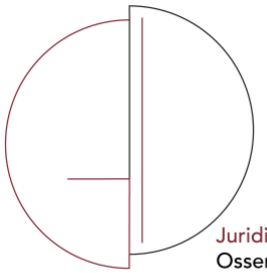

DIRITTO E NUOVE TECNOLOGIE*

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.** ***Adottato il Regolamento 'macchine' (UE) 2023/1230*** [2023/3(1)VR]**. - 2.** ***La decisione di adeguatezza della Commissione europea del 10.7.2023 sul nuovo piano di trasferimento dei dati personali EU-U.S. (Privacy Framework) e la nota informativa dell'EDPB*** [2023/3(2)CR]**. - 3.** ***La designazione di Alphabet, Amazon, Apple, Bytedance, Meta e Microsoft come gatekeepers ai sensi del DMA*** [2023/3(3)RA]. - **4.** ***Verso il FIDA: la proposta di regolamento europeo sull'accesso ai dati finanziari del 28.6.2023*** [2023/3(4)BC]. - **5.** ***Il parere dell'EDPS del 22.8.2023 sulla proposta di regolamento europeo sull'accesso ai dati finanziari (FIDA)*** [2023/3(5)TB]. - **6.** ***Le Linee guida AGID del 4.8.2023 sui dati aperti nel settore pubblico versione 1.0*** [2023/3(6)FDA]. - **7.** ***La sentenza CGUE del 4.7.2023 nel caso C-252/21 sui rapporti tra privacy e antitrust, sulla pubblicità dei dati sensibili e sulla inadeguatezza della base del legittimo interesse per il trattamento dei dati inerenti la pubblicità comportamentale di Meta (sentenza Meta abuso di posizione dominante)*** [2023/3(7)CAT]**. - 8.** ***Il provvedimento del 14.7.2023 del Garante norvegese per la protezione dei dati personali sulla base del legittimo interesse per la pubblicità comportamentale di Meta*** [2023/3(8)GDI]**. - 9.** ***La sentenza CEDU del 4.7.2023 sul diritto all'oblio (caso 57292/16 Hurbain c. Belgio)*** [2023/3(9)EB]**. - 10.** ***La decisione vincolante EDPB 2/2023 del 2.8.2023 e la conseguente decisione finale del Garante irlandese per la protezione dei dati personali del 1.9.2023 su c.d. dark (o deceptive design) patterns e altre pratiche riguardanti i bambini e la verifica dell'età poste in essere da TikTok*** [2023/3(10)IG]**. - 11.** ***I provvedimenti dei Garanti per la protezione dei dati personali austriaco e della Bassa Sassonia, dell'aprile e del maggio 2023, in materia di cookie paywall impiegati da testate di giornali online*** [2023/3(11)RMo]**. - 12.** ***Emessa in Cile il 9.8.2023 la prima sentenza al mondo sui neurodiritti (a proposito di 'Insight' un dispositivo neurotecnologico non terapeutico e non invasivo in commercio del tipo elettroencefalogramma mobile progettato per ottenere informazioni sull'attività cerebrale)*** [2023/3(12)AAM]. - **13.** ***La sentenza della Corte Costituzionale del 27.7.2023 sul valore di corrispondenza dei messaggi whatsapp e email*** [2023/3(13)EWDM]. - **14.** ***Le modifiche alla legge italiana sul diritto d'autore per il contrasto della pirateria online (L. 93/2023)*** [2023/3(14)FG]**. - 15.** ***Il provvedimento dell'AGCM del 18.7.2023 sugli impegni di Google relativi alla portabilità dei dati personali*** [2023/3(15)RA]. - **16.** ***L'intesa tra il governo USA e i "giganti" dell'Intelligenza Artificiale del 21.7.2023 e del 12.9.2023 su safety, security e trust della IA generativa*** [2023/3(16)TDMCDV]**. - 17.** ***L'opinion del 18.8.2023 (e il collegato provvedimento) del Giudice Howell del District of Columbia nel caso Thaler su IA generativa e copyright*** [2023/3(17)FG] **- 18.** ***Le raccomandazioni del 17.7.2023 del Financial Stability Board sui Global Stable Coin Arrangements e sui mercati in criptoattività*** [2023/3(18)IT. - **19.** ***Le nuove regole della SEC su cybersecurity risk, governance, management e incident disclosure efficaci dal 5.9.2023*** [2023/3(19)ES]. - **20.** ***La seconda fase di sperimentazione Fintech*** [2023/3(20)ES]. - **21.** ***Gli obblighi informativi nel rapporto di lavoro relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati (D.L. 48/2023 conv. con modifiche da L. 85/2023) e la sentenza del Tribunale di Torino del 5.8.2023 sulla condotta antisindacale di Glovo*** [2023/3(21)RMa]**. - 22.** ***Emanato il Decreto 7.9.2023 sul fascicolo sanitario elettronico (FSE) 2.0 dopo i pareri positivi del Garante privacy del 8.6.2023 e della Conferenza Stato-Regioni del 2.8.2023*** [2023/3(22)EG]

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

2023/3(1)VR

Adottato il Regolamento 'macchine' (UE) 2023/1230

Il 14 giugno 2023 è stato approvato il Regolamento (UE) 2023/1230 relativo alle macchine, che abroga la direttiva 2006/42/CE e la direttiva 73/361/CEE ("**Regolamento macchine**"), dando così seguito alla relativa proposta adottata il 21 aprile 2021 (coeva alla proposta di AI Act) COM(2021) 202 final.

Come evincibile dal Preambolo, il legislatore europeo ha inteso rafforzare il quadro normativo in uno dei pilastri industriali dell'economia dell'Unione al precipuo fine di contenere il costo sociale del crescente impiego dei prodotti macchina attraverso l'integrazione dei requisiti di sicurezza (Considerando n. 2). In quest'ottica, si è ritenuto opportuno, anzitutto, agire sul piano della tecnica normativa: in linea con una tendenza recente della regolazione europea volta al massimo contenimento delle divergenze normative nelle legislazioni domestiche, si è privilegiata la via dell'uniformazione. La concreta applicazione della (ora abrogata) direttiva 2006/42/CE ("**Direttiva macchine**") aveva infatti mostrato forti carenze nella copertura dei prodotti e nelle procedure di valutazione della conformità, rendendo opportuna la sua sostituzione con una fonte regolamentare (Considerando nn. 3, 4, 85).

