infrastrutture. L'uso di modelli pre-addestrati ha infine ridotto i costi e i tempi di sviluppo, facilitando l'adozione dell'IA anche in realtà meno strutturate.

Dal lato della domanda, l'impiego dell'IA va incontro alla ricerca, da parte delle istituzioni finanziarie, di strumenti in grado di migliorare la propria efficienza operativa, attraverso l'automazione e l'ottimizzazione dei processi. L'IA consente la creazione di prodotti finanziari personalizzati, migliorando l'esperienza del cliente e rendendola più adatta alle sue esigenze. L'IA offre inoltre strumenti avanzati per l'analisi del rischio e la compliance al quadro normativo vigente. La necessità di rimanere competitivi spinge così un sempre maggior numero di intermediari a effettuare nuovi investimenti per potenziare le proprie infrastrutture tecnologiche attraverso l'uso di IA. Questa tendenza espansiva non coinvolge esclusivamente i soggetti regolati, ma anche le autorità di regolazione, le quali fanno correntemente uso delle tecnologie di IA per lo svolgimento dei propri incarichi di supervisione (c.d. **SupTech**), come per il caso dei software che individuano manipolazioni di mercato.

Il report approfondisce alcuni specifici casi applicativi dell'uso di IA nel settore finanziario. La mancanza di una mappatura completa di dati rende difficile una valutazione approfondita e quantitativa, sebbene le evidenze disponibili suggeriscano un'accelerazione significativa nell'uso dell'IA, specie nell'arco temporale intercorso dal primo report. La maggior parte dei casi d'uso si concentra sul miglioramento delle operazioni interne e sulla compliance normativa, mentre le applicazioni che generano nuovi flussi di entrate non sono ancora ampiamente diffuse. L'IA viene utilizzata per automatizzare processi ripetitivi, riducendo i costi operativi e minimizzando gli errori umani. Gli algoritmi di IA analizzano grandi volumi di dati per identificare tendenze di mercato, comportamenti dei clienti e opportunità di investimento. L'IA aiuta a monitorare le transazioni per rilevare attività fraudolente e garantire la conformità alle normative. I chatbot basati su IA forniscono assistenza ai clienti, migliorando l'efficienza e la soddisfazione. I "robo-advisor" offrono consulenza sugli investimenti basata su algoritmi, rendendo i servizi finanziari più accessibili e a minor costo. Questa tendenza espansiva nell'utilizzo dell'IA ha coinvolto anche nuove applicazioni di LLM e GenIA in ambito finanziario. I modelli linguistici sono in grado di sintetizzare documenti complessi, facilitando l'analisi delle informazioni. L'IA migliora la capacità di recuperare informazioni pertinenti da grandi dataset e assiste nella scrittura di codici, accelerando lo sviluppo di software di analisi finanziaria.

I vantaggi apportati dalla diffusione dei sistemi di IA non devono tuttavia indurre a trascurare, secondo l'FSB, i rischi legati all'esacerbarsi di vulnerabilità già esistenti, così come alla creazione di nuovi fattori di instabilità.

Molte istituzioni finanziarie dipendono da un numero ristretto di fornitori di IA e infrastrutture cloud, il che potrebbe aumentare il rischio di

ISSN 2239-8570

propagazione in caso di malfunzionamenti o attacchi informatici. Un'interruzione dei servizi di un fornitore chiave potrebbe avere effetti a catena su tutto il sistema finanziario. La diffusione di modelli di IA comuni tra diverse istituzioni può inoltre indurre alla costruzione di pattern decisionali simili, aumentando la correlazione tra assets e amplificando l'effetto contagio delle crisi. Se molte istituzioni reagissero simultaneamente a un segnale di trading generato da un algoritmo, ciò potrebbe aggravare la volatilità dei mercati. Gli strumenti di IA possono essere utilizzati anche per generare attacchi informatici sofisticati, deepfake e frodi su larga scala, con rischi legati principalmente alla compromissione dei dati. L'FSB sottolinea poi la problematica legata alla qualità e trasparenza dei dati. Molti modelli di IA si basano su dati non strutturati e fonti di informazione opache, che rendono difficile valutarne l'affidabilità delle previsioni generate. Inoltre, l'assenza di una governance solida potrebbe portare allo sviluppo di *bias* decisionali e forme di discriminazione. Infine, la diffusione di sistemi di IA, in ambito finanziario così come in altri settori, ha un importante effetto trasformativo sul mercato del lavoro, per via dell'automatizzazione di compiti tradizionalmente svolti da esseri umani e della corrispondente riduzione della necessità di determinati profili professionali.

Per mitigare questi rischi, l'FSB rivolge una serie di raccomandazioni a regolatori e istituzioni finanziarie. Le autorità di regolamentazione dovrebbero raccogliere dati più dettagliati sull'uso dell'IA, per comprendere meglio i suoi effetti sulla stabilità finanziaria. Gli enti di vigilanza dovrebbero inoltre farsi carico di sviluppare linee guida specifiche per garantire un uso etico e sicuro dell'IA, con particolare attenzione ai modelli di apprendimento automatico opachi. La natura globale del sistema finanziario richiede una cooperazione tra le diverse giurisdizioni per armonizzare le regolamentazioni sull'IA e ridurre i rischi sistemici. Le istituzioni finanziarie dovrebbero inoltre diversificare, per quanto possibile, i fornitori di servizi IA e adottare strategie di sicurezza informatica più robuste per proteggere i dati sensibili e garantire la continuità operativa.

L'FSB sottolinea la necessità di un approccio bilanciato tra innovazione e regolamentazione, per favorire uno sviluppo dell'IA compatibile con gli obiettivi di stabilità finanziaria. Attraverso una governance adeguata, una supervisione efficace e una collaborazione internazionale, l'IA può essere utilizzata in modo responsabile per favorire uno sviluppo sostenibile del settore finanziario.

FEDERICO PISTELLI

https://www.fsb.org/uploads/P14112024.pdf

2024/4(37)AAM

37. Lo studio del Consiglio UE del settembre 2024 sulle tecnologie Brain-Computer Interface (BCI)

ISSN 2239-8570

Nel mese di settembre 2024, il Consiglio dell'Unione europea (il **Consiglio**) ha pubblicato un *research paper* dal titolo "*From vision to reality. Promises and risks of Brain-Computer Interfaces*" che ricostruisce l'attuale sviluppo dei dispositivi di *Brain-Computer Interface* (**BCI**), ovvero le neurotecnologie in grado di creare un percorso di comunicazione diretta tra il cervello umano e un dispositivo esterno. Noti fin dalla fine degli anni Settanta del secolo scorso – quando con il primo esperimento si riuscì a mantenere il controllo di un cursore su di uno schermo grazie all'attività cerebrale del partecipante – i dispositivi che impiegano tecnologie di questo tipo attraggono sempre più ingenti investimenti da parte di ricercatori e grandi aziende sia in ambito clinico, per consentire il recupero di funzioni fisiche e mentali che molte persone possono aver perso; sia per un loro impiego sempre più massivo al di fuori dell'ambito clinico, che solleva diverse e cruciali questioni da un punto di vista sociale, etico e giuridico. Partendo dal profilo tecnico, il documento elaborato dal Consiglio mette ben in evidenza come, se l'elemento che accomuna tutti i dispositivi di BCI (oramai numerosi e diversificati) è la capacità di rilevare e interpretare i segnali elettrici del cervello e convertirli in output eseguibili dal computer, una possibile categorizzazione può essere fatta tra BCI **invasivi**, BCI **non invasivi**, BCI **parzialmente invasivi** (o semi invasivi). Nel primo caso, si tratta di impianti cerebrali altamente avanzati che comportano procedure chirurgiche per inserire elettrodi direttamente nel cervello o sulla sua superficie. Sebbene questi sistemi presentino rischi intrinseci e potenziali complicazioni per l'utente, offrono un'acquisizione del segnale ad alta risoluzione, fondamentale per le applicazioni che richiedono un controllo preciso. Le soluzioni non invasive, invece, utilizzano sensori esterni, eliminando così i rischi legati alla chirurgia. Questi sistemi registrano l'attività cerebrale utilizzando tecniche come l'elettroencefalogramma (**EEG**). In questo caso, tuttavia, i segnali sono più deboli e maggiormente suscettibili al rumore e alle interferenze. Infine, con i dispostivi di BCI semi invasivi è richiesto un intervento chirurgico minimo oppure si utilizzano tecnologie mediche preesistenti, come stent e cateteri, per inserire gli elettrodi in prossimità del cervello senza dover ricorrere a un intervento chirurgico aperto.

Rispetto al segnale cerebrale registrato, invece, e al modo in cui i dati vengono trasmessi tra il cervello e il computer, si può distinguere tra BCI **unidirezionali** (il segnale è registrato dal cervello e trasmesso al computer e viceversa ma senza stimolazione mirata) e BCI **bidirezionali** (consente uno scambio interattivo e in tempo reale tra l'utente e il computer, registrando il segnale cerebrale e fornendo una stimolazione mirata in maniera simultanea).

Gli **ambiti di applicazione** attuali e potenziali di cui si discute sono ormai molti ed eterogenei. Non più solo l'ambito medico per la cura di patologie neurodegenerative - come l'Alzheimer, Parkinson ma anche depressione ed epilessia - dove l'impiego di BCI contribuisce ad una società più inclusiva per le persone con disabilità, ma anche il settore del benessere (*wellbeing*), favorendo il rilassamento e la concentrazione, e quello dei prodotti di consumo con applicazioni che possono modificare il nostro

ISSN 2239-8570

approccio al mondo del lavoro, dell'arte, dell'istruzione e, in senso più ampio, delle relazioni sociali. Negli ambienti professionali, infatti, uno degli impatti immediati che le BCI potrebbe avere è la capacità di monitorare da vicino l'attività cerebrale, migliorando così le prestazioni e la produttività ma anche la sicurezza dei compiti ad alto rischio, avvertendo i lavoratori quando sono distratti o in pericolo. Inoltre, le BCI possono dare origine a nuovi strumenti e piattaforme di collaborazione che rendono il lavoro a distanza più naturale e coinvolgente.

Allo stesso modo, le BCI potrebbero cambiare in modo significativo il modo di fare arte, consentendo agli individui di generare opere, dipinti o musica semplicemente utilizzando la propria attività cerebrale. Già sono noti diversi casi di persone con disabilità che, pur non avendo l'utilizzo degli arti superiori, hanno creato opere d'arte con dispositivi di BCI, poi esposte e vendute in importanti mostre. Nel campo dell'istruzione, le BCI potrebbero trasformare i processi di apprendimento. Gli strumenti attualmente disponibili, come gli occhiali intelligenti, forniscono un *feedback* istantaneo per aiutare gli utenti a concentrarsi. In prospettiva, le BCI potrebbero facilitare le interfacce di apprendimento diretto, consentendo la rapida assimilazione di concetti complessi e forse anche il trasferimento istantaneo delle conoscenze, come nel caso dell'apprendimento di una nuova lingua. Questa tecnologia potrebbe adattare le esperienze educative agli stili di apprendimento individuali, rendendo potenzialmente l'istruzione più efficiente e accessibile. Nel 2021, poi, il noto caso della scimmia che ha giocato ad un videogioco utilizzando un dispositivo di BCI invasivo (impiantato) ha reso evidente come anche l'industria del gioco possa essere modificata da queste nuove tecnologie rendendo le esperienze di gioco più interattive e coinvolgenti, consentendo ai giocatori di controllare un gioco usando i loro pensieri. Inoltre, nel settore del marketing, le BCI hanno il potenziale per ridefinire la ricerca sui consumatori, fornendo approfondimenti in tempo reale sulle risposte emotive e cognitive che potrebbero portare a una comprensione più profonda del comportamento dei consumatori. Da ultimo, uno dei settori che promette rivoluzioni senza precedenti, è quello della sicurezza e difesa nazionale. In tale ambito, le BCI hanno il potenziale per aumentare le funzioni cognitive per migliorare le prestazioni dei soldati, accelerare il processo decisionale, gestire gli stati fisici ed emotivi, riducendo potenzialmente il dolore o regolando emozioni come la paura durante il combattimento. Anche in questo caso, gli investimenti sono notevoli, se si considera che la *Defence Advanced Research Projects Agency* (**DARPA**) degli Stati Uniti sta lavorando attivamente allo sviluppo di BCI non invasive o minimamente invasive per controllare sistemi di difesa informatica o sciami di veicoli aerei senza pilota (droni). Sul piano specifico della sicurezza, inoltre, le BCI potrebbero offrire una nuova dimensione ai sistemi di monitoraggio, dove gli operatori potrebbero utilizzare input neurali per controllare e interpretare i dati di sorveglianza con velocità ed efficienza senza precedenti, migliorando il rilevamento e la previsione delle minacce alla sicurezza.

ISSN 2239-8570

Se quelli appena indicati sono ambiti e applicazioni dei dispositivi di BCI più o meno note, il *Paper* del Consiglio UE completa il quadro di analisi con gli scenari futuri e le potenzialità ancora inesplorate delle BCI: la prospettiva di decodificare i pensieri direttamente dai modelli neurali potrebbe aprire la strada a una forma di telepatia, in cui gli individui comunicano attraverso il solo pensiero, senza bisogno di linguaggio parlato o scritto. Le ricerche in corso includono sforzi per ricostruire i segni dai segnali cerebrali, utilizzando l'intelligenza artificiale e i dati EEG per generare immagini dal subconscio. Ulteriori progressi potrebbero aprire possibilità che oggi sembrano del tutto fantasiose, come la possibilità di registrare digitalmente tutte le esperienze di vita di una persona. Un concetto ipotizzato da Stephen Hawking, il caricamento della mente umana in un computer, potrebbe essere un'altra possibilità. Infine, lo studio fa notare come sebbene l'idea che gli esseri umani debbano fondersi con le macchine e diventare cyborg per rimanere rilevanti in un'era dominata dall'intelligenza artificiale può sembrare estrema, tuttavia speculazioni di questo tipo evidenziano l'importanza di considerare la traiettoria e le implicazioni a lungo termine dello sviluppo delle BCI. Ciò soprattutto dal punto di vista dei possibili rischi che tali tecnologie possono determinare per le persone.

Se i benefici potenziali, come visto, sono molti e spesso consentono di realizzare un principio di inclusione in una società che spesso con le normali risorse non riesce ad essere aperta ed accessibile per tutti, dall'altro è essenziale valutare criticamente le sfide che queste tecnologie pongono, soprattutto in termini di impatto sui diritti fondamentali delle persone, primo fra tutti la salute. Per quanto riguarda le BCI invasive, naturalmente i rischi sono quelli associati all'uso di dispositivi impiantati, tra cui infezioni ed emorragie che potrebbero danneggiare il tessuto cerebrale, oltre che la risposta immunitaria dell'organismo che può anche portare al rigetto dell'impianto. Più in generale, occorre poi considerare i possibili malfunzionamenti o guasti del dispositivo e il necessario aggiornamento dei sistemi impiantati e la gestione dell'hardware abbandonato all'interno del corpo. Sia per le BCI invasive che per quelle non invasive, inoltre, l'uso prolungato può causare **affaticamento cognitivo** e rischi per il benessere fisico e psicologico dell'utente nel lungo periodo.

Ciò ha delle immediate ricadute anche sul piano della sicurezza: **la linea che separa il potenziamento umano dall'intervento terapeutico** è spesso ambigua, mentre la definizione di ciò che è considerato "normale" in termini di capacità umane è oggetto di continuo dibattito. Non sottovalutabile, inoltre, sul piano sociale, il possibile nuovo **divario digitale** che potrebbe verificarsi, dati i costi elevati di una tecnologia che potrebbe non essere alla portata di tutti, svilendo dunque le potenzialità innanzi illustrate sul piano dell'accessibilità e inclusione sociale che tali dispositivi potrebbero invece garantire.

Le regioni e i Paesi con strutture sanitarie limitate, livelli inferiori di infrastrutture tecnologiche e meno professionisti medici specializzati potrebbero avere difficoltà a implementare e mantenere le BCI.

ISSN 2239-8570

Oltre alle barriere finanziarie e infrastrutturali, ci sono anche importanti considerazioni etiche e politiche su chi può accedere a queste tecnologie e per quali scopi. Il Consiglio nel suo lavoro mette allora ben in evidenza come l'allocazione delle risorse per lo sviluppo e la distribuzione delle BCI deve essere guidata da principi di uguaglianza sociale, garantendo che le popolazioni vulnerabili, come le persone con disabilità o malattie croniche, abbiano la priorità. Tuttavia, senza politiche deliberate e inclusive, queste popolazioni potrebbero essere trascurate a favore di applicazioni più redditizie della tecnologia.

Accedere al cervello umano, comporta poi profonde implicazioni anche per la **privacy** personale e la **sicurezza** dei numerosi dati raccolti dalle BCI. I dati personali collegati all'attività cerebrale – **dati neurali** – pongono diversi quesiti in merito alla loro esatta **qualificazione giuridica** e alla **liceità del loro trattamento**, onde evitare il rischio di elaborare una serie di informazioni altamente sensibili, che vanno dai pensieri e dalle emozioni alle preferenze e alle intenzioni, senza tuttavia riuscire a garantire alla persona il suo diritto fondamentale di mantenere il controllo su tali informazioni, di consentire l'accumulo e la monopolizzazione degli stessi da parte delle aziende private, che potrebbero potenzialmente sfruttare queste informazioni a fini politici o commerciali, come la pubblicità mirata. Inoltre, poiché le BCI si interfacciano sempre più spesso con dispositivi e reti esterne, le questioni relative alla **proprietà** dei dati si amplificano ulteriormente, mostrando l'importanza di chiarire chi è il proprietario di questi dati, oppure come viene ottenuto e gestito il consenso, le finalità per cui i dati possono essere raccolti e utilizzati, le condizioni in cui possono essere condivisi e le misure di sicurezza in atto per prevenire l'uso non autorizzato e proteggere i diritti alla privacy.

Infine, alcuni tipi di BCI possano essere utilizzati per **manipolare** o influenzare le decisioni.

Se utilizzate su larga scala, le BCI potrebbero avere notevoli implicazioni per la democrazia, mettendo in discussione l'integrità della formazione delle opinioni personali e del processo decisionale indipendente. Gli attori politici e i gruppi di interesse potrebbero sfruttare questa tecnologia per alterare le percezioni delle persone, influenzando così l'opinione pubblica e i risultati elettorali. Inoltre, le BCI potrebbero consentire un livello di sorveglianza senza precedenti, permettendo ai regimi totalitari di accedere e monitorare gli stati mentali di individui e gruppi. Ciò potrebbe facilitare l'identificazione del dissenso e semplificare gli sforzi per sopprimerlo e consolidare il potere.

Questi possibili sviluppi sollevano anche la questione della **responsabilità**. Ad esempio, alcuni pazienti sottoposti a stimolazione cerebrale profonda hanno sperimentato cambiamenti comportamentali, tra cui un aumento dell'imprudenza e dell'impulsività. L'uso delle BCI potrebbe **alterare lo stato mentale** di un utente al punto da non essere più la stessa persona che era prima dell'uso della tecnologia. Di conseguenza, sarebbe difficile stabilire chi debba essere ritenuto responsabile di determinate azioni.

ISSN 2239-8570

Infine, il report del Consiglio si focalizza sulle possibili **scelte di governance** delle neurotecnologie, per anticipare il mercato e le grandi aziende tecnologiche (**Apple, Meta, Microsoft, Neuralink,** che stanno già investendo nelle BCI per ottenere un vantaggio in questo settore emergente, ognuna con la propria strategia e le proprie aree di interesse) consentendo loro uno **sviluppo non regolamentato** con possibile amplificarsi dei riferiti rischi di tali tecnologie.

In tale scenario, gioca un ruolo fondamentale anche la posizione precisa di ciascun Paese nella corsa alle BCI: attualmente gli St**ati Uniti** sono in testa alla competizione, in termini di investimenti sia privati che pubblici, mentre la **Cina** sta aumentando il ritmo e creando le condizioni per uno sviluppo industriale su larga scala. L'**Unione europea** ha adottato un approccio collaborativo ed etico allo sviluppo delle BCI, con una forte enfasi sulle applicazioni mediche e sul miglioramento della qualità della vita delle persone con disabilità. L'UE ha finanziato progetti attraverso programmi come Horizon 2020 e il suo successore, Horizon Europe, che mirano a incoraggiare la ricerca e l'innovazione in un'ampia gamma di settori, comprese le BCI.