Ne viene un quadro regolatorio assai più corposo e puntuale, che consta di 86 Considerando, 54 articoli e ben 7 Allegati. Anche in ragione di ciò, nonostante la fonte entri in vigore dopo l'ordinaria *vacatio legis* di venti giorni, il legislatore europeo ha ritenuto necessario disporne un'applicazione differita (*recte*, graduale) affinché gli operatori economici possano uniformarsi alle prescrizioni e gli Stati membri approntino le necessarie infrastrutture amministrative (Considerando n. 86). Pertanto, ai sensi dell'art. 54, il Regolamento macchine si applicherà nella sua globalità a partire dal 14 gennaio 2027; nelle more: gli artt. 26-42 si applicheranno a decorrere dal 14 gennaio 2024; l'art. 50, par. 1 si applicherà a decorrere dal 14 ottobre 2023; l'art.6, par. 7 e gli artt. 48 e 52 si applicheranno a decorrere dal 13 luglio 2023; l'art. 6, parr. 2-6, 8 e 11 e gli artt. 47 e 53, par. 3 si applicheranno a decorrere dal 14 luglio 2024.

Il Regolamento macchine si applica alle macchine e alle «quasi-macchine» (in inglese: «*partly completed machines*»), definite come segue:

- «macchina»:

a) insieme equipaggiato o destinato a essere equipaggiato di un sistema di azionamento diverso dalla forza umana o animale diretta, composto di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidamente per un'applicazione ben determinata;
b) insieme di cui alla lettera a), al quale mancano solamente elementi di collegamento al sito di impiego o di allacciamento alle fonti di energia e di movimento;
c) insieme di cui alle lettere a) e b), pronto per essere installato e che può funzionare solo dopo essere stato montato su un mezzo di trasporto o installato in un edificio o in una costruzione;
d) insiemi di macchine di cui alle lettere a), b) e c) o di quasi-macchine, che per raggiungere uno stesso risultato sono disposti e comandati in modo da avere un funzionamento solidale;
e) insieme di parti o di componenti, di cui almeno uno mobile, collegati tra loro solidalmente e destinati al sollevamento di pesi e la cui unica fonte di energia è la forza umana diretta;
f) insieme di cui alle lettere da a) ad e) al quale manca soltanto il caricamento del *software* destinato all'applicazione specifica prevista dal fabbricante.

- «quasi-macchina»: un insieme che non costituisce ancora una macchina in quanto, da solo, non è in grado di eseguire un'applicazione specifica e che è soltanto destinato a essere incorporato o assemblato ad altre macchine o ad altre quasi-macchine o apparecchi per costituire una macchina.

Un lungo elenco di esclusioni è previsto al paragrafo 2 dell'art. 2, lettere da *a*) a *q)*. Tra esse, si segnala l'esclusione per i veicoli a motore e i relativi rimorchi, nonché i sistemi, i componenti, le unità tecniche separate, le parti e le attrezzature progettate e costruite per tali veicoli, che rientrano nell'ambito di applicazione del regolamento (UE) 2018/858 attinente alla loro omologazione.

Il Considerando n. 19 sottolinea che (come da corrispondente previsione della lettera *f)* della definizione di macchina, sopra riportata) le macchine alle quali manca solamente il caricamento di *software* destinati all'applicazione specifica prevista dal fabbricante e che sono oggetto della procedura di valutazione della conformità di tali macchine rientrano nella definizione di macchina e non nelle definizioni di prodotti correlati o di quasi-macchine. I prodotti correlati sono le attrezzature intercambiabili, i componenti di sicurezza, gli accessori di sollevamento, le catene, funi e cinghie e i dispositivi amovibili di trasmissione meccanica, come meglio definiti nel medesimo Regolamento

macchine. Inoltre, sempre nel Considerando n. 19 si specifica che la definizione di componenti di sicurezza riguarda non soltanto i dispositivi fisici ma anche quelli digitali. Si aggiunge in proposito che, al fine di tenere conto del crescente ricorso al *software* come componente di sicurezza, il *software* che svolge una funzione di sicurezza ed è immesso in maniera indipendente sul mercato deve essere considerato un componente di sicurezza.Il Regolamento macchine intende accrescere la tutela della sicurezza e della salute delle persone e, «*ove opportuno*» («*where appropriate*» in inglese), degli animali domestici (espressione che ricomprende quelli di allevamento: Considerando n. 5), nonché la tutela dei beni, specie nei confronti dei rischi che derivano dall'uso previsto o da qualsiasi uso scorretto ragionevolmente prevedibile. Espressamente menzionata, sia pure solo con la formula «*se del caso*» («*where applicable*» in inglese), è anche la tutela dell'ambiente (art. 1). Per quanto attiene alla protezione delle persone, particolare enfasi è posta sui lavoratori e i consumatori (Considerando n. 5), tenendo conto delle ridotte conoscenze tecniche degli utilizzatori non professionali nella gestione delle macchine o dei prodotti correlati (Considerando n. 11). La regola generale, di cui all'art. 8, è dunque che le macchine o i prodotti correlati sono messi a disposizione sul mercato o messi in servizio soltanto se, quando debitamente installati, sottoposti a manutenzione e utilizzati conformemente al loro uso previsto o in condizioni ragionevolmente prevedibili, soddisfano i requisiti essenziali di sicurezza e di tutela della salute di cui all'Allegato III; similmente, le quasi-macchine sono messe a disposizione sul mercato solo se rispettano i pertinenti requisiti essenziali di sicurezza e di tutela della salute di cui all'Allegato III.

Similmente a quanto si trova nella proposta di AI Act e nella nuova legislazione UE sui prodotti, di cui al c.d. NLF (*New Legislative Framework for the marketing of products*: nuovo quadro legislativo per la commercializzazione dei prodotti) di cui alla decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, e al regolamento (UE) 2019/1020 sulla vigilanza del mercato e sulla conformità dei prodotti, il Regolamento macchine prevede delle definizioni di «messa a disposizione sul mercato», «immissione sul mercato» e «messa in servizio». Più generalmente, appare sicuramente apprezzabile, almeno negli intenti, l'attenzione riposta sul piano definitorio (art. 3) e dell'esatta perimetrazione dell'ambito di applicazione materiale del regolamento, muovendo dall'evocata distinzione tra macchine, prodotti correlati e quasi-macchine (art. 2; Considerando nn. 14 e 15). A tal proposito, si tiene debitamente conto delle implicazioni in termini di *product safety* dell'emergere delle nuove tecnologie digitali quali l'intelligenza artificiale, l'IoT e la robotica e della necessità di disciplinarne i rischi specifici (Considerando n. 12). Ciò rileva almeno su due fronti: *in primis*, sul terreno della stessa definizione di macchina, che – come visto – richiede di essere adattata al progressivo impiego di mezzi digitali e *software* in fase di progettazione (Considerando n. 19); *in secundis*, sul piano generale di contenimento dell'obsolescenza del regime in commento, deve garantirsi l'aggiornamento dei criteri classificatori di cui all'Allegato I sull'onda dell'evoluzione dello stato dell'arte (Considerando n. 24). L'obiettivo di effettività delle tutele garantite dal regolamento richiede, infine, un appropriato coordinamento con gli altri atti normativi dell'Unione (di cui ai Considerando nn. 6-9, 22, all'art. 9 e al nutrito elenco di esclusioni di cui all'art. 2, par. 2).