Nell'ecosistema delle BCI ci sono poi anche altri attori importanti che stanno utilizzando metodi innovativi. Ad esempio, la startup israeliana **InnerEye** utilizza la tecnologia EEG per accedere direttamente all'elaborazione visiva del cervello, facilitando così un più rapido riconoscimento delle immagini e migliorando potenzialmente l'efficienza sul posto di lavoro. In Australia, **Synchron** utilizza tecnologie mediche preesistenti, come stent e cateteri, per accedere al cervello con un approccio meno invasivo.

Il report del Consiglio UE pone allora l'accento sulla necessità di promuovere un dialogo continuo e ben informato sulle neurotecnologie, elemento essenziale per accrescere la consapevolezza e migliorare la comprensione pubblica dei potenziali benefici e delle sfide presentate dalle BCI. Diverse iniziative riflettono questa crescente attenzione. La Raccomandazione dell'OCSE del 2019 sull'innovazione responsabile nelle neurotecnologie stabilisce il primo standard internazionale, guidando i governi e gli innovatori ad anticipare e affrontare le sfide etiche, legali e sociali promuovendo l'innovazione. L'UNESCO sta lavorando a un quadro globale per l'etica delle neurotecnologie e mira a presentarlo per l'adozione entro la fine del 2025 avendo a tal fine nominato un panel di esperti. La Francia ha introdotto sin dal 2022 una carta per lo sviluppo responsabile delle neurotecnologie, con l'intenzione di espandere questa iniziativa in tutta l'UE.

Nell'ambito dell'Unione europea, la legislazione esistente affronta già diversi aspetti pertinenti allo sviluppo e all'applicazione delle BCI, tra cui le **norme sulla sicurezza dei dispositivi medici**, sulla **protezione dei dati**, sull'**intelligenza artificiale** e sulla **sicurezza informatica**. Gli sforzi futuri potrebbero concentrarsi sull'identificazione e la chiusura di potenziali lacune che potrebbero portare a un uso non etico o a una protezione insufficiente dei diritti e delle libertà degli individui. A livello globale, diversi attori si stanno muovendo in questo senso. Nell'ottobre 2021, il **Cile** è stato il primo

ISSN 2239-8570

Paese a modificare la propria Costituzione per salvaguardare i dati cerebrali e la privacy dei cittadini (sulla Ley n. 21.383 di modifica costituzionale v. in questa Rubrica la notizia n. 12 nel numero 3/2023 [2023/3(12)AAM] e *Atlante* p. 395). Nell'aprile 2024, il **Colorado** è stato il primo Stato americano ad approvare una legge che protegge i dati ricavati dalle onde cerebrali (sul Colorado House Bill 24-1058, v. in questa Rubrica la notizia n. 38 nel numero 2/2024 [2024/2(38)AAM]).

Con il progredire di queste iniziative, sarà importante mantenere un delicato equilibrio che non impedisca l'innovazione e gli investimenti, soprattutto alla luce del notevole successo che le BCI hanno dimostrato in campo medico. Per guidare lo sviluppo delle BCI è quindi necessario stabilire solidi standard etici, favorire un ambiente normativo che promuova sia la sicurezza che l'innovazione e assicurare un'efficace collaborazione tra le parti interessate pubbliche e private. Un approccio di questo tipo aiuterebbe a massimizzare i benefici delle BCI minimizzando i rischi, contribuendo in ultima analisi al benessere e al progresso della società.

ANNA ANITA MOLLO

https://www.consilium.europa.eu/media/fh4fw3fn/art_braincomputerinterfaces_2024_web.pdf?utm_source=linkedin.com&utm_medium=social&utm_campaign=20241002-art-research-paper&utm_content=visual

2024/4(38)ES

38. I due studi della Banca d'Italia dell'ottobre 2024 su protezione del consumatore, *neurofinance* e *neuroeconomics*

Nel mese di ottobre 2024 la Banca d'Italia ha pubblicato gli *occasional papers* n. 888 e 890 intitolati, rispettivamente, "*The case for mindful customer protection: a review and some thoughts on neuroeconomics and neurofinance*" e "*The role of behavioural economics and neurofinance in financial consumer protection policy*".

Il *paper* n. 888/2024 evidenza che la neuroeconomia e la neurofinanza giocano un ruolo fondamentale nella definizione della migliore tutela dei consumatori da parte delle Autorità di regolazione e di vigilanza di settore. La neuroeconomia è una disciplina relativamente recente affermatasi negli Stati Uniti d'America negli anni '90 del secolo scorso. Essa analogamente alla neurofinanza combina neuroscienze, economia e psicologia utilizzando strumenti di diagnostica medica per studiare le reazioni celebrali degli individui mentre compiono determinate attività e prendono delle decisioni. In tal modo, è possibile approfondire la comprensione dei processi decisionali degli individui anche in materia finanziaria.

Il *paper* analizza l'evoluzione e lo stato dell'arte degli studi in ambito neuroeconomico, descrive alcuni dei principali strumenti di indagine e passa in rassegna la letteratura scientifica rilevante evidenziando come non manchino autori critici verso la neuroeconomia. In ogni caso, "*both critics*

ISSN 2239-8570

and advocates of neuroeconomics acknowledge that neuroscience can provide a relevant contribution to traditional analyses". L'obiettivo che si pone il quaderno di ricerca è contribuire allo studio delle neuroscienze valutando il loro potenziale uso e i benefici in ambito regolatorio, economico e finanziario. Per tale ragione, particolare attenzione è dedicata all'analisi delle reazioni dei consumatori mentre prendono le loro decisioni economiche. Il *paper* afferma che tanto gli esperti di neuromarketing, quanto le Authorities possono beneficiare dei risultati degli studi in materia di neuroscienze. Per le Authorities, infatti, una migliore comprensione dei processi decisionali può aiutare a implementare la tutela dei consumatori migliorando, ad esempio, l'informativa precontrattuale e l'educazione finanziaria. In definitiva, quindi, la ricerca si propone di contribuire allo sviluppo di *policy* e norme in materia di protezione dei consumatori.

Il *paper* 890/2024 evidenzia che i *policymakers* e la letteratura scientifica stanno sviluppando una crescente consapevolezza del fatto che la regolazione del mercato, la sua supervisione e l'informativa (pre)contrattuale sono spesso poco efficienti a causa di diversi fattori tra cui si annoverano la complessità degli strumenti finanziari, il basso livello di educazione finanziaria dei consumatori, nonché soprattutto i *biases* cognitivi e comportamentali dei consumatori medesimi in ambito finanziario. Di conseguenza, molte Authorities mostrano crescente interesse verso la neuroeconomia e la neurofinanza poiché tali scienze, come detto sopra, possono offrire gli strumenti per aiutare a definire le migliori politiche a tutela dei consumatori in ambito finanziario. Lo studio ricorda che l'economia comportamentale, al cui interno si annoverano la neuroeconomia e la neurofinanza, coniuga psicologia ed economia al fine di studiare i processi decisionali degli individui in maniera innovativa. Le scelte dei consumatori, infatti, sono pesantemente influenzate da fattori psicologici, emotivi, culturali e sociali che sono oggetto di analisi da parte dell'economia comportamentale, ma non dai classici studi economici. In particolare, il *paper* in commento evidenza che le scelte decisionali sono influenzate da *bias* cognitivi tra cui annovera fenomeni come l'*anchoring*, ossia l'assunzione di decisioni in base ad un fattore ritenuto imprescindibile anche se così non è, e l'*overconfidenc*e. Lo studio, quindi, espone la c.d. "*nudge theory*" secondo cui le decisioni assunte in base ad alcuni elementi, i *bias* appunto, appaiono come preferibili rispetto alle alternative anche se non lo sono nella realtà e si interroga su come l'economia comportamentale possa contribuire a migliorare la tutela finanziaria dei consumatori. Essa, infatti, consente un'approfondita comprensione dei processi decisionali e, quindi, la migliore definizione delle politiche e norme a tutela dei consumatori. "*Behavioural economics and neurofinance have the potential to significantly strengthen the toolkit for financial consumer protection*".

EMANUELE STABILE

https://www.bancaditalia.it/pubblicazioni/qef/2024-0888/QEF_888_24.pdf
https://www.bancaditalia.it/pubblicazioni/qef/2024-0890/QEF_890_24.pdf?language_id=1

ISSN 2239-8570

2024/4(39)BP

39. Il D.Lgs. 144/2024 di adeguamento dell'ordinamento italiano al DGA: la disciplina sanzionatoria e la nomina di AgID come autorità competente per i servizi di intermediazione e altruismo dei dati, come organismo di assistenza degli enti pubblici che concedono o rifiutano il riutilizzo di dati, e come punto unico di contatto

È entrato in vigore il 25 ottobre 2024 il Decreto legislativo 7 ottobre 2024, n. 144 (il **Decreto**) recante l'adeguamento della normativa nazionale al regolamento (UE) 2022/868, il Data Governance Act (su cui v. in questa Rubrica la notizia n. 1 del n. 2/2022 [2022/2(1)RA] e in *Atlante*, p. 181) (**DGA** o il **Regolamento**).

Costituito da cinque articoli, l'intervento normativo, come spiega l'art. 1 del Decreto («oggetto e ambito di applicazione») al comma primo, risponde all'esigenza, imposta dal Regolamento eurounitario, di designazione delle autorità competenti per i servizi di intermediazione dei dati e per la registrazione di organizzazioni per l'altruismo dei dati e dell'organismo competente per assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo dei dati da essi detenuti, nonché di attuazione della disciplina sanzionatoria. Specifica, in ogni caso, lo stesso art. 1, co. 2, che «restano ferme le disposizioni in materia di protezione dei dati personali e di controllo sul trattamento dei medesimi dati nonché le competenze del Garante per la protezione dei dati personali, dell'Agenzia per la cybersicurezza nazionale e dell'Autorità garante della concorrenza e del mercato».

Ai sensi, dunque, dell'art. 2, co. 1 del Decreto viene designata l'Agenzia per l'Italia digitale (**AgID**) quale autorità competente allo svolgimento dei compiti relativi alla **procedura di notifica per i servizi di intermediazione dei dati** (ai sensi dell'art. 13 DGA), nonché quale autorità competente alla **registrazione di organizzazioni per l'altruismo dei dati** (ai sensi dell'art. 23 DGA). Come vuole, poi, l'art. 26 DGA, l'art. 2, co. 2 del Decreto specifica che l'AgID «svolge la propria attività in maniera imparziale, trasparente, coerente, affidabile e tempestiva, salvaguardando, nell'esercizio della propria attività, la concorrenza leale e la non discriminazione», precisando altresì che essa «opera in stretta e leale cooperazione con l'Agenzia per la cybersicurezza nazionale, l'Autorità garante della concorrenza e del mercato e il Garante per la protezione dei dati personali e, a tal fine, può stipulare con gli stessi specifici **accordi di collaborazione** non onerosi», i quali accordi prevedono in particolare «forme specifiche di consultazione del Garante per la protezione dei dati personali, ogniqualvolta il procedimento amministrativo realizzato da AgID abbia implicazioni in termini di protezione dei dati». In attuazione dell'art. 16 DGA, il successivo art. 2, co. 3 del Decreto prevede quindi che «l'AgID, sentite l'Agenzia per la cybersicurezza nazionale, l'Autorità garante della concorrenza e del mercato

ISSN 2239-8570

e il Garante per la protezione dei dati personali per gli aspetti di rispettiva competenza, stabilisce con proprio provvedimento […] le disposizioni tecniche e organizzative per facilitare l'altruismo dei dati nonché le informazioni necessarie che devono essere fornite agli interessati in merito al riutilizzo dei loro dati nell'interesse generale». Attuativi invece rispettivamente degli artt. 14 e 24 DGA, i commi quarto e quinto dell'art. 2 del Decreto stabiliscono che l'AgID provveda anche al monitoraggio e al controllo della conformità dei fornitori dei servizi di intermediazione dei dati e delle organizzazioni riconosciute per l'altruismo dei dati ai requisiti per essi sanciti (rispettivamente) dal capo III e IV del DGA.

Ai sensi del successivo art. 3 del Decreto, sempre l'AgID è designata (in attuazione dell'art. 7 DGA) quale organismo competente **per assistere gli enti pubblici che concedono o rifiutano l'accesso al riutilizzo** delle categorie di dati di cui all'art. 3, par. 1 DGA **e per concedere l'accesso per il riutilizzo** delle categorie di dati ai sensi dell'art. 7, par. 2, del medesimo Regolamento e (in attuazione dell'art. 8 DGA) quale «sportello unico e provvede all'implementazione delle relative funzioni **estendendo il punto d'accesso unico garantito dal catalogo nazionale dei dati aperti** di cui all'articolo 9, comma 2, del decreto legislativo 24 gennaio 2006, n. 36» (sul D.Lgs. 36/2006 come modificato dal D.Lgs. 8 novembre 2021, n. 200, in attuazione della direttiva 'Open Data' (UE) 2019/1024, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, v. in questa Rubrica la notizia n. 2 del n. 1/2022 [2022/1(2)RA] e in *Atlante*, p. 152).

L'art. 4 del Decreto detta la disciplina sanzionatoria in attuazione del rinvio operato dall'art. 34 DGA. Più in dettaglio, replicato al comma secondo quanto disposto dall'art. 34(2) DGA (per cui «le sanzioni per le violazioni di cui al comma 1 devono essere effettive, proporzionate e dissuasive e devono tenere conto dei seguenti criteri: a) la natura, la gravità, l'entità e la durata della violazione; b) qualsiasi azione intrapresa dal fornitore di servizi di intermediazione dei dati o da un'organizzazione per l'altruismo dei dati riconosciuta al fine di attenuare il danno derivante dalla violazione o porvi rimedio; c) qualsiasi precedente violazione da parte del fornitore di servizi di intermediazione dei dati o dell'organizzazione per l'altruismo dei dati riconosciuta; d) i vantaggi finanziari ottenuti o le perdite evitate dal fornitore di servizi di intermediazione dei dati o da un'organizzazione per l'altruismo dei dati riconosciuta in ragione della violazione, nella misura in cui tali profitti o perdite possano essere determinati in modo attendibile; e) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso»), il comma primo prescrive che ferma restando l'applicazione della disciplina in materia di protezione dei dati personali e salvo che il fatto costituisca reato, «in caso di violazione degli obblighi in materia di trasferimento di dati non personali a Paesi terzi a norma dell'articolo 5, paragrafo 14, e dell'articolo 31 del regolamento, dell'obbligo di notifica per i fornitori di servizi di intermediazione dei dati a norma dell'articolo 11 del regolamento, delle condizioni per la fornitura di servizi di intermediazione dei dati a norma dell'articolo 12 del regolamento, delle condizioni per la registrazione come organizzazione per l'altruismo dei dati riconosciuta a norma degli articoli 18, 20, 21 e 22 del regolamento da

ISSN 2239-8570

parte dei fornitori di servizi di intermediazione dei dati e delle organizzazioni per l'altruismo dei dati, l'AgID adotta, all'esito della procedura di cui all'articolo 18-bis del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, sanzioni amministrative pecuniarie da un minimo di euro 10.000 fino a un massimo di euro 100.000, ovvero, per le imprese, fino al 6 per cento del fatturato mondiale totale annuo dell'esercizio precedente».

L'art. 5 del Decreto, infine, pone una clausola di invarianza finanziaria.

BENIAMINO PARENZO

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024;144

2024/4(40)ES

40. Il D. Lgs. 134/2024 di attuazione della direttiva (UE) 2022/2257 relativa alla resilienza dei soggetti critici (direttiva CER)

Il 4 settembre 2024 è stato pubblicato il D. Lgs. 134/2024 (da ora anche il **Decreto**) che adegua l'ordinamento italiano alla dir. 2022/2257/UE del Parlamento europeo e del Consiglio relativo alla resilienza dei soggetti critici (direttiva **Critial Entities Resilience** o **CER**). Ai fini della presente analisi ci si concentrerà sugli aspetti riguardanti l'infrastruttura digitale e l'Agenzia per la cybersicurezza nazionale.

L'art. 1 del Decreto, innanzitutto, stabilisce che esso si occupa di garantire che i "*servizi essenziali per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente*" siano forniti senza interruzioni. Il Decreto disciplina altresì i criteri per l'individuazione dei soggetti critici e una serie di loro obblighi volti a favorire il raggiungimento di un buon livello di resilienza. L'art. 1, comma 6 specifica che il provvedimento in esame non si applica "*agli organi e alle articolazioni della pubblica amministrazione, nonché agli enti di cui all'articolo 2, comma 1, lettera l), che operano nei settori della pubblica sicurezza, della difesa nazionale o dell'attività di contrasto, compresi l'indagine, l'accertamento e il perseguimento di reati, nonché agli organismi di informazione per la sicurezza di cui alla legge 3 agosto 2007, n. 124, all'Agenzia per la cybersicurezza nazionale ... al Parlamento, alla Banca d'Italia, all'Unità di informazione finanziaria per l'Italia ... e agli organi giudiziari*". L'art. 2 contiene una serie di definizioni tra cui quella di i) servizio essenziale, "*un servizio fondamentale per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della sicurezza pubbliche o dell'ambiente*"; ii) soggetto critico, "*un soggetto pubblico o privato individuato, ai sensi dell'articolo 8, nell'ambito delle categorie di soggetti che operano nei settori e sottosettori di cui all'allegato A ...*"; e iii) di infrastruttura critica la quale indica "*un elemento, un impianto, un'attrezzatura, una rete o un sistema o una parte di essi*

ISSN 2239-8570

necessari per la fornitura di un servizio essenziale …". Il Decreto riserva al Presidente del Consiglio dei ministri l'adozione della strategia nazionale di resilienza, che deve recare i contenuti di cui all'art. 6, e la direzione e la responsabilità delle politiche in materia di resilienza (art. 2). In seno alla Presidenza del Consiglio è costituito il Comitato interministeriale per la resilienza ("CIR") che si occupa di proporre al Presidente del Consiglio "*gli indirizzi generali per le politiche di resilienza*", sorveglia sull'attuazione della strategia nazionale per la resilienza e promuove l'adozione di misure volte al rafforzamento della medesima (art. 4). All'interno della Presidenza del Consiglio è altresì costituito il punto di contatto (c.d. "PCU") che assicura il coordinamento tra le autorità settoriali competenti, con la Commissione europea e con i PCU degli altri paesi membri (art. 5, commi 5 ss.).

Si noti che sempre l'art. 5 del Decreto individua tra le autorità settoriali competenti (c.d. "ASC") in materia di resilienza l'Agenzia per la cybersicurezza nazionale (**ACN**), per il settore delle infrastrutture digitali previsto dal n. 8 dell'allegato A del Decreto, in collaborazione con il Ministero delle imprese e del made in Italy. Ad essi spettano la valutazione del rischio (art. 7) e l'individuazione dei soggetti critici (art. 8) che sono poi comunicati al PCU e da quest'ultimo all'ACN.

L'art. 9 definisce i criteri per stabilire se gli effetti negativi di un evento riguardante un servizio essenziale, inclusa l'infrastruttura digitale, sono rilevanti. Si tratta, tra l'altro, del numero di utenti impattati dall'evento, dal grado di interconnessione tra gli altri settori di cui all'allegato A del Decreto e il servizio essenziale, l'area geografica interessata dall'incidente, ecc. Per quanto qui interessa, infine, l'art. 10 prevede che le norme ivi elencate, ossia l'art. 12 e i capi III, IV e VI del Decreto, non si applichino ai soggetti operanti nel settore delle infrastrutture digitale. Il Decreto è entrato in vigore il 18 ottobre 2024.

EMANUELE STABILE

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024;134

2024/4(41)MC

41. Le nuove disposizioni sulla tutela del giocatore contro il gioco patologico e sull'impiego di sistemi di intelligenza artificiale in materia di riordino del settore dei giochi (d.lgs. 41/2024)

Il decreto legislativo 25 marzo 2024, n. 41 (il **Decreto**), ha introdotto un ampio riordino del settore dei giochi pubblici, con particolare attenzione ai giochi a distanza. Il Decreto si inserisce nel quadro di una riforma generale, finalizzata a garantire maggiore trasparenza, legalità e tutela dei consumatori, in linea con i princìpi sanciti dalla legge delega n. 111/2023. Tali misure mirano a contrastare l'emergere di nuove criticità, legate in

ISSN 2239-8570

particolar modo all'evoluzione tecnologica e al dilagare del gioco patologico nelle sue diverse forme, ma rispondono altresì alla frammentarietà delle norme di settore, a lungo evidenziate dalla dottrina e dagli operatori commerciali.

Anzitutto, nella prima parte del Decreto (Titoli I e II) vengono dettate le regole essenziali per la disciplina pubblicistica del gioco pubblico, con particolare attenzione al meccanismo delle concessioni.

Successivamente, nel Titolo III, si approfondiscono le regole e le misure poste a "tutela e protezione del giocatore".

Il titolo IV disciplina sul piano tecnico alcuni profili essenziali del gioco a distanza (offerta, raccolta, vincite; giochi numerici e lotterie a estrazione istantanea) mentre il titolo V stabilisce alcune norme per il contrasto al gioco illegale.

Da ultimo, il Titolo VI prevede disposizioni transitorie e finali, disposizioni finanziarie e rimanda a successivo d.lgs. per le abrogazioni di norme incompatibili con il d.lgs. n. 41/2024.

L'obiettivo primario di tale 'testo unico' è quello di offrire una revisione organica e unitaria delle norme riguardanti i giochi pubblici, o autorizzati. Nei fatti, invero, esso si configura più propriamente come un quadro regolatorio, non del tutto esaustivo, relativamente ai giochi pubblici ammessi in Italia.

Sul piano generale, all'art. 2 vengono, fra l'altro, offerte delle definizioni dei vari tipi di giochi oggetto del decreto, all'art. 3 vengono individuati i "princìpi ordinamentali" del gioco pubblico in Italia, fra cui la tutela dei minori d'età, la legalità, la trasparenza e la sicurezza del gioco, la promozione del gioco responsabile, da coordinare con i princìpi rilevanti di derivazione europea di cui al successivo art. 4, valevoli "quale criterio interpretativo preferenziale delle norme applicabili al gioco".

Invero, sul piano applicativo è il Titolo II in tema di rapporto concessorio per i giochi a distanza a venire maggiormente in rilievo, ove vengono riorganizzate le norme regolanti il sistema concessorio di settore. Vengono individuati i giochi sottoposti alla relativa disciplina, fra cui quelli svolti "in modalità virtuale o digitale, anche attraverso il metaverso" (art. 6, comma 1), per i quali si prevedono alcune disposizioni generali, salvo poi l'adozione di appositi regolamenti dell'Agenzia delle Dogane e dei Monopoli e di specifiche regole da prevedere. Si hanno, poi, fra l'altro, specifiche regole sulle domande di partecipazione, sulla raccolta e sul contratto di conto di gioco, oltre che sulla gestione delle concessioni, della rete telematica e dei punti vendita delle ricariche.

In una diversa prospettiva, poi, deve considerarsi che il Decreto mira ad offrire una migliore tutela della salute del giocatore. Tale obiettivo traspare in diverse disposizioni del decreto: esso, quantomeno, emerge, direttamente e indirettamente, nei princìpi individuati all'art. 2, e sembra intravedersi all'art. 6, comma 8, nelle regole previste per il contratto di conto di gioco. Tuttavia, è agli artt. 14 e 15 componenti il Titolo III rubricato "Tutela e protezione del giocatore" che l'applicazione di tale principio è oggetto di specifica attenzione da parte del legislatore delegato.

ISSN 2239-8570

Così, all'art. 14 viene, anzitutto, (ri-)esplicitato che obiettivo della disciplina dei giochi autorizzati è "quello di perseguire piena e affidabile protezione della salute del giocatore attraverso misure idonee a prevenire ogni modalità di gioco che possa generare disturbi patologici del comportamento o forme di gioco d'azzardo patologico" (comma 1), sì che l'offerta e lo svolgimento dei giochi andranno supportati da "strumenti di tecnologia avanzata, con particolare riguardo anche agli strumenti dell'intelligenza artificiale" per perseguire il menzionato obiettivo (comma 2). Parallelamente, in una prospettiva di sistema, viene istituita (comma 3) una "Consulta permanente dei giochi pubblici ammessi in Italia" con lo scopo di monitorare l'andamento delle attività di gioco, incluse quelle illecite e non autorizzate, i loro effetti sulla salute dei giocatori, nonché di proporre al Governo misure e interventi idonei allo scopo di contrastare lo sviluppo di gioco d'azzardo patologico.

Poi, all'art. 15 vengono predisposte tre tipologie di misure di tutela del giocatore.

In esso, al fine di garantire un'offerta di giochi più rispettosa della salute, si prevede (al comma 1) che le "forme organizzative" e gli strumenti "tecnici, tecnologici e informatici" del concessionario siano finalizzati a tutelare il giocatore dai rischi del gioco attraverso vari accorgimenti, fra cui misure di limitazione e autolimitazione al gioco, avvisi automatici, obblighi informativi, strumenti di autoesclusione, canali di contatto a supporto del gioco responsabile, procedure di monitoraggio dei livelli di rischio dei singoli giochi e meccanismi di controllo della partecipazione di giocatori maggiormente vulnerabili.

Inoltre, viene previsto (al comma 2) l'obbligo per i concessionari di investire una somma pari allo 0,2 per cento dei suoi ricavi netti (ma comunque non superiore a euro 1.000.000 per anno), in campagne e iniziative di sensibilizzazione su temi annualmente stabiliti da una costituenda commissione governativa ad hoc (previo confronto con l'Osservatorio per il contrasto della diffusione del gioco d'azzardo e il fenomeno della dipendenza grave presso il Ministero della salute).

Da ultimo, si prevede (al comma 3) la possibilità per il concessionario di effettuare a proprie spese campagne di sensibilizzazione "anche a fini sociali e comunque coerenti con l'esigenza di promuovere la prevenzione e il contrasto del gioco patologico". Questi messaggi devono riportare il logo del concessionario, contribuendo così a promuovere una maggiore fiducia tra operatori e consumatori del settore.

Invero, il macro-obiettivo di tutela della persona del giocatore viene perseguito anche attraverso il rafforzamento delle attività di contrasto dell'offerta illegale o non conforme di gioco. Difatti, unitamente a misure volte a garantire la tracciabilità dei flussi finanziari, sì da prevenire infiltrazioni criminali e riciclaggio di denaro di provenienza illecita (art. 7) e al menzionato monitoraggio delle attività di gioco illecite e non autorizzate ad opera dell'istituenda Consulta permanente dei giochi pubblici (art. 14, comma 3), sono previste all'art. 22 specifiche regole per il "contrasto all'offerta di gioco a distanza in difetto di concessione".

ISSN 2239-8570

L'art. 22, infatti, prevede, al comma 1, l'adozione di un regolamento per prevedere specifiche modalità volte all'esclusione dell'offerta di gioco tramite reti telematiche o di telecomunicazione effettuata da soggetti non concessionari e, di concerto con la Banca d'Italia, per impedire la relativa attività di raccolta e di versamento di somme per tali operazioni di gioco da parte di non concessionari. In particolare, l'individuazione dei siti di offerta di gioco non legale può essere svolta dall'ADM, d'intesa con la Guardia di Finanza e con società di gestione del sistema informativo, anche attraverso "soluzioni di intelligenza artificiale" (art. 22, comma 2). Attraverso tale attività vengono dunque formate, da un lato, la lista dei siti web di offerta legale e, dall'altro, una lista dei siti di gioco illecito il cui accesso dovrà essere inibito dai fornitori e gestori dei servizi di rete (commi 3, 4 e 5).

In una prospettiva di sistema, dunque, il Decreto cerca di raggiungere un miglior equilibrio tra la necessità di proteggere i consumatori-giocatori e quella di garantire un settore ben regolamentato e trasparente.

Il Decreto, invero, non si sottrae a criticità.

Di là dal fatto che lo stile del drafting normativo appare quantomeno perfettibile, il principale limite riguarda il merito dei profili in esso regolamentati: come accennato, infatti, non si ha un vero e proprio testo unico, ma più che altro una normativa-quadro, finalizzata a regolare prevalentemente i profili pubblicistici essenziali.

Da ciò discendono alcuni limiti applicativi. Mancano, ad esempio, regole specifiche di dettaglio relative all'adempimento (e all'inadempimento) degli obblighi informativi di settore. I diversi giochi, poi, sono definiti in materia sommaria, così che, per ciò che concerne l'evoluzione dei modelli ludici, si ha soltanto una generica clausola di salvaguardia per nuovi giochi virtuali riguardanti il "metaverso" (il cui riferimento all'art. 6, comma 1, rimane peraltro problematico, data l'assenza di definizioni normative univoche e la genericamente controversa definizione dello stesso).

Non si fa, inoltre, riferimento al potenziale impiego di tecniche di *gamification* e *gamblification* in settori di gioco pubblico di fatto, che potrebbero incentivare comportamenti compulsivi e contraddire l'obiettivo della tutela del giocatore vulnerabile.

Si rimanda, infine, a futuri atti normativi per la disciplina della "Consulta permanente dei giochi pubblici", di cui all'art. 14, comma 3, e della "commissione governativa" di cui all'art. 15, comma 2. L'introduzione di nuovi organi consultivi, da regolamentare con atti successivi, potrebbe aggravare la già complessa architettura regolatoria del settore, rischiando peraltro di sovrapporsi all'Osservatorio per il contrasto del gioco patologico, costituito presso il Ministero della salute, e minando l'efficacia complessiva del sistema.

Ciononostante, al legislatore delegato deve riconoscersi il merito di aver previsto, fra l'altro, nuovi e organici requisiti per la partecipazione alle gare pubbliche e per la gestione delle relative concessioni (particolarmente con riguardo ai requisiti tecnici e patrimoniali specificati all'art. 6, commi 5 e 6), di aver rafforzato i meccanismi di controllo e tracciabilità dei flussi finanziari, favorendo la collaborazione tra enti pubblici e concessionari. Parimenti, degno di nota è lo sforzo per cercare di supportare il contrasto al

ISSN 2239-8570

gioco illegale e, più in generale, il sostegno allo sviluppo di misure tecniche di tutela del giocatore.

In questo senso, l'uso di sistemi di intelligenza artificiale, in particolare, per la promozione di offerta e modalità di gioco volte a garantire la protezione della salute del giocatore (art. 14, comma 2) e per il contrasto al gioco non legale (art. 22, comma 2) segna un passo avanti nell'applicazione di tecnologie avanzate per il controllo e il contrasto delle attività di gioco nocive e illecite. Questa innovazione apre scenari interessanti in termini di efficacia delle politiche di enforcement e potrebbe diventare un modello per altri settori regolamentati – per quanto giudizi di merito potranno essere formulati solo a posteriori. Degna di nota, per il momento, è la possibilità che sistemi di IA, che se combinati con il mondo o con le tecniche del gioco possono risultare particolarmente pericolose per l'utente, siano in questo contesto prese in considerazione proprio per favorire un ambiente di gioco più sicuro. Di contro, l'uso di sistemi di IA per monitorare il comportamento dei giocatori potrebbe generare tensioni con il diritto alla protezione dei dati personali.

Tralasciando l'ontologica (e, forse, insanabile) contraddizione che connota il mondo del gioco pubblico ove lo Stato favorisce e contrasta al contempo il gioco e i suoi rischi, il Decreto pare consentire un passo in avanti verso la costruzione di un mercato dei giochi più a misura della persona del giocatore. In definitiva, il d.lgs. n. 41/2024 rappresenta un apprezzabile passo in avanti nel processo di regolamentazione del settore dei giochi pubblici. Tuttavia, la mancata esaustività delle disposizioni normative, unitamente ad una certa vaghezza di alcune innovazioni, lascia margini di incertezza che potrebbero essere sanati con interventi integrativi futuri. L'efficacia del Decreto potrà, dunque, essere pienamente valutata solo alla luce dell'applicazione pratica delle misure ivi previste, essendo, peraltro, essenziale integrare il quadro normativo così descritto con strumenti giuridici più incisivi, capaci di garantire un'effettiva tutela della persona del giocatore e di prevenire adeguatamente i rischi associati alle nuove forme di gioco.

MICHELE CIANCIMINO

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-03-25;41

2024/4(42)GG

42. Chiusa la consultazione pubblica AGCOM su Age Verification

Il 24 settembre 2024 l'Autorità per le Garanzie nelle Comunicazioni (**AGCOM**) ha approvato lo schema di regolamento contenente le "*Modalità tecniche e di processo per l'accertamento della maggiore età degli utenti ai sensi dell'articolo 13 bis del decreto-legge 5 settembre 2023, n. 123 convertito con modificazioni dalla della legge 13 novembre 2023, n. 159*",

ISSN 2239-8570

adottato al termine di una consultazione pubblica avviata con la delibera n. 61/24/CONS, del 6 marzo 2024 (su cui v. in questa Rubrica la notizia n. 9 nel numero 1/2024 [2024/1(9)SGh]). Si tratta dell'individuazione di sistemi tecnici di verifica dell'età anagrafica degli utenti online (*Age Assurance* o *Age Verification*), necessari per l'accesso a siti di carattere pornografico.

La competenza all'adozione dei sistemi di *Age Verification* è contenuta nel Decreto-legge 15 settembre 2023 n. 123, (cd. Decreto Caivano), che all'art. 13-bis ha stabilito che "*i gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto*" (comma 2). La competenza dell'Autorità a stabilire "*le modalità tecniche e di processo […] per l'accertamento della maggiore età degli utenti*" è prevista dal successivo comma 3.

La tutela online dei minori è, inoltre, oggetto di specifica disciplina europea. La Direttiva (UE) 2018/1808 del Parlamento Europeo e del Consiglio del 14 novembre 2018, ha inserito nella Direttiva (UE) 2010/13/UE (cd. Direttiva sui servizi media audiovisivi) l'art. 28-ter. Questa disposizione prevede che "*i fornitori di piattaforme per la condivisione di video […] adottino misure adeguate per tutelare: a) i minori da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale a norma dell'articolo 6 bis, paragrafo 1*" (paragrafo 1). Ai sensi del successivo paragrafo 3, secondo periodo, "*i contenuti maggiormente nocivi sono soggetti alle più rigorose misure di controllo dell'accesso*", tra le quali il legislatore comunitario include anche "*sistemi per verificare l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori*".

Questi obblighi sono stati trasposti nell'ordinamento italiano dal Decreto legislativo 8 novembre 2021, n. 208 (cd. Testo Unico dei Servizi di Media Audiovisivi – TUSMA), il cui 42, comma 7, introduce l'obbligo, in capo ai fornitori di piattaforma per la condivisione di video, di "*predisporre sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori*" (lett. f).

Ulteriori regole a tutela dei minori sono previste dal Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 (cd. Digital Services Act o DSA), a mente del quale le piattaforme online di dimensioni molto grandi (cd. VLOPs) ed i motori di ricerca online di dimensioni molto grandi (cd. VLOSEs), possono adottare "*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*" (art. 35, paragrafo 1, lett. j).

Al fine di dare seguito alle disposizioni del Decreto Caivano, AGCOM ha sottoposto a consultazione il modello del "doppio anonimato", in base al quale la prova della maggiore età è fornita da soggetti terzi indipendenti dai

ISSN 2239-8570

fornitori di contenuti, che non devono sapere per quale servizio viene eseguita la verifica dell'età. Ciò per evidenti esigenze di tutela dei dati personali.

Il processo di *Age Verification* individuato dall'Autorità è diviso in tre fasi:

1. il rilascio di una "prova dell'età" dai soggetti indipendenti, a seguito di apposita identificazione (ad esempio mediante accesso a un sito web tramite browser). Tali soggetti possono essere sia specializzati nella fornitura di identità digitale, sia organizzazioni o soggetti che hanno identificato l'utente in un diverso contesto. Occorre ricordare che il fornitore della prova dell'età non conosce l'utilizzo che l'utente ne farà;
2. la comunicazione della prova dell'età all'utente, che a sua volta la presenterà al sito o piattaforma visitata. La "prova dell'età" può essere, ad esempio, scaricata direttamente dall'utente attraverso il sito web del soggetto certificatore e poi inviata, sempre dall'utente via web, al sito o piattaforma visitata;
3. l'analisi della prova dell'età presentata dall'utente, ad opera del sito o della piattaforma che fornisce il contenuto (autenticazione).

La certificazione e la generazione della prova dell'età sono possibili, altresì, tramite apposita applicazione installata sul dispositivo dell'utente.

È importante rilevare che la validità della verifica dell'età persiste fino al momento in cui l'utente esce dal servizio, ovvero quando termina la sessione (quando l'utente esce dal browser o quando il sistema operativo entra in stand-by) e, comunque, dopo un periodo di 45 minuti di effettiva inattività.

Sotto il profilo tecnico, l'Autorità ha ritenuto opportuno adottare un approccio neutrale, lasciando ai soggetti tenuti alla realizzazione dell'*Age Assurance* una ragionevole libertà di valutazione e scelta, nell'ambito di una serie di principi:

- proporzionalità (giusto equilibrio tra i mezzi utilizzati per la verifica dell'età e il suo impatto sulla limitazione dei diritti delle persone);
- protezione dei dati personali;
- sicurezza (prevedere misure di mitigazione del rischio nel caso di attacchi informatici);
- precisione ed efficacia (efficaci sistemi di contenimento dell'errore nella determinazione dell'età);
- funzionalità, accessibilità, facilità d'uso e non ostacolo all'accesso ai contenuti in Internet (i sistemi di garanzia dell'età devono essere facili da usare e basati sulle capacità e caratteristiche dei minori);
- inclusività e non discriminazione;
- trasparenza (i soggetti regolamentati dovrebbero essere trasparenti nei confronti degli utenti per quanto riguarda i sistemi e i dati trattati e le finalità, mediante spiegazioni semplici, chiare e complete oltre che per maggiorenni anche per i minorenni);

ISSN 2239-8570

- formazione e informazione (l'Autorità ritiene importante informare e sensibilizzare i minori, i genitori, il personale della comunità educativa e della gestione giovanile sulle buone pratiche informatiche, sui rischi connessi a Internet);
- gestione dei reclami.

Il Regolamento in parola è stato notificato alla Commissione europea in quanto regola tecnica; il periodo di *stand still* è in scadenza alla fine di gennaio 2025, decorso il quale l'Autorità procederà all'approvazione definitiva del provvedimento.

GIORGIO GIULIANO
Funzionario AGCOM

https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-del-07-ottobre-2024

2024/4(43)VP

43. La consultazione pubblica di AGCOM sulla proposta di Codice di condotta per gli influencer elaborata dal Tavolo tecnico e su alcune proposta di modifica delle Linee guida degli influencer

Con Delibera 472/24/CONS del 26.11.2024, pubblicata l'11.12.2024 (la **Delibera AGCOM 472/24**), l'Autorità per le Garanzie nelle Comunicazioni (**AGCOM** o l'**Autorità**) ha aperto una consultazione pubblica di 45 giorni sulla proposta di codice di condotta degli influencer redatta dal tavolo tecnico appositamente costituito dall'Autorità con precedente delibera n. 7/24 CONS del 10.1.2024 (rispettivamente: la **Proposta di Codice di condotta**, il **Tavolo tecnico** e la **Delibera AGCOM 7/24**) e su alcune proposte di modifica delle linee guida sugli influencer già approvate con la medesima Delibera 7/24 (le **Linee guida**).

Rinviando a quanto già precedentemente esposto sulla Delibera AGCOM 7/24 e sulle Linee guida (v. in questa Rubrica la notizia n. 29 nel numero 2/2024 [2024/2(29)VP]), qui di seguito riassumiamo la finalità della consultazione pubblica di cui alla Delibera AGCOM 472/24.

In particolare, AGCOM ha deciso di avviare una pubblica consultazione per consentire alle parti interessate di far pervenire all'Autorità le proprie osservazioni in merito ad alcune proposte di modifica (allegate come Allegato A alla Delibera AGCOM 472/24) relative ai **punti 5 e 9, lett. d) delle Linee guida** e alla **Proposta di Codice di condotta** (allegata come Allegato B alla Delibera AGCOM 472/24).

Tali osservazioni andranno dunque ad integrare quelle fornite da chi ha partecipato ai lavori del Tavolo tecnico, ovvero rappresentanti di piattaforme digitali, associazioni di influencer, agenzie di marketing ed altri stakeholders.

Quanto alle Linee guida (sulle quali, v. in questa Rubrica la notizia n. 29 nel numero 2/2024 [2024/2(29)VP]), si ricorda innanzitutto che esse sono

ISSN 2239-8570

volte garantire il rispetto delle disposizioni del D.Lgs. 208/2021 (il Testo **Unico dei servizi di media audiovisivi**, o **TUSMA**, o **Testo Unico**) da parte degli influencer.