Per quanto attiene in particolare all'AI Act - di cui alla proposta di Regolamento UE sull'intelligenza artificiale di cui alla proposta COM(2021) 26 final - si segnala come nella relazione di accompagnamento alla proposta del Regolamento macchine COM(2021)202 final, (la "Relazione"), la Commissione europea così esponeva "*La presente proposta è coerente con la politica dell'Unione in materia di intelligenza artificiale e con l'imminente regolamento sull'intelligenza artificiale, che affronterà i rischi che incidono sulla sicurezza per i sistemi di intelligenza artificiale ad alto rischio integrati in una macchina o che sono componenti di sicurezza nel quadro del futuro regolamento sui prodotti macchina*" (punto 1.3, p. 4 della Relazione) e "*Un ulteriore aspetto di semplificazione è costituito dalla complementarità tra le proposte legislative sull'intelligenza artificiale e sulle macchine, nell'ambito delle quali il regolamento sull'intelligenza artificiale delega la valutazione della conformità a quello sulle macchine affinché la valutazione dei rischi per la macchina completa con i sistemi di intelligenza artificiale venga effettuata una volta soltanto attraverso il futuro regolamento sui prodotti macchina*" (punto 3.4, p. 9 della Relazione).

In punto di allocazione degli obblighi di sicurezza, il Regolamento macchine persegue il consolidato approccio di distribuzione delle responsabilità tra gli operatori economici in funzione dei ruoli da essi rivestiti nella catena di approvvigionamento (Considerando n. 28), al fine di circoscrivere l'immissione nel mercato interno ai soli prodotti conformi alle prescrizioni di legge.

In ragione della razionalità offerta dal criterio della *vicinitas*, il riferente principale del quadro di protezione è il fabbricante (come definito nel Regolamento macchine, ma v. anche artt. 17 e 18). La *ratio* della scelta è dichiarata consistere nella deduzione che il fabbricante, disponendo di conoscenze dettagliate relative al processo di progettazione e produzione, versi nella posizione migliore per eseguire la procedura di valutazione della conformità di cui all'art. 25, che rimane pertanto in linea di principio suo obbligo esclusivo (Considerando n. 31). A tale valutazione si accompagna la redazione della pertinente documentazione tecnica. Ai sensi dell'art. 10, par. 2, in caso di esito positivo della procedura di valutazione della conformità, i fabbricanti redigono la dichiarazione di conformità UE conformemente all'art. 21 e appongono la marcatura CE conformemente all'art. 24. La marcatura CE è soggetta ai principi generali contenuti nell'art. 30 del regolamento (CE) n. 765/2008 (art. 23 Regolamento macchine).

Il fabbricante è tenuto a effettuare una precisa valutazione del rischio per il prodotto che intende immettere sul mercato o mettere in servizio, stabilendo gli opportuni requisiti essenziali di sicurezza e le misure di gestione dei rischi specifici che potrebbero manifestarsi durante il ciclo di vita del prodotto. In altri termini, la perdurante conformità dei prodotti macchina deve essere garantita lungo tutto quest'arco temporale, tenendo debitamente da conto le modifiche del processo produttivo, della progettazione o delle caratteristiche dei beni, nonché delle altre specifiche tecniche o delle specifiche comuni di cui all'art. 20 (art. 10, par. 4). Laddove i fabbricanti abbiano motivo di ritenere che una macchina o un prodotto correlato da essi immesso sul mercato o messo in servizio non sia conforme al Regolamento macchine, essi devono adottare immediatamente le azioni correttive necessarie per ripristinarne la conformità ovvero disporre, a seconda dei casi, il ritiro o il richiamo. Gli stessi sono poi tenuti a informare immediatamente le competenti autorità nazionali, fornendo informazioni dettagliate (art. 10, par. 9). Un regime analogo, *mutatis mutandis*, è previsto per le quasi-macchine dagli artt. 11 e 22. Per esse, in caso di valutazione positiva della conformità, è redatta una «dichiarazione di incorporazione UE» che, al pari della dichiarazione di conformità, attesta che è stata dimostrata la conformità ai requisiti essenziali di sicurezza e di tutela della salute di cui all'Allegato III (v. rispettivamente, artt. 20, 21 e 22).

Per determinate categorie di macchine o prodotti correlati che presentano un fattore di rischio più elevato, si rende necessario che i fabbricanti siano coadiuvati da organismi notificati al fine di assicurare procedure di valutazione della conformità più rigorose (Considerando n. 59: v. Capo V, artt. 26 ss.).

È poi necessario garantire la conformità ai requisiti del regolamento dei prodotti macchina provenienti da paesi extra-UE. Pertanto, gli importatori devono anzitutto assicurarsi che per essi siano state condotte dal fabbricante le relative verifiche (Considerando n. 36). Più precisamente, ai sensi dell'art. 13, gli importatori di macchine e prodotti correlati devono assicurarsi che il fabbricante: abbia svolto le adeguate procedure di valutazione *ex* art. 25; abbia redatto la documentazione tecnica di cui all'Allegato IV, parte A; che sia stata apposta la marcatura CE di cui all'art. 23; che la macchina o il prodotto correlato siano accompagnati dai documenti prescritti; in generale, che il fabbricante abbia rispettato le prescrizioni di cui all'art. 10, parr. 5, 6 e 8. In caso di esito negativo della verifica, l'immissione sul mercato è interdetta sino a che il prodotto non è reso conforme; se da esso possono derivare rischi, l'importatore ne informa il fabbricante e le autorità di vigilanza (art. 13, par. 4; ma v. anche par. 7). Prescrizioni equipollenti sono dettate per gli importatori di quasi-macchine (art. 14).

In seguito all'immissione nel mercato interno, l'obbligo di garantire la conformità del prodotto macchina all'atto della sua concreta messa a disposizione degli utenti trasla sul distributore, il quale deve peraltro assicurarsi che essa non venga alterata da eventuali successive manipolazioni del prodotto (Considerando n. 38; se la modifica è apportata direttamente dai distributori, v. *infra*, art. 17). Le verifiche prescritte sono puntualmente elencate agli artt. 15, par. 2 e 16, par. 2, rispettivamente per i distributori di macchine e quasi-macchine.

Di là dalle etichette formali, ai fini del Regolamento macchine un importatore o distributore è considerato un fabbricante, con conseguente addossamento dei relativi obblighi *ex* artt. 10 e 11, quando immette sul mercato un prodotto macchina con il proprio nome o marchio commerciale o modifica un prodotto già immesso sul mercato in un modo suscettibile di incidere sulla conformità ai requisiti applicabili (art. 17). Più in generale, è considerato fabbricante ai sensi del Regolamento macchine qualsiasi soggetto, persona fisica o giuridica, che apporta una modifica sostanziale alla macchina o a un prodotto correlato (art. 18).

Infine, tutti gli operatori economici coinvolti nella catena sono tenuti a far sì che la documentazione pertinente, *i.e.* le istruzioni per l'uso, contenga

informazioni precise e comprensibili e sia il più possibile aggiornata tenendo conto degli sviluppi tecnologici e delle (prevedibili) variazioni del comportamento degli utilizzatori (Considerando n. 39, art. 10, parr. 6 e 7).

Merita evidenziare la centralità dell'art. 20, che realizza un importante punto di equilibrio tra le concorrenti finalità, enunciate all'art. 1, di consentire la messa a disposizione sul mercato o la messa in servizio dei prodotti macchina e di garantire, al contempo, un livello elevato di tutela della salute e di sicurezza. Ai sensi della citata disposizione, un prodotto rientrante nell'ambito di applicazione del Regolamento macchine conforme alle norme armonizzate o alle parti di esse i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea è considerato conforme ai requisiti essenziali di sicurezza e di tutela della salute di cui all'Allegato III contemplati da tali norme o da parti di esse.

Al fine di garantire un'applicazione corretta ed uniforme del regolamento, è essenziale implementare un quadro di coordinamento dell'attività di vigilanza (Considerando n. 68). A tal fine, è opportuno prescrivere il coinvolgimento degli operatori economici con maggiore prossimità al mercato, cioè a dire, anzitutto, i distributori e gli importatori, chiamati a coadiuvare le autorità nazionali competenti assicurando la circolarità informativa e una pronta e diretta partecipazione ai controlli (Considerando n. 41). Ai sensi dell'art. 43, le autorità di vigilanza del mercato di uno degli Stati membri, qualora abbiano sufficienti ragioni per ritenere che un prodotto rappresenti un rischio per i beni giuridici tutelati dal Regolamento macchina, effettuano una valutazione della conformità di esso a tutte le pertinenti prescrizioni del regolamento stesso. In caso di esito negativo della verifica, le medesime autorità sollecitano tempestivamente l'operatore economico interessato affinché siano adottate le opportune misure correttive al fine di porre termine allo stato di non conformità e/o di eliminare o, quantomeno, contenere i rischi. L'operatore economico in questione è tenuto a provvedere di conseguenza. Laddove ciò non avvenga, le autorità provvedono affinché il prodotto interessato sia ritirato o richiamato ovvero affinché la sua messa a disposizione sul mercato sia vietata o limitata, informando immediatamente il pubblico, la Commissione e gli altri Stati membri.

Infine, due articoli sono dedicati *(i)* alla possibilità di contestare i provvedimenti adottati dagli Stati membri in esito agli accertamenti delle autorità di vigilanza nazionali di cui al precitato art. 43, nel superiore interesse dell'Unione, con attribuzione di poteri di iniziativa e decisionali vincolanti alla Commissione europea (art. 44), e *(ii)* alla possibilità accordata agli Stati membri di adottare misure specifiche su prodotti rientranti nell'ambito di applicazione del Regolamento macchine, i quali, pur essendo risultati conformi ai requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato III del medesimo regolamento, siano nondimeno ritenuti «presentare un rischio per la salute o la sicurezza delle persone e, ove opportuno, degli animali domestici nonché per la tutela dei beni e, se del caso, dell'ambiente» (c.d. 'prodotti conformi che presentano un rischio'), prevedendosi tuttavia anche, in tali casi, un dovere di informazione alla Commissione europea da parte degli Stati membri che adottino simili misure, un dovere di consultazione della Commissione europea con gli altri Stati membri, e - anche in questi casi - un potere decisorio finale e vincolante della medesima Commissione europea in ordine alla giustificazione di ogni provvedimento di questo tipo (art. 45).

VALENTINO RAVAGNANI

https://eur-lex.europa.eu/eli/reg/2023/1230/oj

2023/3(2)CR

La decisione di adeguatezza della Commissione europea del 10.7.2023 sul nuovo piano di trasferimento dei dati personali EU-U.S. (Privacy Framework) e la nota informativa dell'EDPB

Il 10 luglio 2023 la Commissione europea ha adottato la decisione di adeguatezza sul nuovo quadro normativo statunitense in materia di protezione dei dati per il trasferimento di dati personali UE-USA ("***Data Protection Framework***"). Si pone così fine alla situazione di incertezza iniziata tre anni fa con l'annullamento del precedente quadro UE-USA (il *Privacy Shield*) in seguito alla sentenza Schrems II (su cui v. in questa rubrica la notizia 1 nel numero 2020/3 [2020/3(1)CR]: http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf).

La Commissione ha dunque ritenuto che attraverso il nuovo accordo, raggiunto dal Presidente USA Joe Biden e dalla Presidente della Commissione europea Ursula von der Leyen, gli Stati Uniti garantiscono un livello di protezione dei dati

personali dei cittadini europei equivalente a quello assicurato nell'UE dal GDPR.
Per raggiungere questo obiettivo, superando le preoccupazioni sollevate dalla Corte di Giustizia in Shrems II, il *Data Privacy Framework* ha introdotto una serie di garanzie vincolanti per le imprese statunitensi che intendono trattare i dati personali dei cittadini dell'UE.
In primo luogo, è stato posto un limite ai poteri delle autorità pubbliche statunitensi che potranno accedere ai dati trasferiti nell'ambito del nuovo quadro limitatamente a quanto necessario e proporzionato ai fini dell'applicazione della legge penale e di sicurezza nazionale.
Altra importante novità è l'introduzione di un meccanismo di ricorso indipendente e imparziale con riferimento alla raccolta e all'utilizzo dei dati personali da parte delle agenzie di *intelligence* statunitensi. I cittadini europei, infatti, potranno presentare reclamo davanti a un tribunale del riesame in materia di protezione dei dati, il *Data Protection Review Court* (**DPRC**), che esaminerà e risolverà i reclami in modo indipendente, anche adottando misure correttive vincolanti. In particolare, se il DPRC ritiene che i dati siano stati raccolti in violazione delle nuove garanzie, potrà ordinarne la cancellazione.
Alla luce di questa decisione di adeguatezza, le imprese statunitensi potranno decidere di aderire al *Data Privacy Framework* sul trasferimento dei dati UE-USA impegnandosi a rispettare una serie di obblighi. Tra gli altri, dovranno impegnarsi a cancellare i dati personali quando non più necessari per lo scopo per cui erano stati raccolti, informare gli interessati dell'adesione al DPF e fornire una serie di informazioni relative al trattamento dei dati, e garantire la continuità della protezione anche quando i dati personali sono condivisi con terzi.
In seguito alla decisione della Commissione europea, lo *European Data Protection Board* (**EDPB**) ha pubblicato una nota informativa con cui ha fornito alcuni chiarimenti sulle implicazioni della decisione di adeguatezza per i cittadini dell'UE e per le imprese che trasferiscono dati personali dall'EU agli Stati Uniti. In particolare, l'EDPB ha chiarito che i trasferimenti basati sul DPF non richiederanno misure supplementari per garantire la protezione dei dati durante il trasferimento, mentre se il trasferimento avviene nei confronti di imprese che non hanno aderito al *Framework*, dovranno essere adottate misure di sicurezza adeguate, come le clausole standard di protezione dei dati o le regole aziendali vincolanti.
L'EDPB ha anche precisato che il funzionamento del quadro UE-USA per la protezione dei dati personali sarà oggetto di riesami periodici effettuati dalla Commissione europea in collaborazione con i rappresentanti delle autorità europee di protezione dei dati e delle autorità statunitensi competenti. Il primo riesame avverrà entro un anno dall'entrata in vigore della decisione di adeguatezza e verificherà che tutti gli elementi del quadro siano stati pienamente attuati nel sistema giuridico statunitense e funzionino efficacemente.
L'emanazione della decisione di adeguatezza è stata già commentata da Maximillian Schrems che ha dichiarato che il DPF non rappresenta un vero passo avanti rispetto ai problemi di sorveglianza che avevano causato l'invalidazione del *Privacy Shield* in quanto sostanzialmente presenta gli stessi meccanismi del vecchio accordo. NOYB e Schrems hanno quindi già prospettato nuovi ricorsi davanti alla Corte di Giustizia per l'invalidazione del nuovo quadro.