La consultazione pubblica **sulle Linee guida** riguarda **tre punti**.

Il primo punto concerne la **nozione di influencer rilevanti** (come definiti al punto 2 delle Linee guida), la quale serve a identificare quali siano i soggetti destinatari delle regole contenute nel Codice di condotta.

A tal proposito, la nuova formulazione si propone di ridurre in maniera significativa le soglie quantitative. Nello specifico, si assoggetta a consultazione pubblica la proposta di modificare le Linee guida in modo che un influencer sarà considerato "rilevante" qualora raggiunga **500.000 follower o un numero di visualizzazioni medie mensili pari ad un milione** su almeno una piattaforma di social media o di condivisione video utilizzata. Tali soglie potranno essere oggetto di periodica revisione da parte dell'Autorità, anche a fronte dell'eventuale implementazione di nuove piattaforme di social media.

Diversamente, gli influencer che operano in modo meno continuativo e strutturato, e che non raggiungono le soglie stabilite, non saranno soggetti alle disposizioni previste dalle Linee-guida e dal codice di condotta.

Per questi soggetti, resta tuttavia fermo l'obbligo di conformità agli artt. 41 e 42 del TUSMA, per quanto riguarda le piattaforme di condivisione dei contenuti.

Il secondo punto della consultazione pubblica sulle Linee guida consiste nella proposta di integrare all'interno del Codice di condotta il c.d. **Regolamento "Digital Chart"** sulla riconoscibilità della comunicazione commerciale diffusa attraverso Internet, elaborato dall'Istituto dell'autodisiplina pubblicitario (IAP), al fine di rendere manifesta la finalità promozionale delle comunicazioni commerciali online.

Il terzo e ultimo punto è quello relativo all'**autopromozione**, intesa come l'attività attraverso la quale un influencer promuove sul proprio profilo beni o servizi riconducibili alle sue aziende. In proposito, la consultazione pubblica ha ad oggetto la proposta di esonerare l'influencer dall'obbligo di segnalazione solo nell'ipotesi in cui si tratti di opere di cui questo è autore o di prodotti / servizi legati ad un marchio che corrisponda chiaramente al suo nome.

Per quanto riguarda la **Proposta di Codice di condotta**, tra gli elementi centrali emerge la proposta di incaricare un **soggetto terzo e imparziale della predisposizione, gestione ed aggiornamento dell'elenco degli influencer**. Il soggetto incaricato dovrà avere una comprovata esperienza nel campo dell'analisi dei dati di audience e di consumo di servizi media. L'elenco dovrà essere aggiornato con cadenza semestrale (par. 2.2 Proposta di Codice di condotta).

Quanto alla **riconoscibilità**, la Proposta di Codice di condotta prevede che gli influencer tenuti al rispetto delle disposizioni richiamate nelle Linee Guida e nel Codice di condotta dovranno inserire nello spazio dedicato alla presentazione del proprio profilo il nome e il cognome oppure, in caso di persona giuridica, la propria denominazione o ragione sociale, il proprio marchio, nonché la dicitura "*influencer in elenco AGCOM*" o, nel caso di

ISSN 2239-8570

influencer virtuale, "*influencer virtuale in elenco AGCOM*" (par. 2.3 Proposta di Codice di condotta).

La Proposta di Codice di condotta contiene inoltre una serie di disposizioni per assicurare il rispetto da parte degli influencer delle norme in tema di **tutela dei diritti fondamentali, dei minori e delle "altre categorie vulnerabili"**, tra cui quelle che vietano la pubblicazione di contenuti gravemente nocivi allo sviluppo fisico, mentale o morale dei minori e che arrecano pregiudizio al decoro o alla reputazione dei minori (par. 3.1 Proposta di Codice di condotta), quelle che prevedono il divieto di sfruttamento di inesperienza, credulità e fiducia (par. 3.2 Proposta di Codice di condotta), e quelle in materia di filtri ed altri meccanismi di modifica dei contenuti (par. 3.3 Proposta di Codice di condotta).

Il cammino verso la creazione di un ambiente digitale più trasparente ed etica è ancora lungo. Tuttavia, l'interesse che sembra crearsi attorno a questa consultazione pubblica, lascia ben sperare, così come la crescente consapevolezza sulle nuove forme di marketing nella dimensione della comunicazione. Il fenomeno della comunicazione, anche commerciale, in un mondo sempre più globalizzato, ha fatto emergere il ruolo degli influencer, non più solo creatori di contenuti di intrattenimento ma veri e propri creatori di strategie di marketing sofisticate, destinate ad incidere in maniera sempre più significativa sulle scelte dei consumatori.

VINCENZO PITTELLI

https://www.agcom.it/sites/default/files/media/allegato/2024/472_24_CONS_Allegato%20A_0.pdf
https://www.agcom.it/sites/default/files/media/allegato/2024/472_24_CONS_Allegato%20B_0.pdf
https://www.agcom.it/sites/default/files/media/allegato/2024/472_24_CONS_Allegato%20C_0.pdf

2024/4(44)EB

44. Il provvedimento n. 755 del 2.11.2024 del Garante privacy di chiusura dell'istruttoria e di irrogazione di sanzione di 15 milioni di euro nei confronti di Open AI per il servizio ChatGPT e la contestuale comunicazione all'autorità di controllo irlandese per l'accertamento di eventuali ulteriori violazioni del GDPR in conseguenza dello stabilimento di OpenAI in Irlanda

Con il provvedimento n. 755 del 2 novembre 2024 (di seguito il **Provvedimento del 2.11.2024**) il Garante per la protezione dei dati personali (il **Garante italiano** o l'**Autorità**) ha chiuso l'istruttoria avente ad oggetto il servizio ChatGPT offerto e gestito da OpenAI OpCo LLC (**OpenAI** o la **Società**).

Le determinazioni del Garante vengono pubblicate, non integralmente, dopo un'istruttoria durata più di un anno, avviata nel marzo del 2023 e due

ISSN 2239-8570

provvedimenti adottati dall'Autorità il 30 marzo 2023 e l'11 aprile 2023 (sui quali v. in questa Rubrica la notizia n. 5 nel numero 1/2023 [2023/1(5)SO], e in *Atlante*, p. 303).

In particolare, l'istruttoria aveva preso avvio nel marzo del 2023 allorquando Autorità apprese, tramite i quotidiani, di alcune problematiche tecniche (*bug*) occorse il 20 marzo 2023, per cui sulla pagina principale del servizio ChatGPT, l'utente visualizzava la cronologia dei titoli delle chat di altri utilizzatori del servizio anziché le proprie. In seguito, la Società pubblicamente confermava l'accaduto e precisava che i dati coinvolti nella problematica tecnica che avrebbero potuto essere visualizzati da utenti diversi dagli interessati erano il nome, il cognome, l'indirizzo e-mail, nonché le ultime quattro cifre e la scadenza della carta di credito utilizzata per il pagamento del servizio ChatGPT Plus (la versione a pagamento del servizio).

Alla luce di quanto sopra, l'Autorità avviava un' istruttoria ex officio rilevando, oltre al **data breach**, diverse e numerose violazioni del regolamento (UE) 2016/679 (**GDPR** di seguito anche solo il **Regolamento**): **mancanza di trasparenza** nei confronti degli utenti e dei non utenti i cui dati sono utilizzati nell'ambito del servizio ChatGPT; **assenza di una base giuridica** idonea all'utilizzo dei dati ai fini dell'addestramento degli algoritmi; non corrispondenza di alcune delle informazioni fornite da ChatGPT al dato reale e conseguente **inesattezza** dei dati personali oggetto delle attività di trattamento del titolare; **assenza di un sistema di age verification**.

Di conseguenza, l'Autorità dapprima, con provvedimento del 30 marzo 2023, limitava provvisoriamente il servizio in Italia, salvo poi revocare tale limitazione e prescrivere a OpenAI, l'11 aprile 2023, una serie di adempimenti per poter commercializzare il servizio in Italia, riservandosi ogni ulteriore intervento, anche di carattere urgente e temporaneo, nel caso di inidonea o insufficiente attuazione delle misure prescritte (v. in questa Rubrica la notizia n. 5 nel numero 1/2023 [2023/1(5)SO], e in *Atlante*, p. 303).

Parallelamente, l'Autorità ha portato avanti una istruttoria per accertarsi se i trattamenti eseguiti fino al 30 marzo 2023 – in quel momento solo censurati – integrassero delle aperte violazioni della normativa sul trattamento dei dati personali, nonché verificare se le prescrizioni impartite fossero state recepite.

Con il Provvedimento del 2.11.2024, il Garante italiano ha di fatto accertato **sei violazioni del GDPR**, alcune di natura non continuata, altre, invece, di natura continuata e attuali alla data del medesimo provvedimento. Per queste ultime, **il Garante italiano si è ritenuto incompetente e ha disposto la trasmissione degli atti** all'autorità di controllo per la protezione dei dati personali irlandese (di seguito anche il **Garante irlandese**) quale **autorità capofila**.

Per spiegare questa parte del Provvedimento del 2.11.2024, bisogna aggiungere che **in data 25 febbraio 2024 OpenAI ha stabilito in Irlanda la sua società consociata Open AI Ireland e che, prima di allora, OpenAI non risultava stabilita nell'Unione europea**. Di conseguenza, per

ISSN 2239-8570

le violazioni continuative (ovvero di natura permanente) ai sensi dell'art. 56 GDPR, il Garante italiano ha ritenuto competente l'autorità di controllo capofila, individuata nel Garante irlandese. Ciò in quanto, sulla scorta del parere dell'EDPB n. 8/2019 [non "8/2020" come si trova citato per errore nel provvedimento in commento] del 9 luglio 2019 sulla competenza di un'autorità di controllo in caso di mutamento delle circostanze relative allo stabilimento principale o unico, il Garante Italiano ha ritenuto di non poter procedere, per questi specifici profili permanenti, e quindi ancora in essere alla data 15 febbraio 2024, *dies a quo* dello stabilimento della Società nell'Unione europea, attraverso la società consociata OpenAI Ireland Ltd. Dovendosi applicare da tale data il meccanismo dello sportello unico con conseguente passaggio della competenza all'autorità di controllo capofila, ai sensi dell'art. 56 del Regolamento, individuata nella Data Protection Commission irlandese, sulla scorta del già citato parere dell'EDPB 8/2019, il Garante italiano ha dunque ritenuto di non poter, per questo specifico profilo, procedere per difetto di competenza e ha disposto la trasmissione degli atti all'autorità capofila irlandese.

Nel merito**, la prima violazione accertata dal Garante italiano è stata la violazione dell'art. 33 GDPR per aver omesso di notificare all'Autorità l'evento di violazione dei dati occorso il 20 marzo 2023.**

A tal proposito, la Società ha dichiarato di aver notificato entro le 72 ore stabilite dal GDPR la violazione di dati personali al Garante irlandese, ritenendo che questa avrebbe poi condiviso le informazioni anche con gli altri membri del Comitato, tra cui il Garante italiano. È, infatti, emerso come nel data breach che ha dato avvio all'istruttoria siano stati coinvolti 440 interessati italiani.

Il Garante italiano però ha ritenuto insufficiente che la violazione sia stata notificata solo al Garante irlandese, poiché il meccanismo dello sportello unico non era applicabile al tempo in cui è si è verificato l'incidente di sicurezza in quanto la Società non era stabilita nell'Unione europea e dunque Open AI avrebbe dovuto informare anche il Garante italiano.

La seconda violazione accertata dal Garante italiano ha ad oggetto gli artt. 5(2) e 6 del GDPR, in quanto la Società non avrebbe individuato una corretta base giuridica prima dell'inizio dell'attività di trattamento, sulla cui scorta effettuare il trattamento dei dati personali per finalità di addestramento del modello GPT sotteso al funzionamento del servizio, reso disponibile al pubblico a far data dal 30 novembre 2022.

In sede di interlocuzione, Open AI ha rappresentato che alla data del lancio di ChatGPT al pubblico questa era in linea con i principî di protezione dei dati, ma non era soggetta al GDPR, in quanto il servizio non era stato "lanciato" agli interessati europei, benché fosse comunque a loro accessibile. In ogni caso, la Società ha sostenuto di aver basato le operazioni di trattamento relative alla fornitura del servizio agli utenti sulla base giuridica dell'esecuzione del contratto (art. 6(1)(b) GDPR) e le operazioni di trattamento relative all'addestramento degli algoritmi sulla base giuridica del legittimo interesse (art. 6(1)(f) GDPR).

ISSN 2239-8570

Tuttavia, l'Autorità ha ritenuto che il supporto documentale allegato a riprova di quanto sopra fosse insufficiente a far ritenere che Open AI avesse, all'epoca dei fatti, individuato la corretta base giuridica su cui fornire il servizio. Inoltre, anche le informazioni rilasciate agli utenti solo in un momento successivo al lancio del servizio, ossia che l'utilizzo dei dati per lo "sviluppo dei servizi" si sarebbe basato sulla base giuridica del legittimo interesse, non sono state ritenute dal Garante italiano sufficientemente chiare e intellegibili, a prescindere da ogni valutazione di merito relativa all'idoneità del legittimo interesse a fungere da base giuridica del trattamento. Tale ultimo aspetto è stato demandato alla competenza del Garante irlandese, in quanto relativa ad una violazione di natura continuata.

Il Garante italiano ha poi contestato a OpenAI la violazione degli artt. 5(1)(a), 12 e 13 GDPR per omissioni e carenze nella privacy policy (versione del 14 marzo 2023), vigente al 30 marzo 2023.

È stato rilevato, infatti, che in un primo momento l'informativa era stata pubblicata in lingua inglese e non risultava di facile reperibilità sul sito. In particolare, il link all'informativa era accessibile solo successivamente alla registrazione, tale per cui l'interessato non era messo nelle condizioni di leggere le informazioni sul trattamento dei dati prima di creare un account.

Inoltre, le informazioni rese al tempo dal titolare si riferivano, esclusivamente, ai dati degli utenti trattati dalla Società per l'utilizzo del servizio, mentre, sia agli utenti che ai non utenti, non veniva fornita alcuna informazione in relazione al trattamento dei dati personali per fini di addestramento degli LLM.

Un ulteriore rilievo ha riguardato la violazione degli artt. 8, 24 e 25(1) GDPR per omessa predisposizione di idonei sistemi atti a verificare l'età dei soggetti alla data del 30 marzo 2023.

Dall'istruttoria, il Garante italiano ha potuto verificare che i minori di età erano compresi tra i potenziali utenti di ChatGPT e che, in tal caso, per perfezionare il vincolo contrattuale con la piattaforma i minori dovessero ottenere il consenso del titolare della responsabilità genitoriale. Tuttavia, è stato notato dall'Autorità come la Società non fosse in grado di appurare che vi fosse stato un effettivo coinvolgimento dei titolari della responsabilità genitoriale.

Alla luce di quanto precede il Garante italiano ha ritenuto che, alla data del 30 marzo 2023, il titolare (OpenAI) non avesse, ex art. 24 GDPR, messo in atto misure volte a garantire che il trattamento dei dati all'atto di iscrizione al servizio ChatGPT fosse conforme al GDPR, né, ex art. 25 GDPR, che la Società avesse adottato misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

OpenAI ha comunque rappresentato come a far data dal 30 marzo 2023 fossero stati introdotti dei meccanismi di age verification tramite un fornitore esterno che non trasmette i dati alla stessa. Inoltre, è stato fatto presente come, con riferimento a quanto contestato, gli utenti, compresi quelli di età inferiore ai 18 anni, hanno avuto la possibilità di opporsi al trattamento delle loro conversazioni ChatGPT ai fini di addestramento fin

ISSN 2239-8570

dall'inizio, quando ChatGPT è stato rilasciato per la prima volta il 30 novembre 2022. Per gli utenti che non si sono opposti all'utilizzo dei loro dati per le finalità di addestramento, OpenAI ha dichiarato di aver adottato misure di protezione della privacy-by-design (pseudonimizzazione e revisione umana), come prescritto dall'articolo 25 GDPR, prima che le conversazioni potessero essere utilizzate nel processo di addestramento.

Invero, quanto accertato dall'Autorità riguarda l'omessa previsione da parte della Società di verifiche funzionali ad impedire l'accesso al servizio ad interessati minori di 13 anni ed a garantire il coinvolgimento nel processo di iscrizione del titolare della responsabilità genitoriale per i minorenni di età compresa tra i 13 ed i 18 anni, ai fini dell'ottenimento della relativa autorizzazione, come richiesto dai termini e dalle condizioni contrattuali definiti dalla Società stessa.

L'Autorità, invece, non ritiene sussistano idonei elementi per ritenere accertata la violazione, contestata ex art. 166, co. 5 del Codice per la protezione dei dati personali (**Codice Privacy**), relativa al consenso digitale dei minori di cui all'art. 8 del Regolamento atteso che la base giuridica di riferimento, come sopra illustrato, è stata individuata nell'esecuzione del contratto ex art. 6(1)(b) GDPR.

Per quanto sopra rappresentato, si ritiene che OpenAI abbia violato gli artt. 24 e 25(1) GDPR e che detta violazione, accertata alla data del 30 marzo 2023, debba ritenersi consumata il 30 novembre 2022 e sia di natura non continuata.

A quanto sopra si aggiunga la violazione delle dell'art. 83(5)(d) GDPR per omessa osservanza di un ordine dell'Autorità, segnatamente l'ordine di messa in conformità di cui al punto 9 del provvedimento n. 114/2023 (ossia delle modalità prescritte per l'esecuzione di una campagna informativa al pubblico, previa consultazione del Garante stesso).

L'Autorità ritiene che OpenAI non abbia adempiuto a quanto dallo stesso prescritto in quanto la campagna informativa promossa, come realizzata alla data del 15 maggio 2023, non è stata concordata con l'Autorità, né la stessa è risultata idonea, per la scelta dei mezzi e delle modalità di comunicazione, nonché per il tempo assai limitato della stessa, a raggiungere la generalità del pubblico interessato dai servizi ChatGPT.

In ultimo, ed è questa la violazione più rilevante, il Garante italiano ha contestato ad OpenAI la violazione dell'art. 5(1)(d) GDPR in quanto il servizio ChatGPT, alla data del 30 marzo 2023, generava output inesatti.

La questione tecnico-giuridica è relativa all'accuratezza dei Large Language Model (**LLM**) ed è stata oggetto di valutazione anche da parte della task force europea creata dall'EDPB il 13 aprile 2023 (su cui v. in questa Rubrica la notizia n. 3 sul numero 1/2023 [2023/1(3)SO], e in *Atlante*, p. 300).

Nel report finale, approvato in data 23 maggio 2024 e pubblicato il successivo 24 maggio (su cui v. in questa Rubrica la notizia n. 13 nel numero 2/2024 [2024/2(13)AN]), la task force ha rilevato come lo scopo del trattamento dei dati di OpenAI sia quello di addestrare il modello linguistico GPT sotteso ai servizi ChatGPT e non necessariamente quello di fornire

ISSN 2239-8570

informazioni accurate, in quanto la natura probabilistica del sistema porta il modello a produrre risultati parziali o discriminatori (biased).

Tuttavia, è probabile che i risultati forniti da ChatGPT siano considerati di fatto accurati dagli utenti finali indipendentemente dalla loro effettiva accuratezza. Risulta, pertanto, importante che il titolare del trattamento fornisca informazioni adeguate sui meccanismi probabilistici di creazione degli output e sul loro limitato livello di affidabilità, compreso un riferimento esplicito al fatto che il testo generato, sebbene sintatticamente corretto, possa essere distorto o discriminatorio.

Nella memoria difensiva, OpenAI ha evidenziato che fin dal lancio del servizio nel novembre 2022, questa ha chiarito agli utenti che ChatGPT non deve essere considerato una fonte affidabile di informazioni. Questo concetto è stato comunicato tramite dichiarazioni, avvisi, articoli, FAQ sul sito web e una finestra pop-up dedicata per avvisare gli utenti sulla possibile imprecisione delle risposte fornite dal servizio.

La Società ha inoltre illustrato le misure adottate durante ogni fase di addestramento: nella fase di pre-addestramento per identificare e rimuovere informazioni imprecise o potenzialmente dannose, nella fase di post-addestramento per insegnare ai modelli a rifiutare di fornire dati privati o sensibili, e durante l'uso del servizio per permettere agli utenti di segnalare inesattezze e richiederne la correzione.

La Società ha sottolineato che, sebbene non sia tecnicamente possibile ottenere un'accuratezza del 100% in un modello linguistico di grandi dimensioni, OpenAI si impegna a migliorare l'accuratezza dei suoi modelli non per renderli fonti di informazioni definitive, ma per rendere ChatGPT più utile agli utenti. Inoltre, uno studio del novembre 2023 avrebbe riconosciuto a ChatGPT (nelle versioni **GPT 4**, **GPT 4 Turbo** e **GPT 3.5**) il più basso tasso di allucinazioni tra i principali servizi di intelligenza artificiale generativa.

Tale ultima violazione del principio di esattezza dei dati è stata accertata dal Garante ma non sanzionata, in quanto, essendo di natura continuativa, dovrà essere affrontato dall'autorità capofila: la Data Protection Commission irlandese.

In conclusione, alla luce delle violazioni sopra descritte il Garante ha comminato a OpenAI **una sanzione di quindici milioni di euro** calcolata anche tenendo conto dell'atteggiamento collaborativo della Società.

Ha, inoltre, ordinato a OpenAI, utilizzando per la prima volta i nuovi poteri previsti dall'articolo 166, comma 7 del Codice Privacy, di realizzare una campagna di comunicazione istituzionale di 6 mesi su radio, televisione, giornali e Internet. Interessante aggiungere, in proposito, che ai sensi della medesima disposizione di legge (art. 166, co. 7 Codice Privacy) la pubblicazione dell'ordinanza-ingiunzione per intero o per estratto sul sito internet del Garante italiano è formulata letteralmente come sanzione accessoria alternativa a quella dell'ingiunzione a realizzare simili campagne promozionali, e che, per questo motivo, effettivamente, del Provvedimento del 2.11.2024 non si è diffusa pubblicamente notizia in Italia fino alla fine del mese di dicembre.

ISSN 2239-8570

Tornando alla campagna promozionale, i relativi contenuti, da concordare con l'Autorità, dovranno promuovere la comprensione e la consapevolezza del pubblico sul funzionamento di ChatGPT, in particolare sulla raccolta dei dati di utenti e non-utenti per l'addestramento dell'intelligenza artificiale generativa e i diritti esercitabili dagli interessati, inclusi quelli di opposizione, rettifica e cancellazione.

La finalità della campagna di comunicazione consiste nel sensibilizzare gli utenti e i non-utenti di ChatGPT su come opporsi all'addestramento dell'intelligenza artificiale generativa con i propri dati personali e, quindi, su come essere effettivamente posti nelle condizioni di esercitare i propri diritti ai sensi del GDPR.

Tale ultima violazione del principio di esattezza dei dati è stata accertata dal Garante ma non sanzionata, in quanto, essendo di natura continuativa, dovrà, eventualmente, essere affrontato dal Garante irlandese, in quanto autorità capofila, per i motivi sopra riassunti.

EMANUELA BURGIO

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085455

2024/4(45)FRo

45. Approvato dal Garante Privacy il 17.10.2024 ed entrato in vigore il 28.11.2024 il "Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale" elaborato da Assosoftware

Con provvedimento n. 10075998 del 17 ottobre 2024, il Garante italiano per la Protezione dei dati personali (il **Garante** o l'**Autorità**) ha approvato il "*Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale*" (il **Codice di Condotta** o solo il **Codice**), elaborato ai sensi dell'art. 40 del regolamento (UE) n. 2016/679 (**GDPR**) dall'Associazione Italiana dei Produttori di Software (**Assosoftware**), che rappresenta le imprese operanti in Italia nel settore della produzione di software di tipo gestionale. Con lo stesso provvedimento, ha altresì deliberato l'accreditamento dell'Organismo di monitoraggio (**ODM**) proposto nel Codice, per un periodo non rinnovabile di 5 anni.

Il Codice è stato dunque pubblicato sulla Gazzetta Ufficiale il 27 novembre 2024, nella Serie Generale n. 278, ed è entrato in vigore il giorno successivo alla pubblicazione (28 novembre 2024), così come indicato dall'**art. 22** del Codice stesso. Esso è costituito da un preambolo, 22 articoli e 5 allegati.

Tra le premesse che hanno indotto il Garante, competente territorialmente a pronunciarsi in merito, a ritenere sia il Codice che l'ODM rispondenti a quanto previsto rispettivamente dagli artt. 40 e 41 del GDPR e

ISSN 2239-8570

dalle "Linee guida 1/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679" del Comitato europeo per la protezione dei dati (**EDPB**), meritano una particolare menzione le considerazioni circa la **sufficiente rappresentatività di Assosoftware** nel settore di riferimento, nonché il ruolo centrale rivestito dai codici di condotta nella definizione di regole operative utili soprattutto alle **micro, piccole e medie imprese**.

Venendo adesso al **contenuto** del Codice di condotta, esso risponde all'esigenza di fornire **regole chiare e pratiche** in materia di protezione dei dati personali alle imprese italiane produttrici di software gestionale – altresì definite "*Software House*" (**art. 2.2, lett. a**) – e attestare l'importanza del settore nel quale esse operano quale volano dell'incremento delle competenze digitali, della modernizzazione dei processi produttivi e, più in generale, dello sviluppo del Paese.

Come riportato nel Preambolo del Codice (**Preambolo n. 1**), il potenziamento di tale settore costituisce, infatti, un **fattore chiave** per la crescita economica e l'occupazione dell'Italia, nonché un elemento essenziale per il completamento di quell'opera di digitalizzazione di imprese, professionisti e pubbliche amministrazioni lungo tutta la catena del valore, che costituisce da tempo l'obiettivo di numerose agende politiche nazionali e internazionali – così come testimoniato, solo da ultimo, dalla strategia dell'UE del c.d. Decennio digitale europeo (2030 Digital Decade).

In linea con quanto predisposto agli artt. 5 e 6 delle già citate Linee Guida dell'EDPB (le **Linee guida EDPB 1/2019**), il Codice di condotta in oggetto (**Preambolo n. 2**) insiste sulla necessità di far fronte alla **concreta esigenza** di assicurare che le attività svolte dalle imprese produttrici di software rappresentate da Assosoftware si conformino ad elevati livelli di protezione dei dati personali nell'intero ciclo di vita del software gestionale: a partire dalla sua progettazione, produzione e sviluppo, sino alla sua installazione e messa in esercizio.

Lo scopo ultimo del Codice di condotta è triplice e comprende l'esigenza di favorire il **rispetto del GDPR**, il proposito di **rafforzare la fiducia** degli utilizzatori di software, compresi i professionisti, le piccole e medie imprese e le pubbliche amministrazioni, e la volontà di fornire, specialmente agli operatori più piccoli del mercato ("micro, piccole e medie imprese", cfr. art. 40(1) GDPR), strumenti adeguati per **conseguire la transizione digitale**.

Sulla scia di tale premessa, il **paragrafo 3 del Preambolo** dà evidenza dell'obiettivo del Codice di fornire un contributo effettivo alla "definizione degli impegni assunti per garantire il diritto alla protezione dei dati personali" e rendere disponibili ai "soggetti che richiedono ai Produttori lo sviluppo ed installazione dei Software Gestionali e le connesse attività di manutenzione ed assistenza" – i c.d. Clienti (**art. 2.2, lett. e**) – **strumenti e funzionalità idonei** per adempiere ai propri obblighi di protezione dei dati in relazione ai trattamenti dagli stessi svolti, in qualità di titolari o responsabili del trattamento, tramite i predetti software.

A tal fine, il Codice stabilisce un sistema uniforme ed avanzato di regole di condotta e di misure tecniche e organizzative (**Preambolo n. 4 e 5**), volto a promuovere tra i Clienti richiedenti e gli utilizzatori di software gestionali

ISSN 2239-8570

la conformità ai principi di *privacy-by-design* e *privacy-by-default*, così come richiamati anche dall'art. 40(2)(h) GDPR e dall'art. 3 delle Linee guida EDPB 1/2019.

Tra le **attività oggetto del Codice di condotta** rientrano tutte quelle che possono comportare operazioni di trattamento di dati personali da parte dei Produttori di software per conto dei Clienti, quali ad esempio l'**installazione, il test, il collaudo, l'assistenza, la manutenzione e l'aggiornamento** dei Software Gestionali (**Preambolo n. 6**), nonché quelle svolte dalle Software House **quali titolari del trattamento** per finalità amministrative, contabili, organizzative e tecniche correlate alla gestione del rapporto contrattuale in essere con i propri Clienti (**art. 8**). Le attività di progettazione e sviluppo del software, non implicando di regola il trattamento di dati personali, sono oggetto del Codice di condotta **solo laddove comportino, in via eccezionale,** lo svolgimento di simili operazioni di trattamento.

Sono, invece, **escluse dall'ambito applicativo** del Codice di condotta le attività di trattamento di dati personali eventualmente svolte dal Produttore del Software **per conto del Cliente**, quali servizi di elaborazione di dati a fini contabili, amministrativi, retributivi, previdenziali, assistenziali e fiscali, come ad esempio, l'elaborazione di paghe, la tenuta della contabilità, la fatturazione, ecc. (**Preambolo n. 7**).

Dell'articolato che costituisce il cuore del Codice di condotta, destano particolare attenzione **l'art. 1**, che ne delinea l'ambito di applicazione, limitandolo territorialmente ai trattamenti di dati effettuati in Italia, nonché **l'art. 2**, che fornisce un elenco di definizioni specifiche del settore della produzione dei software gestionali e risponde così al proposito, ben evidenziato dall'art. 6.2 delle Linee guida EDPB 1/2019, di facilitare una più efficace applicazione del GDPR in tale campo tramite la fissazione di concetti comuni. Tra queste, vi sono le già richiamate definizioni di Produttore di Software e di Clienti, ma anche quella di Software Gestionale, di Servizi, di Attività di Sviluppo e di Utenti.

Interessanti sono altresì l'**art. 3**, che richiama **l'allegato A** recante le misure tecniche e organizzative che devono essere poste in essere dai Produttori di software per garantire il rispetto dei principi di *privacy-by-design* e *privacy-by-default* nelle attività di sviluppo dei software gestionali, nonché l'**art. 11**, che rimanda all'**Allegato B**, contenente le misure di sicurezza da adottare per lo svolgimento dei servizi di installazione, messa in esercizio, assistenza, ecc. L'importanza di tali allegati è tanto più evidente se si considera che essi costituiscono un esempio concreto di quello sforzo di specificazione delle disposizioni del GDPR che rappresenta uno dei punti cardine dell'adozione di simili codici di condotta.

Meritano una particolare menzione anche gli artt. **4, 5, 6 e 7**, che forniscono alcune regole operative a cui i Produttori di software devono uniformarsi ogniqualvolta svolgono attività per conto del Cliente in qualità di Responsabili o Sub-responsabili del trattamento *ex* art. 28 GDPR. Tra queste, è fatto espresso richiamo alle attività di migrazione di dati finalizzata all'installazione del Software, attività di assistenza e

ISSN 2239-8570

aggiornamento dei software con accesso da remoto, acquisizione o esportazione di copia di dati per la verifica di problematiche tecniche, ecc.

Significativi sono inoltre **l'art. 19**, che istituisce un ODM preposto a garantire il rispetto del Codice di condotta (cfr. definizione di cui all'art. 2 delle Linee guida EDPB 1/2019), rimandando all'**Allegato D** l'esplicazione del suo operato, nonché l'**art. 20**, che reca indicazioni circa le modalità di adesione al Codice di condotta, altresì specificate nell'**Allegato E**, e **l'art. 21** che sancisce, in caso di necessità, come ad esempio alla luce di eventuali novità normative, la possibilità di un suo riesame.

Il resto dell'articolato fornisce, infine, ulteriori regole specifiche per il settore della produzione dei software gestionali, che includono ad esempio indicazioni sulla tenuta dei registri dei trattamenti (**art. 9**), sullo svolgimento della valutazione d'impatto privacy (**art. 10**), sulle istruzioni e sulla formazione da impartire alle persone autorizzate al trattamento operanti sotto il controllo della *Software House* (**art. 13**), sulla gestione degli incidenti di sicurezza (**art. 12**), delle istanze per l'esercizio dei diritti degli interessati (**art. 14**) e delle richieste di informazioni da parte del Cliente (**art. 17**), sul trasferimento dei dati in Paesi terzi (**art. 15**), sulla definizione dei tempi di conservazione dei dati (**art. 16**) e sulla cooperazione con le autorità competenti in caso di controlli e attività istruttorie dalle stesse svolte (**art. 18**).

FRANCESCA ROTOLO

https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10075998

https://www.gpdp.it/documents/10160/0/Codice+di+condotta+per+il+trattamento+dei+dati+personali+effettuato+dalle+imprese+di+sviluppo+e+produzione+di+software+gestionale.pdf/a89ad70a-ee18-22fa-8e01-578b04f1023e?version=2.0

2024/4(46)EG

46. La notifica da parte del Garante privacy di procedimenti correttivi e sanzionatori a 18 Regioni e alle Province autonome di Trento e Bolzano per violazioni della disciplina sul FSE 2.0

Con comunicato apparso sulla *newsletter* del 26 giugno 2024, il Garante per la protezione dei dati personali (il **Garante** o l'**Autorità**) ha reso noto di aver avviato procedimenti correttivi e sanzionatori nei confronti di 18 Regioni e nei confronti delle Province autonome di Trento e Bolzano per violazione della normativa in materia dei dati personali nell'attuazione – da parte delle Province e Regioni coinvolte – del c.d. fascicolo sanitario elettronico 2.0 ("**FSE 2.0**") disciplinato nel decreto del Ministero della salute del 7 settembre 2023.

ISSN 2239-8570

Le violazioni riscontrate all'esito dell'istruttoria sul FSE avviata dal Garante a fine gennaio 2024, originano dalla circostanza che 18 Regioni e le due Province autonome del Trentino Alto Adige hanno "*modificato, anche significativamente, il modello di informativa predisposto dal Ministero, previo parere del Garante, che avrebbe dovuto essere adottato su tutto il territorio nazionale"*. Infatti *"le difformità riscontrate hanno reso evidente che alcuni diritti (es. oscuramento, delega, consenso specifico) e misure (es. misure di sicurezza, livelli di accesso differenziati, qualità dei dati) introdotte dal decreto, proprio a tutela dei pazienti, non sono garantite in modo uniforme in tutto il Paese. Oppure sono esercitabili ed esigibili solo dagli assistiti di talune Regioni e Province autonome, con un potenziale e significativo effetto discriminatorio sugli assistiti"*.

La *ratio* sottesa alle decisioni assunte dal Garante risulta più comprensibile se collocata nel contesto normativo in cui si inserisce la nuova disciplina del FSE 2.0.

Il Decreto del 7 settembre 2023 emanato dal Ministero della Salute (su cui v. in questa Rubrica notizia n. 22 del numero 3/2023 [2023/3(22)EG] e in *Atlante*, p. 414) (innanzi il **Decreto**) stabilisce, infatti, i contenuti del FSE 2.0, delineando i confini delle responsabilità e i doveri dei soggetti designati alla sua realizzazione. Inoltre, definisce le modalità di fruizione, nonché le tutele e le misure di protezione da adottare nella gestione dei dati personali ai fini di una piena e corretta tutela dei diritti dell'assistito. A tal proposito, l'art. 7 del Decreto specifica che: "*in ottemperanza all'adempimento di cui agli articoli 13 e 14 del Regolamento UE 2016/679, quale presupposto di liceità del trattamento, entro tre mesi dalla data di entrata in vigore del presente decreto, deve essere fornita all'assistito, da parte del Ministero della salute, delle Regioni e Province autonome, idonea informativa che espliciti i trattamenti dei dati del FSE*". In poche parole, emerge in modo evidente la necessità di garantire all'assistito informazioni chiare e complete in relazione alle caratteristiche e alle modalità di trattamento dei suoi dati personali all'interno del FSE. Ancora, al comma 4 dello stesso articolo, si stabilisce che: "*al fine di garantire all'interessato informazioni omogenee e uniformi nel territorio nazionale, il Ministero della salute predispone, in collaborazione con le Regioni e Province autonome, un modello di informativa, che mette a disposizione attraverso la pubblicazione sull'area pubblica del Portale nazionale FSE*". La normativa impone, dunque, la necessità di fornire agli assistiti un modello di informativa, previamente predisposto dal Ministero, che sia uniforme per tutto il territorio nazionale.

Da ultimo, l'art. 8 del Decreto specifica che la consultazione dei dati e dei documenti del FSE da parte di soggetti diversi dell'interessato, per le finalità di diagnosi, cura e riabilitazione, prevenzione e profilassi internazionale può avvenire solo dopo che l'assistito ha espresso il proprio consenso, a seguito della presa visione dell'informativa privacy.

È, dunque, dal panorama normativo qui richiamato che il Garante desume le violazioni delle 18 Regioni e delle Province autonome del Trentino Alto Adige. Le condotte poste in essere dalle Regioni e dalle Province interessate determinano, infatti – secondo l'Autorità - una "*disomogeneità*" nel trattamento degli assistiti, che contraddice lo spirito

ISSN 2239-8570

della riforma del FSE 2.0 volta ad introdurre, invece, "*misure, garanzie e responsabilità omogenee sul territorio nazionale"*. Un tale atteggiamento, sottolinea il Garante, rischia "*di compromettere anche le funzionalità, l'interoperabilità e l'efficienza del sistema FSE 2.0*.".

Il Garante, sottolinea infine che le infrazioni delle Regioni e delle Province autonome – pur differendo per livello di gravità e responsabilità – possono comunque comportare l'applicazione delle sanzioni contenute nel GDPR.

ELISA GROSSI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10029439#1

2024/4(47)RMa-RoM

47. Il provvedimento del Garante privacy del 13.11.2024 contro Foodinho per trattamento illecito dei dati personali dei ciclofattorini (rider) ai sensi del GDPR per violazioni relative alla gestione automatizzata dei lavoratori

Con provvedimento del 13 novembre 2024, il Garante per la protezione dei dati personali (il **Garante Privacy**) ha inflitto una nuova pesante sanzione di 5 milioni di euro a Foodinho S.r.l., società del gruppo Glovo, per gravi violazioni del Regolamento europeo sulla privacy (GDPR).

Il provvedimento fa seguito al precedente provvedimento del Garante privacy del 10 giugno 2021 adottato nei confronti della Società che all'epoca era stata condannata a modificare il trattamento dei dati dei propri *rider* e verificare che gli algoritmi di prenotazione e assegnazione degli ordini di cibo e prodotti non producessero forme di discriminazione portando alla limitazione delle consegne assegnate a ciascun *rider* o all'esclusione stessa dalla piattaforma.

In quell'occasione, il Garante Privacy aveva prescritto alla Società di individuare misure per tutelare i diritti e le libertà dei *rider* a fronte di decisioni automatizzate infliggendo altresì una sanzione di 2,6 milioni di euro per i trattamenti illeciti effettuati.

A distanza di pochi anni, la Foodinho S.r.l. è stata nuovamente sanzionata dal Garante a seguito di una complessa istruttoria che ha messo in luce un trattamento illecito dei dati personali di oltre 35.000 *rider* attraverso la piattaforma digitale utilizzata per la gestione delle consegne.

L'attività ispettiva era stata avviata d'ufficio a seguito della pubblicazione di notizie giornalistiche relative all'avvenuta disattivazione dell'account di un *rider* deceduto in un incidente stradale due giorni prima durante l'effettuazione di una consegna per conto della stessa Società.

Numerose sono state le violazioni rilevate, legate alla gestione automatizzata dei dipendenti.

ISSN 2239-8570

Tra le tante irregolarità riscontrate emerge, in primo luogo, l'invio automatico da parte della piattaforma utilizzata dalla Società di un unico messaggio standard in caso di disattivazione o blocco dell'account che, tuttavia, non informa il lavoratore della possibilità di contestare la decisione e chiedere il ripristino dell'account.

Problematico è altresì il sistema automatizzato utilizzato per la gestione dei turni e delle consegne, in particolare il cosiddetto "sistema di eccellenza", che assegna punteggi ai *rider*, determinando chi ha priorità nell'accesso ai turni di lavoro, così come il processo automatizzato che decide la distribuzione degli ordini all'interno del turno. Entrambi i sistemi sono stati implementati senza rispettare le garanzie previste dal GDPR, in particolare l'obbligo di garantire ai lavoratori il diritto di ricevere una revisione umana delle decisioni prese dai sistemi, di contestare le scelte e di esprimere la propria opinione.

Un'altra criticità rilevata è quella relativa all'uso della geolocalizzazione. La Società, infatti, inviava a terzi i dati personali dei *rider*, compresa la posizione geografica, senza che questi fossero adeguatamente informati.