CHIARA RAUCCIO

https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3721
https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf

2023/3(3)RA

La designazione di Alphabet, Amazon, Apple, Bytedance, Meta e Microsoft come gatekeepers ai sensi del DMA

Lo scorso 6 settembre 2023, la Commissione europea ha designato 6 *gatekeeper* – individuati in Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft – a norma del *Digital Markets Act* ("**DMA**"), entrato in vigore nel novembre 2022 e applicabile dal maggio 2023 (v. in questa Rubrica notizia 2 nel numero 2022/4 [2022/4(2)RA]: http://www.personaemercato.it/wp-content/uploads/2023/01/Osservatorio.pdf), identificando 22 servizi di piattaforma di base forniti da tali soggetti (tra cui: Facebook, Instagram, TikTok, Whatsapp, YouTube, Google Search, Amazon Marketplace, App Store e Safari).
A norma del DMA, infatti, la Commissione europea può designare come *gatekeeper* le piattaforme digitali che forniscono un punto di accesso rilevante tra imprese e consumatori in relazione ai servizi di piattaforma di base.
I *gatekeeper* così individuati hanno ora sei mesi di tempo per garantire la piena osservanza degli

obblighi e dei divieti stabiliti dal DMA per ciascuno dei loro servizi di piattaforma di base.
Segnatamente, sotto il primo profilo, i *gatekeeper* dovranno ad esempio: rendere i propri servizi interoperabili per i terzi in talune specifiche situazioni; consentire agli utenti commerciali di accedere ai dati che generano utilizzando la piattaforma; fornire alle imprese che fanno pubblicità sulla piattaforma gli strumenti e le informazioni necessarie per consentire agli inserzionisti e agli editori di effettuare verifiche indipendenti dei messaggi pubblicitari ospitati dalla piattaforma; consentire agli utenti commerciali di promuovere la loro offerta e concludere contratti con clienti al di fuori della piattaforma.
Sotto il secondo profilo, ad esempio, i *gatekeeper* non dovranno: riservare ai propri servizi e prodotti un trattamento di favore rispetto a servizi o prodotti analoghi offerti da terzi sulla loro piattaforma; impedire ai consumatori di mettersi in contatto con le imprese al di fuori della piattaforma; impedire agli utenti di disinstallare applicazioni o software preinstallati, se lo desiderano; tenere traccia per motivi pubblicitari degli utenti finali al di fuori dei servizi essenziali della piattaforma, senza previo consenso dei diretti interessati.
La Commissione monitorerà l'effettiva attuazione e l'osservanza di tali obblighi e divieti. Nel caso in cui un *gatekeeper* non osservi gli obblighi sanciti dal DMA, la Commissione potrà irrogare ammende il cui importo non supera il 10% del fatturato totale realizzato a livello mondiale dall'impresa (e potrà essere non superiore al 20% di tale fatturato in caso di recidiva). In caso di violazioni c.d. sistematiche, alla Commissione è inoltre conferito il potere di adottare rimedi aggiuntivi, quali l'obbligo per il *gatekeeper* di vendere un'impresa (o parte di essa) ovvero il divieto per il *gatekeeper* di acquisire altri servizi.
Si segnala infine che la qualifica di *gatekeeper* è presa in considerazione dalla proposta di Data Act COM(2022) 68 *final* del 23.2.2022 , ai sensi della quale, relativamente ai dati generati dall'uso di prodotti interconnessi o servizi correlati, i terzi con i quali i medesimi dati possono essere condivisi ai sensi di quella disciplina non possono essere *gatekeepers* (artt. 5, 6 della proposta di Data Act COM(2022) 68 *final* del 23.2.2022, su cui v. la notizia 4 nel numero 2022/1 di questa Rubrica [2022/1(4)SO]: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf).

RICCARDO ALFONSI

https://ec.europa.eu/commission/presscorner/detail/it/ip_23_4328

2023/3(3)RA

Verso il FIDA: la proposta di regolamento europeo sull'accesso ai dati finanziari del 28.6.2023

Il 28 giugno 2023, la Commissione europea ha pubblicato la proposta per un "Regolamento del Parlamento Europeo e del Consiglio relativo a un quadro per l'accesso ai dati finanziari" COM(2023) 360 final (di seguito "**FIDA**", acronimo dall'inglese Financial Data Access).
La proposta di regolamento FIDA si inserisce, a pieno titolo, nella Strategia per la Finanza Digitale dell'Unione Europea ed è mirata alla creazione di uno spazio comune europeo per la gestione dei dati finanziari e per la condivisione di tali informazioni tra gli operatori del settore. Con questa proposta, la Commissione europea compie di fatto un altro passo in avanti nella direzione dell'open banking. La proposta di regolamento FIDA è coerente con altre proposte incluse nel Payment Package, ovvero il set di proposte normative varato dalla Commissione, sempre il 28 giugno 2023, contenente, tra le altre cose, la proposta della nuova direttiva sui servizi di pagamento (la PSD3) e il nuovo Payment Services Regulation (PSR).
Come chiarito nelle premesse del regolamento FIDA, tale proposta mira a risolvere alcune criticità connesse al fatto che "*i clienti del settore finanziario dell'UE non possono controllare efficacemente l'accesso ai loro dati e la condivisione degli stessi al di là dei conti di pagamento […]; le imprese che desiderano accedere ai dati dei clienti per fornire servizi innovativi, hanno problemi ad accedere ai dati detenuti dai titolari dei dati, ossia gli enti finanziari che raccolgono, conservano e trattano tali dati dei clienti*"
La proposta di regolamento FIDA intende, dunque, "*affrontare questi problemi consentendo ai consumatori e alle imprese di controllare meglio l'accesso ai loro dati finanziari".* Tramite l'auspicato miglioramento delle modalità di accesso e condivisione dei dati finanziari, si *"consentirebbe ai consumatori e alle imprese di beneficiare di prodotti e servizi finanziari adattati alle loro esigenze sulla base di dati per loro pertinenti, evitando nel contempo i rischi intrinseci […] e migliorare i risultati economici per i clienti dei servizi finanziari (consumatori e imprese) e le*

imprese del settore finanziario promuovendo la trasformazione digitale e accelerando l'adozione di modelli aziendali basati sui dati nel settore finanziario dell'UE".