Ancor più grave è stata ritenuto il fatto che la violazione abbia riguardato non solo il periodo lavorativo, ma anche quello extra-lavorativo, ovvero quando il rider non lavorava, quando l'app era in background e, fino ad agosto 2023, anche quando l'app non era attiva.

Inoltre, il Garante Privacy ha riscontrato altresì la violazione dell'art. 1-bis del D. Lgs. 152/1997 introdotto dal D. Lgs. 104/2022, c.d. "decreto trasparenza", sugli obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati, nonché la violazione dei principi di minimizzazione del trattamento, di cui all'art. 5(1)(c) del GDPR, e di privacy by design di cui all'art. 25(1) del GDPR e la mancata effettuazione della valutazione di impatto dei trattamenti.

Relativamente alla prima violazione, il Garante Privacy ha richiamato il suo documento intitolato "Prime indicazioni sul d. lgs. 27 giugno 2022, n. 104, c.d. decreto trasparenza" (doc. web n. 9844960), dove si chiarisce che i nuovi obblighi informativi introdotti dall'art. 4, d. lgs.27/6/2022, n. 104 costituiscono una disciplina più specifica e di maggior tutela, per gli interessati, nel contesto lavorativo, ai sensi di quanto stabilito dall'art. 88 del GDPR, a mente del quale gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro.

Alla luce delle molteplici violazioni riscontrate, il Garante Privacy – oltre a comminare la sanzione amministrativa di euro 5 milioni – ha imposto alla Società di riformulare i messaggi inviati ai *rider* in caso di disattivazione o blocco dell'account.

Particolarmente interessante è la parte del provvedimento del Garante Privacy adottato in conformità con quanto stabilito dalla recente direttiva (UE) 2024/2831 del 23 ottobre 2024 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, pubblicata nella Gazzetta Ufficiale dell'Unione europea dell'11.11.2024

ISSN 2239-8570

(sull'approvazione del cui testo v. in questa Rubrica la notizia n. 8 nel numero 2/2024 [2024/2(8)RiM]).

Ai sensi dell'art. 24 di questa direttiva, non ancora attuata in Italia, le autorità di controllo incaricate di controllare l'applicazione del GDPR sono altresì responsabili del controllo e del rispetto dell'applicazione degli articoli da 7 a 11 della medesima direttiva "per quanto concerne le questioni relative alla protezione dei dati, conformemente alle pertinenti disposizioni dei capi VI, VII e VIII del [GDPR]".

Gli articoli da 7 a 11 della direttiva (UE) 2024/2831, prevedono, rispettivamente, una serie di divieti e limitazioni del trattamento dei dati personali mediante sistemi di monitoraggio automatizzati o di sistemi decisionali automatizzati (art. 7), un obbligo di valutazione di impatto ai sensi dell'art. 35(1) GDPR (art. 8), obblighi di trasparenza dei sistemi di monitoraggio automatizzati e dei sistemi decisionali automatizzati (art. 9), obblighi di supervisione umana dei sistemi di monitoraggio automatizzati e dei sistemi decisionali automatizzati, nonché una serie di previsioni sul diritto di spiegazione e sul riesame umano (art. 10).

Orbene, nel suo provvedimento qui in commento, il Garante Privacy ha ordinato alla Società di individuare misure appropriate per garantire il diritto dell'interessato "*di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, in relazione ai trattamenti automatizzati compresa la profilazione effettuati mediante la piattaforma, garantendo un'adeguata formazione degli operatori addetti nonché la possibilità per gli operatori stessi di ignorare, se del caso, l'output del processo algoritmico, per evitare la possibile tendenza a farvi automaticamente affidamento*".

La Società dovrà inoltre disattivare la geolocalizzazione quando l'app è in background e garantire che i *rider* siano informati in tempo reale dell'attivazione del GPS sui loro dispositivi, attraverso un'icona che segnalerà quando la geolocalizzazione è in funzione.

Il Garante ha infine nuovamente prescritto a Foodinho di individuare misure appropriate volte ad introdurre strumenti per evitare usi impropri e discriminatori dei meccanismi reputazionali basati su *feedback*.

RICCARDO MARAGA/ROBERTA MARCIANO

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10074601

2024/4(48)FG

48. Il provvedimento del Garante Privacy del 27.11.2024 nei confronti di GEDI per l'accordo con Open AI

Il provvedimento n. 741 del 27 novembre 2024 del Garante per la protezione dei dati personali (**Garante** o **Autorità**) si inserisce in un contesto di crescente attenzione sulle modalità di trattamento dei dati

ISSN 2239-8570

personali nell'era dell'intelligenza artificiale. In questo caso, l'Autorità ha rivolto un avvertimento formale al Gruppo Editoriale GEDI, in relazione all'accordo triennale a titolo oneroso firmato con OpenAI OpCo LLC con sede in USA (**OpenAI**) il 24 settembre 2024, che prevede la comunicazione dei dati contenuti negli archivi digitali delle testate giornalistiche a OpenAI, con l'obiettivo di consentire a quest'ultima di utilizzarli per addestrare i propri algoritmi di intelligenza artificiale. Il provvedimento è stato adottato dopo i primi riscontri forniti dalla società OpenAI, nell'ambito dell'istruttoria avviata dall'Autorità in data 26 settembre u.s. (su cui v. in questa Rubrica la notizia n. 9 del numero 3/2024 [2024/3(9)FG]). Il Garante ha sollevato numerosi dubbi sulla legittimità di tale trattamento, evidenziando il rischio che vengano violati i principi stabiliti dal regolamento (UE) 2016/679 (**GDPR** o il **Regolamento**), in particolare per quanto riguarda il trattamento di dati personali di milioni di persone, tra cui informazioni sensibili. L'archivio di un giornale contiene infatti una quantità enorme di dati che spaziano dalle informazioni generali agli aspetti più privati della vita degli individui. In questo scenario, il Garante ha sottolineato che tali dati non possono essere ceduti a terzi per finalità di addestramento dell'intelligenza artificiale senza rispettare adeguate cautele previste dalla normativa. L'Autorità ha rilevato che la valutazione d'impatto sulla protezione dei dati (**DPIA**) che GEDI ha presentato non analizza in modo sufficiente la base giuridica sulla quale si fonda l'operazione. In altre parole, non è chiaro su quale base legale l'editore potrebbe cedere o licenziare l'uso dei dati personali a OpenAI, dato che il trattamento di dati sensibili per addestrare algoritmi non trova una giustificazione immediata nel GDPR. In particolare, l'articolo 9 del Regolamento prevede limitazioni molto severe sull'uso dei dati sensibili, come quelli riguardanti la salute o le convinzioni religiose, che potrebbero essere contenuti negli archivi giornalistici. Il Garante ha anche messo in luce come non siano stati adeguatamente rispettati gli obblighi di trasparenza e informativa nei confronti degli utenti. Infatti, non sono stati aggiornati in maniera opportuna gli avvisi e le informative privacy delle testate coinvolte nell'accordo, come La Repubblica e La Stampa, per informare gli utenti che i loro dati potrebbero essere condivisi con OpenAI. Le informazioni fornite agli utenti non sembrano essere sufficienti, e non è stato chiarito in modo esaustivo come i dati vengano utilizzati o conservati. Questo porta a una violazione degli articoli 13 e 14 del GDPR, che obbligano le aziende a fornire informazioni chiare e trasparenti su come i dati vengono trattati, anche prima che avvenga il trattamento stesso. Oltre alla trasparenza, il Garante ha espresso preoccupazioni riguardo alla possibilità che gli utenti possano esercitare efficacemente i propri diritti, in particolare il diritto di opposizione previsto dall'articolo 21 del GDPR. Nonostante GEDI abbia dichiarato che gli utenti potrebbero opporsi al trattamento dei propri dati, il Garante ha messo in evidenza che tale opposizione sarebbe complicata da esercitare, in quanto gli utenti dovrebbero rivolgersi direttamente a OpenAI e non alle testate giornalistiche, che sono i soggetti con cui hanno un rapporto diretto. Questo impedirebbe una protezione adeguata dei diritti degli interessati e potrebbe costituire una violazione del diritto alla

ISSN 2239-8570

protezione dei dati personali. L'avvertimento del Garante sottolinea, quindi, come l'accordo tra GEDI e OpenAI, se non adeguatamente revisionato, comporti il rischio di un trattamento illecito dei dati personali, con possibili sanzioni a carico del Gruppo Editoriale. L'Autorità ha chiesto una revisione delle modalità di gestione dei dati, con particolare attenzione alla trasparenza, al rispetto dei diritti degli utenti e alla valutazione legittima della base giuridica per il trattamento. In sostanza, il Garante invita GEDI a garantire il rispetto dei principi fondamentali del GDPR per evitare conseguenze giuridiche e sanzionatorie. Un punto rilevante sottolineato dal Garante riguarda la difficoltà di applicare la base giuridica del legittimo interesse, che GEDI ha scelto come giustificazione per il trattamento dei dati. Questo approccio è stato ritenuto insufficiente, specialmente per quanto riguarda il trattamento di dati sensibili, come quelli legati alla salute o alle condanne penali, che non possono essere trattati esclusivamente sulla base di un interesse legittimo. Il Garante ha messo in evidenza che la DPIA non analizza sufficientemente come GEDI possa legittimamente cedere i dati a OpenAI, dato che l'attività di addestramento dell'intelligenza artificiale è sottratta al controllo diretto di GEDI e delle sue testate. Un altro tema fondamentale riguarda il diritto all'oblio. La diffusione indiscriminata dei dati contenuti negli archivi giornalistici, senza adeguate cautele, potrebbe compromettere l'esercizio di questo diritto, già tutelato tramite deindicizzazione dei contenuti dai motori di ricerca. Il trattamento dei dati da parte di OpenAI potrebbe vanificare gli sforzi di deindicizzazione e limitare la possibilità per gli interessati di far valere il proprio diritto a rimanere nell'anonimato. Il Garante ha espresso preoccupazione per come questo tipo di trattamento possa interferire con la protezione del diritto all'oblio, specialmente in relazione ai dati che non dovrebbero essere ripubblicati o utilizzati per scopi ulteriori. Il Garante, nel suo provvedimento, ha pertanto avvertito GEDI Gruppo Editoriale S.p.A. e le altre società del gruppo coinvolte nell'accordo con OpenAI, ovvero GEDI News Network S.p.A., GEDI Periodici e Servizi S.p.A., GEDI Digital S.r.l., Monet S.r.l., e Alfemminile S.r.l., che potrebbero trovarsi in una posizione di violazione del GDPR.

FRANCESCO GROSSI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10077129

2024/4(49)FDA

49. La sentenza del Tribunale di Torino, Sezione Lavoro del 20.9.2024, n. 2287 sul risarcimento del danno derivante dall'uso di algoritmi per la distribuzione delle supplenze nelle scuole superiori

ISSN 2239-8570

Con la sentenza n. 2287 del 20 settembre 2024 la Sezione Lavoro del Tribunale ordinario di Torino ha condannato il Ministero dell'istruzione e del merito (**MIM**) a risarcire una docente penalizzata dal difettoso funzionamento di un algoritmo utilizzato nelle procedure volontarie per distribuire le supplenze nelle scuole secondarie superiori.

Nel caso di specie l'algoritmo ministeriale avrebbe dovuto assegnare a ciascun docente il miglior incarico didattico sulla base del profilo professionale e della conseguente collocazione nella graduatoria di merito; ma, per un difetto tecnico, ha ingiustamente attribuito alla ricorrente un punteggio più basso rispetto ad altri colleghi meno titolati.

Nel dettaglio, i fatti di causa risalgono all'anno scolastico 2021/2022 quando la ricorrente aveva presentato domanda di inserimento nelle graduatorie provinciali per le supplenze (**GPS**), chiedendo espressamente che le fosse assegnato un orario didattico "*intero*" ai sensi dell'art. 12, co. 10 dell'ordinanza ministeriale n. 60 del 10 luglio 2020 (in base al quale "*l'aspirante cui è conferita una supplenza a orario non intero in caso di assenza di posti interi, conserva titolo, in relazione alle utili posizioni occupate nelle diverse graduatorie di supplenza, a conseguire il completamento d'orario, esclusivamente nell'ambito della provincia di inserimento, fino al raggiungimento dell'orario obbligatorio di insegnamento previsto per il corrispondente personale di ruolo, tramite altre sup-plenze correlate ai posti di cui all'articolo 2 a orario non intero*").

L'algoritmo chiamato a gestire la procedura – per un problema tecnico intrinseco – le aveva invece assegnato una docenza a tempo ridotto, retrocedendola in seconda fascia nella graduatoria finale.

Accortasi dell'errore, la ricorrente aveva subito chiesto al MIM di rettificare la graduatoria stilata dall'algoritmo senza ottenere alcuna risposta; e nel frattempo aveva stipulato con un istituto scolastico locale un contratto annuale di supplenza "*non intero*" per nove ore settimanali poi integrato con un successivo incarico di sei ore.

Accogliendo il ricorso depositato nel 2023, il Tribunale di Torino ha dichiarato che l'algoritmo ministeriale ha leso la docente e l'ha privata del diritto di completare l'orario lavorativo; in particolare ha rilevato che la ricorrente, dopo la prima assegnazione di nove ore di supplenza, avrebbe potuto stipulare non uno ma "*diversi contratti di completamento orario*" che sono stati invece "*assegnati a docenti con punteggio più basso*" (p. 5).

Per queste ragioni ha condannato l'amministrazione a corrispondere alla docente una somma di denaro per le retribuzioni non percepite a causa del malfunzionamento del sistema algoritmico; e un ulteriore importo per il mancato riconoscimento dei benefici economici previsti dalla legge per l'aggiornamento e la formazione del personale docente nelle scuole superiori.

FILIPPO D'ANGELO

https://shorturl.at/FYpBO

ISSN 2239-8570

2024/4(50)FS

50. La sentenza del Tribunale di Amburgo del 27.9.2024 nel caso Kneschke/LAION: la prima decisione europea sull'utilizzo di opere protette dal diritto d'autore per l'addestramento di sistemi di intelligenza artificiale

Il 27 settembre 2024 il Tribunale di Amburgo ha pronunciato la prima decisione europea sul tema della riproduzione di opere dell'ingegno pubblicate su internet (nel caso di specie, una fotografia) per la creazione di dataset da utilizzare per l'addestramento di sistemi di intelligenza artificiale. La corte tedesca, escludendo nella fattispecie l'applicabilità dell'eccezione c.d. di *text and data mining* ai sensi (della norma tedesca di attuazione) **dell'art. 4** della direttiva (UE) 2019/790 sulla protezione del copyright nel mercato unico digitale (**Direttiva DSM**), e rinvenendo gli estremi per l'eccezione di estrazione di testo e di dati **per scopi di ricerca scientifica ai sensi** (della disposizione di diritto tedesco in attuazione) **dell'art. 3 della medesima direttiva**, ha offerto un'interessante interpretazione dei concetti sottostanti nel contesto dell'attuale scenario tecnologico e normativo.

I fatti sottoposti al giudizio del Tribunale di Amburgo, e il relativo oggetto del contendere, ruotavano intorno alla **contestazione di una riproduzione non autorizzata** di una fotografia dell'autore Robert Kneschke per la creazione di un set di dati finalizzato all'addestramento di sistemi di IA. La fotografia era stata pubblicata su internet, con il consenso dell'autore, come parte dello stock di una agenzia fotografica che ne concedeva in licenza i diritti al pubblico a titolo oneroso. La pubblicazione della fotografia, inoltre, era corredata da una dichiarazione di riserva che **vietava espressamente la riproduzione automatizzata del database mediante tecniche di web scraping**. Ciò nondimeno, la fotografia era stata riprodotta dalla convenuta (la no-profit tedesca **LAION**) nell'ambito del processo di creazione del proprio data set, consistente in oltre 6 miliardi di immagini. In realtà, **il data set controverso non conteneva di per sé riproduzioni di immagini protette dal diritto d'autore**, piuttosto i dati di correlazione tra ciascuna immagine e l'URL che consentiva l'identificazione della risorsa sul web, correlazione che per essere "estratta" aveva richiesto il download di ciascuna immagine. La condotta scrutinata dal Tribunale, quindi, afferisce ad una fase preliminare dello sviluppo di sistemi di IA, quella relativa alla raccolta e selezione dei dati funzionali al *training* del sistema, restando per contro irrilevanti le riproduzioni effettuate a livello di elaborazione tutta interna al modello (c.d. *black box*) come pure a livello di output.

La riproduzione temporanea (art. 5, par. 1, Direttiva Infosoc).

Il Tribunale ha anzitutto escluso che la riproduzione in commento potesse considerarsi esentata ai sensi della disposizione del diritto tedesco in attuazione dell'art. 5(1) della direttiva 2001/29/CE (**Direttiva Infosoc**), norma che sottrae all'esclusiva dell'autore gli atti di riproduzione che cumulativamente: (i) siano temporanei; (ii) siano transitori o accessori; (iii)

ISSN 2239-8570

costituiscano parte integrante ed essenziale di un procedimento tecnologico; (iv) siano eseguiti all'unico scopo di consentire la trasmissione in rete tra terzi con l'intervento di un intermediario o un utilizzo legittimo di un'opera o altri materiali protetti; (v) siano privi di un rilievo economico proprio.

Nella fattispecie, la corte ha escluso tanto il requisito della temporaneità quanto l'elemento dell'indispensabile correlazione al procedimento di analisi dei dati; il primo, sulla base della considerazione che le riproduzioni contestate non erano destinate *ab origine* ad automatica cancellazione dopo un certo lasso di tempo; il secondo, sulla base dell'osservazione che il download delle immagini non costituiva parte integrante ed essenziale del procedimento di analisi dei dati sottostanti, bensì era stato effettuato a monte in modo mirato e successivamente sottoposto ad uno specifico software di analisi.

In secondo luogo, la corte si soffermava sulla **dichiarazione di riserva dell'agenzia fotografica e sul suo valore ai sensi dell'art. 4(3) Direttiva DSM.**

In particolare, relativamente alla dichiarazione di *opt-out* contenuta sul sito web dell'agenzia fotografica da cui LAION aveva scaricato la fotografia controversa, il Tribunale di Amburgo ha enunciato i seguenti principi:

- La dichiarazione di riserva che consente di escludere l'eccezione di *text and data mining*, si applica a pieno titolo all'estrazione di testo e dati finalizzata alla creazione di data set destinati all'addestramento di sistemi di IA, come espressamente previsto dall'art. 53(1)(c) del regolamento UE 1689/2024 sull'intelligenza artificiale (**AI Act**).
- La dichiarazione di riserva può essere effettuata direttamente dall'autore ovvero dai suoi successori o aventi causa, sì che nel caso di specie il titolare dei diritti poteva legittimamente avvalersi della dichiarazione di riserva espressa dall'agenzia fotografica. Essa, inoltre, deve essere effettuata in maniera espressa ed univoca, ma senza necessità di specifici riferimenti normativi all'eccezione di *text and data mining*.
- La dichiarazione di riserva deve considerarsi espressa in modo appropriato, secondo quanto prescritto dall'art. 4(3) della Direttiva DSM, anche se formulata in linguaggio direttamente comprensibile all'uomo (quindi, non in "linguaggio macchina"). In questo senso, l'art. 53(1)(c) AI Act, nell'imporre ai fornitori di modelli IA per finalità generali l'adozione di "*tecnologie all'avanguardia*" onde riconoscere una dichiarazione di riserva, prende in considerazione proprio il caso in cui *l'opt-out* sia espresso in linguaggio "naturale". Sarebbe, inoltre, contraddittorio consentire ai fornitori di modelli di IA di sviluppare modelli sempre più potenti per la comprensione e la creazione di testi, da un lato, e allo stesso tempo non richiedere loro di utilizzare i modelli di IA esistenti - ed in grado (già dal 2021, periodo dei fatti di causa) di rilevare dichiarazioni espresse in linguaggio naturale - per rispettare le limitazioni imposte dalla Direttiva DSM, dall'altro.
- Il fatto che la direttiva (UE) 1024/2019 sul riutilizzo dei dati

ISSN 2239-8570

del settore pubblico (**direttiva Open Data**) preveda al considerando 35 requisiti più stringenti per la "leggibilità a macchina" di un documento liberamente accessibile sul web, non rileva nel caso concreto, in quanto tale direttiva persegue obiettivi diversi dalla Direttiva DSM sulla protezione del copyright nel mercato unico digitale.

L'eccezione di estrazione di testo e dati per scopi di ricerca scientifica (art. 3 Direttiva UE 2019/790).

Esclusa l'operatività dell'eccezione di *text and data mining* **ai sensi della disposizione di diritto tedesco corrispondente all'art. 4 della Direttiva DSM** (§44b della legge tedesca sul diritto di autore e i diritti connessi - *Urhberrechtsgesetz* **UrhG** – riguardante il TDM per fini non scientifici), il Tribunale di Amburgo ha nondimeno ritenuto che nella fattispecie LAION potesse qualificarsi come organismo di ricerca ai sensi della Direttiva DSM e che la riproduzione contestata potesse beneficiare dell'eccezione prevista dalla **disposizione di diritto tedesco corrispondente all'art. 3 della Direttiva DSM** (§60d UrhG: TDM per fini scientifici) che esenta le riproduzioni effettuate da organismi di ricerca e da istituti di tutela del patrimonio culturale (come definiti dall'UrhG in attuazione della medesima direttiva DSM) ai fini dell'estrazione, **per scopi di ricerca scientifica**, di testo e di dati da opere o altri materiali cui essi hanno legalmente accesso.

Tale conclusione è stata motivata sulla scorta delle seguenti considerazioni:

- **La creazione di un data set, che può costituire la base per l'addestramento di sistemi di IA, può essere considerata una ricerca scientifica**: sebbene la creazione dell'insieme di dati in sé non comporti un'immediata acquisizione di conoscenza, si tratta comunque di una fase di lavoro fondamentale con l'obiettivo di utilizzare l'insieme di dati per acquisire conoscenze in un momento successivo.
- Nel caso concreto, depone in tal senso il fatto che il dataset fosse stato pubblicato gratuitamente e messo a disposizione dei ricercatori nel campo delle reti neurali artificiali, mentre è irrilevante il fatto che il medesimo set di dati venisse utilizzato anche da aziende commerciali per l'addestramento o lo sviluppo dei loro sistemi di intelligenza artificiale, poiché anche la ricerca condotta da aziende commerciali rientra nel concetto di ricerca scientifica.
- Il semplice fatto che singoli membri dell'organismo di ricerca svolgano anche attività remunerate per società commerciali che forniscono sistemi di IA, oltre al loro impegno per l'organismo di ricerca, non è sufficiente per attribuire all'ente no-profit le attività di queste società.

In **conclusione**, la sentenza del Tribunale di Amburgo sembra destinata ad avere un impatto significativo in tutti gli Stati membri relativamente alla corretta interpretazione dell'eccezione di *text and data mining*, fornendo indicazioni di notevole importanza pratica in merito alla nozione di riproduzione di opere protette, alla creazione di data set di addestramento di sistemi di IA e all'applicazione delle relative eccezioni. Essa, inoltre,

ISSN 2239-8570

sembra avvantaggiare le società specializzate nella raccolta di dati di addestramento, nella misura in cui ha ritenuto che anche la fase c.d. di *pre-training* del modello possa beneficiare dell'eccezione di *text and data mining*, purché vengano rispettate le dichiarazioni di riserva dei titolari dei diritti.

Specularmente, l'aver equiparato la creazione di un dataset per finalità di addestramento ad un'attività di ricerca scientifica rilevante ai fini dell'eccezione prevista dall'art. 3 della Direttiva DSM, sembra **indebolire la posizione dei titolari dei diritti**, i quali, seguendo questa interpretazione, non possono opporsi alla riproduzione delle loro opere laddove effettuata da enti no-profit per finalità di *pre-training* (raccolta, selezione e filtraggio dei dati di addestramento) di modelli di IA, e sempre che, naturalmente, tali enti soddisfino anche i requisiti per qualificarsi come "organismi di ricerca" ai sensi della normativa nazionale di attuazione della relativa definizione di cui all'art. 2, n. 1) della Direttiva DSM:

"*un'università, comprese le relative biblioteche, un istituto di ricerca o qualsiasi altra entità il cui obiettivo primario sia condurre attività di ricerca scientifica oppure condurre attività didattiche che includano altresì attività di ricerca scientifica:*

a) senza scopo di lucro o reinvestendo tutti gli utili nella propria attività di ricerca scientifica, o

b) con una finalità di interesse pubblico riconosciuta da uno Stato membro,

in modo che non sia possibile l'accesso su base preferenziale ai risultati generati da detta ricerca scientifica da parte di un'impresa che esercita un'influenza determinante su tale organismo".

FRANCESCO SANTONASTASO

https://pdfupload.io/docs/4bcc432c

2024/4(51)FG

51. Il ricorso del 26.9.2024 contro la decisione dell'U.S. Copyright Office di negare la protezione del copyright all'opera *Théâtre d'Opéra Spatial* generata con l'uso del sistema di IA Midjourney

L'artista Jason Allen, conosciuto per la sua creazione *Théâtre d'Opéra Spatial*, il 26 settembre 2024 ha presentato ricorso presso la Corte distrettuale del Colorado (causa n. 1:24-cv-02665), intentando un'azione legale nei confronti dell'U.S. Copyright Office (**USCO**) e della sua direttrice, Shira Perlmutter, poichè l'Ufficio statunitense per il diritto d'autore ha negato la protezione del copyright della sua opera, in quanto generata con sistemi di intelligenza artificiale. Il Sig. Allen ha chiesto la protezione legale per la sua opera *Théâtre D'Opéra Spatial*, perché sebbene l'opera sia stata parzialmente generata utilizzando il sistema di intelligenza artificiale (Midjourney), l'autore sostiene che si tratta di un prodotto del suo

ISSN 2239-8570

processo creativo e non di un semplice algoritmo che agisce in modo indipendente.

Nel settembre 2022 il signor Allen ha presentato all'USCO una prima domanda di registrazione per ottenere la protezione del copyright della sua opera *Théâtre d'Opéra Spatial* senza dichiarare che fosse stata realizzata utilizzando il sistema di intelligenza artificiale Midjourney. L'USCO era a conoscenza del lavoro fatto con il coinvolgimento di sistemi di intelligenza artificiale e ciò a causa dell'interesse a livello nazionale che si è creato intorno all'opera che ad agosto 2022 **ha ricevuto il primo premio** nella categoria Digital Arts/ Digitally Manipulated Photography alla Colorado State Fair. Per la prima volta, quindi, un concorso artistico ha premiato una creazione dell'intelligenza artificiale, anche se Allen sostiene di essere stato coinvolto nel processo creativo e che non tutto è stato generato dall'AI.

Prima di prendere una decisione, l'Ufficio ha richiesto all'artista ulteriori informazioni sul processo creativo dell'opera esprimendo le sue preoccupazioni sul fatto che l'opera d'arte generata tramite Midjourney fosse in grado di soddisfare il requisito della paternità umana dell'opera [così come previsto da copiosa casistica (ex multis Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 58 (1884); Naruto v. Slater, 888 F.3d 418, 426 (9th Cir. 2018)) e dalle linee guida dello stesso Ufficio *Compendium of U.S. Copyright Office Practices § 306* (3d ed. 2021)].

Allen ha risposto sostenendo che, nonostante l'uso del servizio di generazione di immagini di Midjourney come parte del processo creativo, ogni singolo elemento dell'opera è stato realizzato grazie al suo contributo e riflette la sua paternità.

Il processo creativo di Allen è consistito nell'inserire numerose revisioni e richieste di testo per almeno 624 volte per arrivare alla versione iniziale dell'immagine. Inoltre, dopo aver prodotto la versione iniziale dell'Opera, Midjourney ha utilizzato Adobe Photoshop per rimuovere i difetti e creare nuovi contenuti visivi e ha utilizzato Gigapixel AI per "scalare" l'immagine, aumentandone la risoluzione e le dimensioni. A prescindere dalle considerazioni dell'artista, secondo l'USCO, sebbene Allen sostenesse di aver deciso direttamente il contenuto e la struttura dell'immagine, il processo descritto rende evidente che il sistema di IA non l'ha semplicemente assistito (al pari di software specializzati nell'elaborazione di opere appartenenti all'arte figurative, e.g. Adobe Photoshop) ma ha creato le immagini seguendo un processo che non è lo stesso di un artista, scrittore o fotografo umano; pertanto, le immagini generate da Midjourney non sono frutto di una creazione umana.

A seguito dei chiarimenti intercorsi, nel dicembre 2022 l'Ufficio ha rifiutato di registrare la rivendicazione perché il deposito dell'opera non "fissava solo la presunta paternità del [signor Allen]", ma comprendeva invece "contributi inestricabilmente fusi e inseparabili" sia del signor Allen che di Midjourney. Nel gennaio 2023 il sig. Allen ha presentato una seconda richiesta all'USCO al fine di riconsiderare il suo iniziale rifiuto di registrare l'opera, sostenendo sia che l'esaminatore aveva applicato erroneamente il requisito della paternità umana, in quanto il suo "input creativo" in Midjourney, comprendeva "l'inserimento di una serie di prompt,

ISSN 2239-8570

la regolazione della scena, la selezione di porzioni da mettere a fuoco e l'imposizione del tono dell'immagine", e tutto ciò "alla pari di quello espresso da altri tipi di artisti e quindi tutelato dal diritto d'autore" sia che la dottrina del fair use "consentirebbe la registrazione dell'opera" perché "consente usi trasformativi di materiale protetto da copyright". Dopo aver rivalutato le rivendicazioni del sig. Allen, nel settembre 2023 l'USCO Review Board (responsabile dell'esame dei ricorsi amministrativi presentati da un richiedente, in caso di doppio rifiuto di registrazione dell'opera dell'Ufficio) ha negato la registrazione del copyright poiché l'opera non ha la paternità umana necessaria per supportare una richiesta di copyright e, più in dettaglio, "*contiene più di una* quantità minima *di contenuti generati dall'intelligenza artificiale, che devono essere esclusi in una domanda di registrazione*".

Con il provvedimento di rigetto della registrazione del copyright dell'opera di Allen, l'U.S. Copyright Office ha confermato la sua precedente posizione su analoghe domande di registrazione, come:

- un'opera figurativa ('**A Recent Entrance to Paradise'**) creata interamente con un sistema di intelligenza artificiale generativa. La domanda di registrazione era stata depositata presso l'USCO dal dr. Stephen Thaler, proprietario del software e il Review Board si è pronunciato in senso negativo in data 14 febbraio 2022 (v. in questa Rubrica notizia n. 17 nel numero 3/2023 [2023/3(17)FG] e in *Atlante*, p. 406);

- una graphic novel ('**Zarya of the Dawn'**) che contiene oltre a elementi testuali dell'autrice, anche opere generate da Midjourney. L'USCO in data 21 febbraio 2023 ha confermato il precedente approccio, negando la registrazione (v. in questa Rubrica notizia n. 18 nel numero 1/2023 [2023/1(18)FG] e in *Atlante*, p. 329).

Nella sua decisione, l'USCO precisa che "i tribunali hanno interpretato l'espressione "opere d'autore" in modo da richiedere la creazione umana dell'opera" ed ha fatto riferimento alla sentenza del Tribunale distrettuale degli Stati Uniti per il distretto delle Columbia nella causa Thaler v. Perlmutter, No. 22-cv-384-1564, (Data della sentenza 18 agosto 2023), sostenendo che "la paternità umana è un requisito fondamentale del diritto d'autore" nell'affermare il rifiuto dell'Ufficio di registrare un'opera "autonomamente" creata dall'IA. Per questo motivo, i tribunali hanno uniformemente respinto i tentativi di proteggere le creazioni di persone non umane attraverso il diritto d'autore.

Vale la pena notare che le linee guida dello stesso Ufficio *Compendium of U.S. Copyright Office Practices § 306* (3d ed. 2021), affermano esplicitamente che solo le opere create dall'uomo sono registrabili. Midjourney produce immagini in modo imprevedibile, pertanto gli utenti del software non sono gli autori delle immagini generate dalla tecnologia. Come ha spiegato la Corte Suprema degli Stati Uniti d'America, nel caso Burrow-Giles Lithographic Co. v. Sarony, l'autore di un'opera tutelata dal copyright è la persona che ha effettivamente realizzato l'immagine, la "mente inventiva" dietro l'opera stessa.

Secondo l'Ufficio, è ormai assodato che il diritto d'autore può proteggere solo il materiale che è il prodotto della creatività umana. Il termine "autore",

ISSN 2239-8570

utilizzato sia dalla Costituzione Americana sia dalla normativa sul Copyright, esclude autori non umani.

I regolamenti per la registrazione delle opere pubblicati dell'USCO riflettono le indicazioni della legge e della giurisprudenza in materia. Ai sensi delle Linee Guida, l'Ufficio valuterà ai fini della registrazione, caso per caso, se i contributi dei sistemi di IA sono il risultato di una "riproduzione meccanica" o invece di una "concezione mentale originale" dell'autore. La risposta dipenderà dalle circostanze, in particolare dal funzionamento dello strumento di IA e dal modo in cui è stato utilizzato per creare l'opera finale.

Secondo l'Ufficio, ad oggi, i sistemi di intelligenza artificiale generativa attualmente disponibili non consentono agli utenti di esercitare un controllo creativo sul modo in cui tali sistemi interpretano i suggerimenti e generano materiale. L'USCO equipara la situazione attuale a quella in cui un cliente incarica un'artista di creare un'immagine dandogli indicazioni approssimative e generali sul risultato finale.

In tali casi, l'autore sarebbe l'artista che ha ricevuto le istruzioni e ha determinato in maniera del tutto autonoma il modo migliore per esprimerle. Il committente fornisce l'idea che non è tutelabile mentre è l'artista che la esprime in un oggetto tangibile.

L'Ufficio precisa come i richiedenti abbiano il dovere di rivelare l'inclusione di contenuti generati dai sistemi di IA in un'opera presentata per la registrazione e di fornire una breve spiegazione dei contributi dell'autore umano all'opera (a differenza di quanto avvenuto per la registrazione dell'opera *Théâtre d'Opéra Spatial* del sig. Allen).

A seguito del secondo diniego alla registrazione del copyright della sua opera, il sig. Allen in data 26 settembre 2024, ha presentato ricorso presso la Corte distrettuale federale del Colorado (causa n. 1:24-cv-2665), intentando un'azione legale contro l'USCO e la sua direttrice, Shira Perlmutter e chiedendo la protezione legale per la sua opera *Théâtre D'Opéra Spatial*, creata utilizzando lo strumento di intelligenza artificiale (AI) Midjourney. Sebbene l'opera d'arte sia stata parzialmente generata dall'IA, Allen (confermando la sua posizione tenuta presso l'USCO) sostiene che si tratti di un prodotto del suo processo creativo e non di un semplice algoritmo che agisce in modo indipendente.

La richiesta di risarcimento di Allen si basa su un'interpretazione articolata delle normative relative alla protezione del diritto d'autore, in particolare sulla decisione dell'USCO di respingere la sua domanda di registrazione per l'opera "Théâtre D'Opéra Spatial", creata con l'assistenza di un sistema di IA. Allen ritiene che il rifiuto dell'USCO violi l'APA (Legge sulla procedura amministrativa), che stabilisce che un'azione amministrativa possa essere invalidata se risulta arbitraria o capricciosa. Secondo Allen, la decisione dell'USCO non rispetta il quadro normativo che prevede la protezione delle opere creative, e il tribunale dovrebbe intervenire per invalidarla.

Inoltre, Allen sostiene che la sua opera soddisfi i requisiti fondamentali per la protezione del diritto d'autore secondo il **Copyright Act** (17 U.S.C. § 102(a)). La sua creazione è un'opera originale d'autore fissata su un supporto

ISSN 2239-8570

tangibile, e Allen ritiene che il suo intervento umano nel processo creativo sia sufficiente a soddisfare il criterio di "creatività minima" richiesto per il copyright. Nonostante l'opera sia stata realizzata con l'aiuto dell'IA, il suo ruolo nel processo di creazione è stato determinante, in quanto ha fornito istruzioni precise e dettagliate al sistema, che non ha agito autonomamente.

Uno dei punti principali del ricorso riguarda il requisito della "paternità umana", che l'USCO ha interpretato in modo troppo restrittivo. L'USCO ha respinto la domanda di Allen, sostenendo che non vi fosse stato un sufficiente coinvolgimento umano nella creazione dell'immagine generata dall'intelligenza artificiale. Allen, al contrario, afferma che l'immagine non è stata generata in modo autonomo dall'IA, ma seguendo le sue complesse e dettagliate istruzioni. Il suo contributo creativo, che ha incluso la selezione e la guida durante la generazione dell'immagine, è stato decisivo e non può essere ridotto a una mera supervisione.

Inoltre, Allen fa riferimento al caso storico di **Burrow-Giles Lithographic Co. v. Sarony (1884)**, che stabilisce che un'opera può essere protetta anche se creata con l'aiuto di macchine, a condizione che vi sia un significativo contributo umano, come la selezione, la direzione artistica e la disposizione degli elementi. Allen sostiene che, proprio come una macchina fotografica o un computer vengono utilizzati per creare arte, l'IA dovrebbe essere considerata uno strumento legittimo nel processo creativo, trattato alla stessa stregua di altri strumenti tecnologici. L'uso dell'IA non diminuisce l'originalità dell'opera, ma piuttosto la potenzia, in quanto Allen ha esercitato una direzione artistica sostanziale nell'intero processo.

Un altro aspetto del ricorso riguarda la critica di Allen all'USCO per non aver mantenuto una posizione "tecnologicamente neutra". Secondo lui, l'arte contemporanea sta già accettando l'uso dell'IA, mentre l'USCO sembra essere in ritardo nel riconoscere il valore creativo di queste tecnologie. Allen paragona la sua esperienza con quella di altri strumenti moderni utilizzati per la creazione artistica, come Photoshop o i sintetizzatori musicali, che hanno ottenuto la protezione del copyright senza che si sia mai messo in discussione l'intervento umano. Negare il copyright alle opere generate con l'IA, secondo Allen, frena l'innovazione artistica e non rispetta i principi fondamentali della legge sul diritto d'autore, che dovrebbero proteggere la creatività indipendentemente dal mezzo utilizzato.

Allen sottolinea anche che, nel suo caso, l'IA è stata solo uno strumento, utilizzato per eseguire le sue decisioni creative. Il processo di creazione dell'opera è stato iterativo: Allen ha generato 624 variazioni dell'immagine, modificando continuamente le istruzioni date all'IA per raggiungere la visione artistica desiderata. Questo processo di selezione e disposizione degli elementi, che ha incluso l'uso di software come Gigapixel AI e Adobe Photoshop per perfezionare l'immagine finale, dimostra un significativo intervento umano e dovrebbe essere riconosciuto come tale nella determinazione della "paternità" dell'opera.

Con il ricorso presentato, Allen mira a ottenere l'annullamento della decisione dell'USCO e chiede che la Corte distrettuale ordini all'Ufficio di registrare l'opera secondo il **Copyright Act**. La sua richiesta si concentra su una sentenza dichiarativa che stabilisca che l'opera *Théâtre D'Opéra Spatial*

ISSN 2239-8570

sia idonea alla protezione del diritto d'autore. La Corte distrettuale potrebbe seguire l'approccio tradizionale dell'USCO, che ha negato la protezione, oppure adottare una posizione più innovativa, simile a quella della **Corte distrettuale di Columbia in un caso del Dr. Thaler deciso nell'agosto 2023** ("*Stephen Thaler v. Shira Perlmutter*, *Register of Copyrights and Director of the United States Copyright Office, et al.*, Case Number Civil Action No. 22-1564 (BAH)"), dove è stato riconosciuto che le opere generate con l'assistenza dell'IA possano essere protette dal diritto d'autore se vi è un apporto umano significativo.

Il caso di Allen potrebbe avere importanti implicazioni legali per la giurisprudenza sul copyright, poiché potrebbe stabilire un precedente per il trattamento delle opere "assistite dall'IA". La Corte potrebbe decidere di seguire un orientamento più inclusivo, simile ad altri casi internazionali, come quello cinese di **Li Yunkai v. Liu Yuanchun** (su cui v. in questa Rubrica la notizia n. 32 del numero 4/2023 [2023/4(32)FG] e in *Atlante*, p. 499), che ha riconosciuto come protette le opere create tramite IA, a condizione che vi sia un contributo umano che rifletta l'originalità e l'apporto personale dell'autore umano.

In sintesi, il caso di Allen solleva questioni cruciali sulla protezione delle opere create con l'assistenza dell'intelligenza artificiale e sulla necessità di aggiornare le normative sul diritto d'autore per riflettere le innovazioni tecnologiche. La sentenza potrebbe segnare un'importante evoluzione nel riconoscimento delle opere digitali e IA come parte integrante del panorama artistico contemporaneo.