Il FIDA mira a sviluppare un nuovo ecosistema normativo e operativo in cui la condivisione dei dati finanziari sarà funzionale all'innovazione tecnologica in ambito finanziario e alla personalizzazione dei servizi e dei prodotti finanziari che potranno essere sviluppati dall'industria di settore, facendo affidamento su una puntuale conoscenza dei dati dei singoli potenziali clienti.

i. L'ambito di applicazione: i profili oggettivi e soggettivi.

Quanto alla tipologia di dati finanziari, il FIDA troverà applicazione a un limitato set di dati e informazioni finanziarie del cliente (art. 2, comma 1), ovvero relativamente a: *i)* contratti di credito ipotecario, prestiti e conti correnti (ad eccezione dei conti di pagamento come definiti nella PSD2); *ii)* risparmi, investimenti in strumenti finanziari, prodotti di investimento basati su assicurazioni, cripto-attività, beni immobili e altre attività finanziarie correlate (nonché i benefici economici derivanti da tali asset); *iii)* diritti pensionistici; *iv)* prodotti assicurativi non-vita e, infine, *v)* dati relativi a valutazione del merito di credito di un'impresa raccolti nell'ambito di una procedura di richiesta di prestiti o nell'ambito di una procedura di richiesta di rating creditizio.

In relazione al perimetro soggettivo, il regolamento FIDA si applicherà esclusivamente ad alcune categorie di operatori del mercato bancario-finanziario a condizione che agiscano già come titolari o utenti dei dati.

Tali soggetti sono elencati all'art. 2, comma 2, ovverosia enti creditizi, istituti di pagamento (compresi i prestatori di servizi di informazione sui conti); istituti di moneta elettronica; imprese di investimento; prestatori di servizi per le cripto-attività; emittenti di token collegati ad attività; gestori di fondi di investimento alternativi; società di gestione di organismi d'investimento collettivo in valori mobiliari; imprese di assicurazione e di riassicurazione; intermediari assicurativi e intermediari assicurativi a titolo accessorio; enti pensionistici aziendali o professionali; agenzie di rating del credito; fornitori di servizi di crowdfunding; fornitori di PEPP (*prodotto pensionistico individuale paneuropeo*); prestatori di servizi di informazione finanziaria.

L'art. 4 del FIDA regola l'obbligo principale, a carico del titolare dei dati finanziari, prevendo che "*il titolare dei dati, su richiesta presentata da un cliente per via elettronica, mette a disposizione di quest'ultimo i dati di cui all'articolo 2, paragrafo 1, senza indebito ritardo, gratuitamente, in maniera continuativa e in tempo reale".*

In pratica, tale norma, una volta entrato in vigore il FIDA, attribuirà a ciascun cliente (consumatore o impresa) di un soggetto rientrante nel perimetro applicativo di cui all'art. 2, comma 2 il diritto di accedere ai propri dati finanziari mediante una semplice richiesta, anche in forma elettronica, e senza alcun costo a suo carico.

Il successivo art. 5 prevede l'obbligo, a carico dei soggetti elencati all'art. 2, comma 2 (*i.e.* gli utenti dei dati finanziari) che operano come titolari dei dati finanziari, di mettere a disposizione di un altro soggetto (*recte* di un altro utente dei dati) tutti i dati finanziari del cliente che quest'ultimo abbia richiesto di mettere a disposizione. In pratica, la cessione dei dati finanziari da un utente all'altro potrà avvenire esclusivamente previo consenso del cliente cui i dati si riferiscono.

L'obbligo disciplinato dall'art. 5 consentirà al cliente di richiedere che i propri dati siano resi accessibili e messi a disposizione di un altro operatore bancario/finanziario.

Ai sensi dell'art. 5, *"il titolare dei dati, su richiesta presentata da un cliente per via elettronica, mette a disposizione di un utente dei dati i dati del cliente […] per le finalità per le quali il cliente ha concesso l'autorizzazione all'utente dei dati. I dati del cliente sono messi a disposizione dell'utente dei dati senza indebito ritardo, in maniera continuativa e in tempo reale"* .

ii. Le modalità operative per la messa a disposizione del cliente e la condivisione dei dati finanziari: il pannello di gestione e il sistema (multilaterale) di condivisione dei dati finanziari

Mentre la messa a disposizione dei dati finanziari da parte del titolare a favore del cliente dovrà avvenire a titolo gratuito (art. 4), nel caso di condivisione dei dati dal titolare in favore di un altro utente dei dati (*i.e.* di un altro operatore del mercato bancario/finanziario), *"il titolare dei dati può chiedere un compenso a un utente dei dati per aver messo a disposizione i dati del cliente"* (art. 5 comma 2). Il titolare dei dati può chiedere un compenso per la messa a disposizione dei dati solo a condizione che *"i dati del cliente sono messi a disposizione […] conformemente alle norme e alle modalità di un sistema di condivisione dei dati finanziari di cui agli articoli 9 e 10, o se sono messi a disposizione a norma dell'articolo 11".*

L'art. 9 prevede difatti che entro 18 mesi dall'entrata in vigore del Regolamento FIDA, i

titolari e gli utenti dei dati aderiscano a un sistema di condivisione dei dati finanziari.

Prima di analizzare le norme che regolano i sistemi di condivisione dei dati finanziari, merita una menzione particolare il contenuto dell'art. 8, comma 1, che disciplina l'obbligo - per i titolari dei dati - di fornire "*al cliente un pannello di gestione delle autorizzazioni per monitorare e gestire le autorizzazioni fornite dal cliente agli utenti dei dati*".