FRANCESCO GROSSI

https://fingfx.thomsonreuters.com/gfx/legaldocs/gdvzkrrmapw/AI%20COPYRIGHT%20REGISTRATION%20appeal.pdf

2024/4(52)GD

52. I rimedi comportamentali e strutturali proposti dal Dipartimento di Giustizia degli Stati Uniti ("Google must divest Chrome") e da Google a fronte della sentenza del 5.8.2024, con cui è stato dichiarato l'abuso di posizione dominante di Google nelle ricerche online e nella pubblicità degli annunci di testo

Con la storica sentenza del 5.8.2024 nella causa Stati Uniti d'America c. Google LLC, 2024 WL 3647498 (su cui v. in questa Rubrica notizia n. 12 del numero 3/2024 [2024/3(12)GD]), la Corte degli Stati Uniti d'America per il Distretto della Columbia – nella persona del giudice Amit P. Mehta – ha stabilito che Google LLC (**Google**) ha violato la Sezione 2 dello Sherman Act mediante l'utilizzo di accordi di distribuzione esclusiva volti a mantenere illegalmente il suo monopolio nel mercato dei servizi di ricerca online e della pubblicità degli annunci di testo.

ISSN 2239-8570

Con la sentenza si è aperta la seconda fase del processo, attinente alla definizione della sanzione da irrogare a Google.

Il giudice Mehta ha fissato le prossime udienze ad aprile 2025 ed intende adottare una decisone finale entro agosto 2025.

Durante questa seconda fase, le parti – i.e., il Dipartimento di Giustizia degli USA (Department of Justice, **DoJ**) e Google – hanno depositato le proprie proposte di sentenza definitiva (Proposed Final Judgment, **PFJ**) con i possibili rimedi comportamentali e strutturali da imporre a Google.

In particolare, il 20.11.2024 il DoJ – sotto l'amministrazione uscente dell'ex Presidente Biden – ha depositato la sua PFJ. Come riassunto in un documento di circa 23 pagine, il DoJ tra le altre cose, ha chiesto al giudice Mehta di imporre a Google la cessione a terzi del suo motore di ricerca Chrome, citando testualmente: "*Google must divest Chrome*".

Nello specifico, la proposta del DoJ prevede che, dopo la vendita di Chrome, Google non possa possedere un proprio browser, né rientrare nel mercato dei browser per almeno cinque anni, né possedere quote in motori di ricerca concorrenti, prodotti concorrenti basati sull'intelligenza artificiale (AI) o tecnologie pubblicitarie, in quanto ciò – secondo il DoJ – potrebbe compromettere l'efficacia del rimedio proposto.

Questa è una delle misure più dure proposte dal DoJ, che, se accolta, potrebbe influenzare drasticamente il futuro del mondo digitale. Si tratterebbe, infatti, di uno smantellamento storico per il quale bisognerebbe trovare uno valido acquirente, che non riproduca una situazione monopolistica simile a quella attuale. Com'è noto, Chrome rappresenta il browser più utilizzato al mondo, nonché un vantaggio chiave per Google. Infatti, Chrome permette a Google di raccogliere una considerevole mole di dati degli utenti e di promuovere in modo mirato anche i suoi prodotti (tra cui ad esempio Gemini, la piattaforma di intelligenza artificiale che ambisce a diventare un assistente personale universale). In altri termini, la cessione di Chrome colpirebbe duramente il modello di business di Google.

Inoltre, il DoJ ha proposto al giudice Mehta anche i seguenti rimedi:

- vietare a Google di stipulare accordi di esclusiva con terzi (tra cui, ad esempio, Apple e Samsung) per evitare che il motore di ricerca Chrome risulti l'impostazione predefinita su computer, tablet, smartphone e altri dispositivi elettronici;
- imporre a Google di condividere i risultati e i dati di ricerca con i propri concorrenti almeno per un decennio;
- imporre a Google la vendita di Android (*i.e.*, il suo sistema operativo per smartphone) oppure, in alternativa, vietare a Google di adottare misure che costringano le aziende ad abbinare i suoi servizi ai telefoni con sistema operativo Android;
- imporre a Google di cedere tutte le partecipazioni attualmente detenute in società attive nell'intelligenza artificiale, poiché l'intelligenza artificiale può rafforzare la posizione dominante di Google;
- imporre a Google maggiore trasparenza per gli inserzionisti;
- imporre a Google l'implementazione di un programma di sensibilizzazione per informare gli utenti sui cambiamenti

ISSN 2239-8570

intervenuti e aumentare la loro capacità di scegliere tra i fornitori di servizi di ricerca;

- nominare un Comitato tecnico per monitorare l'implementazione dei rimedi da parte di Google e garantire che quest'ultima non eluda la decisione finale del Tribunale.

La proposta del DoJ prevede che i suddetti rimedi rimangano in vigore per un periodo di 10 anni, con possibilità di revisione o modifica.

Il DoJ potrà depositare la versione definitiva della proposta dei rimedi entro il 7.3.2025 (ossia a seguito dell'insediamento dell'amministrazione del Presidente Trump, che potrebbe decidere di cambiare "rotta" rispetto all'amministrazione uscente).

Nel frattempo, il 20.12.2024 Google ha depositato in Tribunale la sua proposta, principalmente volta ad evitare la vendita del motore di ricerca Chrome, ritenendo che il DoJ sia andato ben oltre quanto disposto dal giudice Mehta nella sentenza di agosto 2024.

In particolare, in un documento di circa 12 pagine, Google ha proposto di rivedere gli accordi di esclusiva siglati con i produttori di dispositivi elettronici e con le *browser companies*, come Apple e Mozilla, garantendo loro maggiore flessibilità.

Secondo Google, le *browser companies*, come Apple e Mozilla, dovrebbero continuare a poter stipulare accordi con il motore di ricerca ritenuto migliore per i loro utenti. Ad esempio, per aziende come Mozilla, questi contratti generano entrate vitali. Mozilla ha anche pubblicato un post per sottolineare le conseguenze dannose per Firefox e altri browser alternativi a Chrome, qualora dovessero essere accettati i rimedi proposti dal DoJ).

La proposta di Google prevede la possibilità di cambiare il provider di ricerca predefinito almeno ogni 12 mesi, nonché la possibilità per i produttori di dispositivi elettronici di preinstallare diversi motori di ricerca e preinstallare le app Google senza dover necessariamente preinstallare anche Google Search, Chrome o Play Store.

Anche Google è chiamata a presentare la versione finale dei rimedi entro il 7.3.2025.

Google ha già annunciato di voler impugnare la decisione finale che verrà adottata dal giudice Mehta entro l'estate 2025; per cui è probabile che per conoscere l'esito di questa vicenda occorrerà attendere la pronuncia finale della Corte Suprema.

Ovviamente una sentenza a sfavore di Google potrebbe rappresentare un punto cruciale non solo per l'azienda, ma per l'intero settore tecnologico.

Ciò che accadrà dipenderà anche dalle decisioni della nuova amministrazione della Casa Bianca, anche in considerazione del suo potere di sostituire i membri del Dipartimento di Giustizia incaricati del caso.

Per il momento non resta che attendere il 7 marzo 2025 per scoprire se e in che modo le predette proposte del DoJ e di Google verranno modificate in vista delle successive udienze calendarizzate a partire dal mese di aprile 2025.

GIORGIA DIOTALLEVI

ISSN 2239-8570

https://storage.courtlistener.com/recap/gov.uscourts.dcd.223205/gov.uscourts.dcd.223205.1108.1_1.pdf

Microsoft Word - PFJ Cover Memo 11.20 FINAL (2)

2024/4(53)RRa

53. La legge dell'Australia che vieta ai minori di anni 16 l'utilizzo di utilizzo di alcune piattaforme di social media.

L'Australia ha approvato il 29 novembre 2024 l'*Online Safety Amendment (Social Media Minimum Age) Bill 2024*, mediante il quale, andando a sostituire il previgente l'*Online Safety Act 2021*, introduce un divieto di accedere a determinate piattaforme di social media per minori di età inferiore ai 16 anni.

La legge, pubblicata con numero 147 e con la data del 10 dicembre 2024, stabilisce un'età minima per la fruizione di determinati servizi di social media e un obbligo per i fornitori di piattaforme di social media per i quali è prevista tale restrizione, di agire diligentemente per evitare che i minori di età inferiore all'età minima abbiano un account sulla piattaforma.

Come riporta il sito ufficiale del *Parliament of Australia (www.aph.gov.au)*, il testo definitivo della legge è stato approvato con larga maggioranza e riflette una posizione quasi unanimemente condivisa dal potere politico.

Nei memorandum esplicativi allegati al testo di legge, il provvedimento viene descritto come giustificato dalla preoccupazione per il rischio di danni alla salute e al benessere, anche in termini di soddisfazione della vita, presentato dall'esposizione dei bambini più piccoli ai social media. Lo scopo della legge appare dunque disegnato in termini di sicurezza e di benessere dei minori più giovani e delle loro famiglie e di responsabilità delle aziende di social media.

Nello specifico, la normativa introduce un'età minima legale pari a 16 anni per detenere un account con determinate piattaforme di social media, ponendo a carico di queste ultime il rischio di una eventuale violazione del divieto. Si prevede, infatti, che debbano essere introdotte, entro un anno dall'entrata in vigore della legge, pratiche ragionevoli di *age-gating* e che, in caso di mancato rispetto dei limiti imposti saranno comminate sanzioni pecuniarie da applicarsi con il sistema australiano della penalty unit, nella misura di 30.000 penalty units (art. 63D *"Civil penalty for failing to take reasonable steps to prevent age-restricted users having accounts*").

Ad essere sanzionate in caso di violazione del limite di età sarebbero, dunque, solo le società che gestiscono i *network*, mentre rimarrebbero immuni i minorenni e i loro genitori.

Ai fini dell'applicazione della disciplina, l'art. 63C afferma che si intendono come "piattaforme di social media con limiti di età" tutte quelle che consistono in:

ISSN 2239-8570

"(a) un servizio elettronico che soddisfi le seguenti condizioni:

(i) l'unico scopo, o uno scopo significativo, del servizio è consentire l'interazione sociale online tra 2 o più utenti finali;

(ii) il servizio consente agli utenti finali di collegarsi o interagire con alcuni o tutti gli altri utenti finali;

(iii) il servizio consente agli utenti finali di pubblicare materiale sul servizio;

(iv) altre condizioni (se presenti) stabilite nelle norme legislative; o

b) un servizio elettronico specificato nelle norme legislative".

Al contempo, in veste di clausola di chiusura del sistema, è previsto che, attraverso un apposito iter, il Ministro competente possa includere all'interno della categoria anche altri fornitori di servizi elettronici, allorquando lo ritenga ragionevole e necessario a ridurre il pericolo di danno in capo ai soggetti tutelati.

A mero titolo esemplificativo, sono stati ritenuti destinatari del divieto alcuni tra i giganti della tecnologia, come **Instagram**, **Facebook** e **TikTok**. A contrario, il Governo ha specificato che la legge **non si applicherà alla messaggistica, ai giochi online e ai servizi utili all'istruzione e il supporto sanitario, come Google Classroom e YouTube**.

Il rispetto dell'obbligo di età minima comporterà una qualche forma di garanzia dell'età, che potrebbe richiedere la raccolta, l'uso e la divulgazione di ulteriori informazioni personali. In tali operazioni, tuttavia, al fine di tutelare la privacy degli utenti, è espressamente posto all'art. 63DB il **divieto di raccolta di materiale di identificazione rilasciato dal governo (es. carta di identità) o di utilizzo di servizi accreditati** (ai sensi del *Digital ID Act 2024*). Si dovrà, dunque, invece, provvedere allo sviluppo di sistemi di verifica alternativi.

Le piattaforme **non dovranno utilizzare le informazioni e i dati raccolti a fini di garanzia dell'età per nessun altro scopo**, a meno che l'interessato non abbia fornito il proprio consenso. Inoltre, una volta che le informazioni siano state utilizzate il raggiungimento dello scopo, le stesse devono essere cancellate dalla piattaforma (o da qualsiasi terza parte incaricata dalla piattaforma).

Anche per la violazione (si dice, grave e ripetuta) di tali ultime norme, sono previste sanzioni pecuniarie.

Seppure non siano mancati in questi ultimi anni nel panorama internazionale provvedimenti adottati a tutela dei minori - si può citare, per gli Stati Uniti d'America, il *Children's Online Privacy Protection Act* (**COPPA**) che impone ai minori di 13 anni di fornire il consenso dei genitori per la raccolta dei dati da parte delle aziende tecnologiche (v., in questa Rubrica, la notizia n. 11 nel numero 2/2023 [2023/2(11)LV] e in *Atlante*, p. 359; e anche la notizia n. 27 nel numero 4/2023 [2023/4(27)IG] e in *Atlante*, p. 484) – o, per l'Unione europea, il regolamento (UE) 2022/2065 (*Digital Services Act*, **DSA**), che contiene disposizioni intese ad offrire ai bambini una maggiore protezione online e ad impedire alle piattaforme di rivolgersi ai minori con annunci personalizzati (art. 28 DSA) - la nuova legge australiana costituisce ad oggi un *unicum* per la radicalità della sua misura,

ISSN 2239-8570

e, anche per questo motivo, fungerà sicuramente da punto di riferimento per il dibattito, ancora molto vivo, sulle tematiche della protezione dei minori online.

RACHELE RANIERI

https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7284.
https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7284_ems_b9c134ac-a19a-47b2-9879-b03dda6e3c1a%22
https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr7284_ems_ca8c5dba-cc80-4846-92f5-bea56885dcdf%22

2024/4(54)VR

54. L'audizione di Meta al Senato australiano del 26.11.2024 e la sua ammissione di ricorrere allo *scraping* generalizzato dei dati degli utenti a fini di addestramento dei propri modelli di IA

Il 26 novembre 2024 il Senato australiano ha pubblicato una relazione del *Select Committee on Adopting Artificial Intelligence*.

Il documento analizza – in 6 capitoli lunghi più di 200 pagine – lo stato dell'arte e le sfide future poste dall'Intelligenza Artificiale (**IA**).

Più precisamente, muovendo da alcune premesse che culminano in un quadro rappresentativo dell'impiego delle tecnologie di IA in Australia, si affrontano i seguenti temi: il pertinente sistema normativo e i suoi sviluppi futuri, accompagnato dalla comparazione con ordinamenti stranieri; l'industria dell'IA; l'impatto di tali tecnologie sulle imprese e i lavoratori; i processi decisionali automatizzati; l'impatto ambientale.

In questo contesto, il rapporto affronta in più parti la questione dello *scraping* dei dati degli utenti da parte di alcuni *"Tech Giants"* come **Google**, **Amazon** e **Meta** (cfr. pp. 16, 47, 86, 87). Riguardo quest'ultimo (Meta), le pagine sugellano i risultati delle audizioni avvenute nelle settimane precedenti e in particolare quella del suo *Global privacy policy director* Melinda Claybaugh, la quale, incalzata dal senatore David Shoebridge, ha ammesso pubblicamente che Facebook starebbe da tempo estraendo informazioni da foto, post e altri dati – si badi – pubblici degli utenti australiani a fini di addestramento dei propri modelli di IA.

Il rapporto è di particolare interesse perché si sono espressamente poste a confronto la legislazione australiana e quella europea (quest'ultima già in sede di audizioni) e statunitense. Si è evidenziato che, a differenza delle seconde due, quella australiana nulla dispone circa le tecniche di *scraping* non consensuale di dati personali degli utenti. Se ne è desunto che ciò ha consentito a Meta di procedere, dopo il 2007, all'estrazione generalizzata senza concedere una clausola di *opt-out* o altro rimedio equipollente.

ISSN 2239-8570

L'unica soluzione residua per gli utenti australiani sarebbe stata quella di impostare i propri dati (foto, post ecc.) come privati, ma nessuna comunicazione veniva fornita sulla facoltà di Facebook di potervi attingervi liberamente in caso contrario.

Da questo punto di vista, la relazione in commento testimonia in modo tangibile l'effetto che la qualità e la severità della regolazione sono in grado di avere sull'operato delle imprese e le implicazioni dirette per le vita – e i diritti – dei cittadini.

VALENTINO RAVAGNANI

https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000470/toc_pdf/SelectCommitteeonAdoptingArtificialIntelligence(AI).pdf

2024/4(55)LC

55. L'iniziativa del governo dell'Australia di vietare il dynamic pricing come pratica commerciale scorretta

Il governo australiano, sotto la guida del Primo Ministro Anthony Albanese, ha avviato nel novembre scorso una consultazione pubblica per l'introduzione del divieto di nuove fattispecie di pratiche commerciali scorrette nella vigente legge a tutela dei consumatori (*Competition and Consumer Act 2010*). Tra queste pratiche figurano, in particolare, le c.d. *subscription traps* (letteralmente, "abbonamenti trappola") laddove gli utenti abbiano una certa facilità ad iscriversi ad un servizio online e, viceversa, non altrettanta all'atto della disiscrizione, riscontrando invece non poche difficoltà nel procedere alla cancellazione dei dati forniti; il c.d. *drip pricing* (letteralmente, "prezzo a goccia"), particolarmente diffuso nei servizi di prenotazione di voli aerei e hotel, ove il costo inizialmente offerto aumenta gradualmente con l'aggiunta di tariffe obbligatorie durante il processo di finalizzazione dell'acquisto; infine, il c.d. *dynamic pricing* (letteralmente, "prezzo dinamico"), ove il prezzo aumenta all'aumentare del numero di utenti che simultaneamente effettuano l'acquisto dello stesso prodotto. Quest'ultimo fenomeno presenta caratteristiche peculiari ed è invalso soprattutto nell'acquisto di biglietti di concerti di *band* musicali particolarmente note al grande pubblico, come nel caso del tour dei Green Day, band punk-rock americana, che ha acceso il dibattito in Australia e acceso i riflettori del governo su tali pratiche: a causa della grande domanda sulla piattaforma Ticketmaster, il costo di un singolo biglietto è passato rapidamente da 100 a 500 dollari australiani. Da qui la definizione di prezzo "dinamico", comunemente usato per riferirsi alla pratica di variare i prezzi per un bene o un servizio in base a fattori come la domanda in tempo reale. Il *dynamic pricing* funziona attraverso un algoritmo che regola il prezzo sulla base di quanti utenti sono disposti a pagare per ottenerlo; per calcolarlo viene creata una "coda digitale" di accesso al sito su cui vengono venduti i biglietti. Se da un lato tale meccanismo è servito a contrastare la rivendita

ISSN 2239-8570

dei biglietti tramite il c.d. *secondary ticketing*, dall'altro lato ha contribuito a un aumento generalizzato ed eccessivo dei prezzi. Più nel dettaglio, atteso che questo aumento di prezzo si verifica in un breve lasso di tempo, coincidente con il processo di acquisto online, e che il prezzo finale potrebbe non essere rivelato fino alla conclusione dell'acquisto, i consumatori potrebbero essere presi alla sprovvista e indotti ad un'irragionevole decisione di consumo, proprio a causa di tale rapidità di distorsione dei prezzi. Inoltre, tali pratiche possono essere combinate con altre, volte ad esercitare pressioni ingiustificate sui consumatori, come l'attivazione di contatori di *timeout* e notifiche di scarsità dei biglietti. Tale combinazione di fattori sarebbe idonea ad ingenerare nei consumatori il timore o che il prezzo aumenti ulteriormente, potenzialmente oltre le loro capacità economiche, o che perdano del tutto l'occasione di acquistare il biglietto del loro beniamino, facendo così leva anche sull'emotività. Resta inteso che il *dynamic pricing* non configura di per sé una pratica illecita, ma la sua riconducibilità o meno alla fattispecie di pratica commerciale scorretta dipenderà dalle circostanze del singolo caso concreto. La consultazione si è chiusa il 13 dicembre scorso e nel torno dei prossimi mesi si attendono ulteriori passi da parte del governo centrale australiano, di concerto con i singoli governi territoriali, nell'iter di modifica della legge sulle pratiche commerciali scorrette per l'introduzione di nuovi divieti per la tutela dei consumatori, in particolare contro il dynamic pricing.

LUCIO CASALINI

https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/consultation-underway-ban-business-practices-ripping
https://treasury.gov.au/consultation/c2024-602157
https://treasury.gov.au/sites/default/files/2024-11/c2024-602157-cp.pdf

ISSN 2239-8570