I clienti, una volta attuato il FIDA, potranno accedere a una *dashboard* (panello di gestione) che dovrà essere messa a disposizione da ciascun titolare di dati; attraverso tale *dashboard* il cliente potrà ottenere "*una panoramica di ogni autorizzazione in corso concessa agli utenti dei dati, tra cui: i) il nome dell'utente dei dati cui è stato concesso l'accesso; ii) il conto, prodotto finanziario o servizio finanziario del cliente cui è stato concesso l'accesso; iii) la finalità dell'autorizzazione; iv) le categorie di dati condivisi; v) il periodo di validità dell'autorizzazione"* Tale *dashboard*, inoltre *"consente al cliente di revocare l'autorizzazione concessa a un utente dei dati; […] di ripristinare un'autorizzazione revocata* [e] *comprende un registro delle autorizzazioni revocate o scadute per un periodo di due anni".*

Tornando ora ad analizzare la disciplina prevista per la condivisione dei dati, il Titolo IV del FIDA è dedicato alla disciplina di una realtà totalmente innovativa, nella prospettiva sia del mercato bancario, sia della regolazione di settore. In pratica, il Titolo IV del FIDA regola i sistemi di condivisione dei dati finanziari, ovvero quei sistemi che, all'atto pratico, serviranno proprio per permettere la condivisione e la gestione dei flussi dei dati finanziari.

Gli articoli 9 e 10 del FIDA contengono le regole per la creazione e la *governance* di tali sistemi. La finalità dei sistemi di condivisione dei dati finanziari è, in pratica, far sì che tutti i titolari dei dati, gli utenti dei dati e le organizzazioni dei consumatori possano disporre di un sistema condiviso e centralizzato per la gestione e il flusso dei dati.

Alcuni profili di criticità del regolamento FIDA derivano dall'assenza di una disciplina di dettaglio che regoli il funzionamento di tali sistemi di condivisione dei dati finanziari; dal punto di vista strutturale e funzionale, infatti, tali sistemi parrebbero configurarsi – almeno dalla prospettiva civilistica italiana – come contratti atipici, aperti all'adesione di più parti (*i.e.* gli utenti dei dati).

La funzione di tali sistemi di condivisione dati è, in pratica, quella di: *i)* predisporre regole comuni per la gestione condivisa dei flussi di dati e per regolare il funzionamento delle interfacce e dei meccanismi di coordinamento per il funzionamento dei pannelli di gestione delle autorizzazioni per l'accesso ai dati finanziari; *ii)* creare un quadro contrattuale standardizzato comune che disciplini l'accesso a specifiche serie di dati; *iii)* stabilire le norme sulla governance di tali sistemi nonché sugli obblighi di trasparenza e sui compensi spettanti agli utenti che mettono a disposizione di altri utenti i dati finanziari; *iv)* le regole di responsabilità e risoluzione delle controversie.

L'art. 9 stabilisce che i dati finanziari, rientranti nell'ambito di applicazione del presente regolamento, devono essere messi a disposizione solo dei membri di uno stesso sistema di condivisione dei dati finanziari, rendendo obbligatoria l'adesione ad uno o più degli stessi.

L'art. 10 definisce i processi di *governance* di tali sistemi, comprese le norme sulla responsabilità contrattuale dei suoi membri e il meccanismo di risoluzione extragiudiziale delle controversie. L'articolo 10 prevede inoltre l'elaborazione di norme comuni per la condivisione dei dati e la creazione di interfacce tecniche da utilizzare per la condivisione dei dati.

Tali sistemi di condivisione dei dati devono essere notificati alle autorità competenti, devono beneficiare di un passaporto per le operazioni all'interno dell'Unione Europea e, a fini di trasparenza, i sistemi devono far parte di un registro pubblico tenuto dall'ABE.

L'art. 11 prevede l'ipotesi in cui, *"entro un tempo di lasso ragionevole"* – che tuttavia non è definito – *"non sia stato realizzato alcun sistema di condivisione dei dati finanziari per una o più categorie di dati del cliente"*. In tale scenario, connotato dunque dall'inerzia degli operatori privati, è previsto che alla Commissione europea sia "*conferito il potere di adottare un atto delegato […]al fine di integrare il presente regolamento specificando le seguenti modalità in base alle quali il titolare dei dati mette a disposizione i dati del cliente a norma dell'articolo 5, paragrafo 1, per tale categoria di dati: a) norme comuni per i dati e, se del caso, le interfacce tecniche per consentire ai clienti di richiedere la condivisione dei dati a norma dell'articolo 5, paragrafo 1; b) un modello per determinare il compenso massimo che il titolare dei dati ha il diritto di addebitare per la messa a disposizione dei dati; c) la responsabilità delle entità coinvolte nella messa a disposizione dei dati del cliente".*

iii. Il quadro normativo in materia di vigilanza, sanzioni e poteri della Commissione

Il Titolo VI del regolamento FIDA regola il quadro deli poteri di vigilanza e supervisione attribuito alle autorità nazionali competenti. L'articolo 17 prescrive che gli Stati membri designino le autorità nazionali competenti.

L'articolo 18 stabilisce invece disposizioni di dettaglio relative ai poteri delle autorità competenti; l'articolo 19 prevede la facoltà per gli Stati membri di stabilire norme che consentano alla autorità nazionale designata di stipulare accordi transattivi e di ricorrere a procedure di esecuzione accelerata nei confronti dei soggetti vigilati.

Gli articoli 20 e 21 meritano una menzione particolare dal momento che introducono sanzioni amministrative, nonché ulteriori misure e sanzioni in caso di reiterazione dell'inadempimento. L'applicazione delle sanzioni è rimessa, come di regola in ambito bancario-finanziario, alla competenza delle autorità competenti.

Le norme successive del Titolo VI prevedono, tra l'altro, le specifiche circostanze concrete che dovrebbero essere prese in considerazione dalle autorità competenti allorché siano chiamate ad emanare sanzioni amministrative nonché l'obbligo del segreto d'ufficio per gli scambi di informazioni tra autorità competenti.

Il Titolo VI contiene ulteriori norme sul diritto di impugnazione (art. 24) e sulla procedura prevista per la pubblicazione delle sanzioni amministrative e delle misure amministrative imposte (art. 25), nonché ulteriori norme relative allo scambio di informazioni tra autorità competenti (art. 26) e sulla risoluzione delle controversie tra di esse (art. 27).

Il Titolo VII prevede una procedura di notifica alle autorità nazionali competenti per le imprese che esercitano il diritto di stabilimento e di libera prestazione di servizi (articolo 28), nonché l'obbligo di comunicazione da parte delle autorità competenti quando adottano misure che comportano restrizioni alla libertà di stabilimento (articolo 29).

Infine, il Titolo VIII regola l'esercizio della delega laddove la Commissione debba adottare atti delegati in esecuzione di quanto previsto dal regolamento FIDA. Degno di nota, all'interno di tale Titolo, è l'articolo 30 che contiene la disciplina applicabile al caso in cui la Commissione sia chiamata ad adottare un atto delegato a norma dell'articolo 11 laddove, come previsto da questo articolo, non sia stato realizzato alcun sistema di condivisione dei dati finanziari entro un lasso di tempo ragionevole (successivo all'entrata in vigore del regolamento FIDA).

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CONSIL:ST_11220_2023_INIT

2023/3(5)TB

Il parere dell'EDPS del 22.8.2023 sulla proposta di regolamento europeo sull'accesso ai dati finanziari (FIDA)

In ossequio a quanto previsto dall'art. 42, par. 1 del Regolamento UE 2018/1725, la Commissione europea ha richiesto al Garante Europeo per la Protezione dei Dati ("**EDPS** o l'"**Autorità**") di esprimere un parere sulla proposta di regolamento relativo ad un quadro per l'accesso ai dati finanziari COM(2023) 360 final del 28.6.2023, di cui al contributo qui sopra [2023/3(4)BC] (la "**Proposta**"), alla luce del potenziale impatto delle disposizioni in essa contenute sulla protezione dei diritti e delle libertà delle persone fisiche cui i dati si riferiscono.

L'EDPS ha quindi emesso in data 22 agosto 2023 il Parere n. 38/2023 (il "**Parere**"), nel quale ha, da un lato, accolto positivamente la finalità della Proposta di consentire agli individui di avere maggior controllo e libertà di scelta sulle modalità di utilizzo dei loro dati e sulla selezione dei soggetti legittimati a tale utilizzo; dall'altro lato, l'Autorità ha evidenziato l'opportunità di apportare alcuni interventi correttivi al *draft* della Proposta in una prospettiva di mitigazione dei rischi per la protezione dei dati personali degli interessati.

Il primo profilo posto in rilievo nel Parere concerne la nozione di dati del cliente (*customer data)*, definiti nella proposta come i "*dati personali e non personali raccolti, conservati e altrimenti trattati da un ente finanziario nell'ambito della sua normale attività commerciale con i clienti, che comprendono sia i dati forniti dal cliente, sia i dati generati dall'interazione tra il cliente e l'istituzione finanziaria"* (Art.3, par. 1, n. 3 della Proposta).

Tale definizione è inclusiva di diverse categorie di dati specificamente incluse nel perimetro della Proposta, tra cui rientrano – a titolo esemplificativo – dati relativi a contratti di credito ipotecario, prestiti, conti, risparmi, investimenti in strumenti finanziari e prodotti assicurativi, fondi pensionistici e dati che fanno parte di valutazioni di merito creditizio, con l'esclusione di polizze assicurative sulla vita e prodotti assicurativi relativi a salute e malattie (Art. 2, par. 1 della Proposta).

Secondo l'Autorità, la definizione di *customer data* attualmente contenuta nella Proposta è eccessivamente ampia e non tiene conto della natura altamente sensibile di alcuni dei dati ricompresi nel perimetro di applicazione della stessa, che ricadono nella definizione di dati personali di categorie particolari ai sensi dell'art. 9, par. 1 del Regolamento EU 2016/679 ("**Regolamento generale sulla protezione dei dati personali**" o "**GDPR**"). Trattasi, ad esempio, di dati relativi alla salute rilevanti ai fini dell'erogazione di *benefit* previsti da determinati fondi pensionistici, o di dati ricompresi nelle valutazioni di rischio di credito al consumatore, che – ove combinati con dati relativi ad altri servizi finanziari, quali prodotti assicurativi o conti di pagamento – potrebbero dare luogo a discriminazioni ingiuste nei confronti degli individui.

Da ciò deriva – prosegue l'EDPS - la necessità di rimodulare la definizione di *customer data* e restringere le categorie di dati previste dalla Proposta, in ottemperanza al principio di minimizzazione dei dati che permea il GDPR, nonché l'opportunità di specificare in modo più chiaro l'esclusione dal perimetro di applicazione della Proposta dei dati ottenuti tramite processi di profilazione, inclusi i dati derivati o inferiti dai dati forniti dal cliente.

Sotto altro profilo, l'Autorità si sofferma poi sulla nozione di "permesso" da parte degli individui cui i dati di natura finanziaria si riferiscono, che gli utilizzatori devono ottenere per poter fare legittimamente uso di tali dati. Tale "permesso" – sottolinea l'EDPS – non coincide e non va confuso con il concetto di "consenso" inteso quale base giuridica del trattamento di dati personali ai sensi dell'art. 6, par. 1, lett. a) del GDPR, né tantomeno con la nozione di consenso esplicito ai sensi dell'art. 9, par. 2, n. 1 del GPDR.

Il "permesso" è infatti la condizione di legittimità che gli utilizzatori devono soddisfare per l'utilizzo dei dati di natura finanziaria ai sensi della Proposta, ma esso non costituisce allo stesso tempo la base giuridica del trattamento di dati personali ai sensi del GDPR, che i titolari del trattamento dovranno comunque individuare caso per caso a legittimazione delle operazioni di trattamento effettuate sui dati personali di natura finanziaria. Proprio per questa ragione, ed alla luce dell'ambiguità semantica tra i termini "permesso" e "consenso", l'EDPS raccomanda di aggiungere nel Considerando n. 48 della Proposta la specificazione che il permesso non dovrebbe essere interpretato come consenso o consenso esplicito o necessità per l'esecuzione di un contratto come definiti nel GDPR.

Tra gli ulteriori accorgimenti segnalati in una prospettiva di protezione dei dati personali degli interessati, vi sono poi diverse indicazioni relative ai pannelli di gestione delle autorizzazioni (*dashboard)* che i detentori dei dati devono mettere a disposizione degli utenti (Art. 5, par. 3, lett. d) della Proposta), cosicché questi ultimi possano monitorare e gestire i permessi forniti ai vari soggetti utilizzatori in un'ottica di maggiore trasparenza, controllo e granularità in relazione alle specifiche categorie di dati oggetto del permesso.

L'EDPS sottolinea che tali pannelli di gestione devono essere progettati in modo tale che gli utenti possano agire in modo informato, muniti di tutte le necessarie informazioni circa il trattamento dei loro dati personali ai sensi dell'art. 13 del GDPR, ed allo stesso tempo libero, in assenza di qualsiasi condizionamento o *deceptive pattern* che influenzi indebitamente le loro scelte.

Per scongiurare utilizzi abusivi dei pannelli di gestione da parte dei detentori dei dati, l'Autorità suggerisce inoltre l'inserimento di una previsione che impedisca agli stessi di vietare l'utilizzo dei servizi finanziari ai clienti che non installino e utilizzino i pannelli di gestione, o neghino la possibilità di condivisione dei dati con i soggetti utilizzatori.

Con riferimento alle richieste di accesso ed utilizzo dei dati finanziari da parte degli utilizzatori, l'EPDS raccomanda l'inclusione di un requisito di precisazione di quali tipologie dei dati sono oggetto della richiesta, con modalità e misure che siano adeguate, rilevanti e necessarie per i fini ed alle condizioni per cui il cliente ha dato il proprio permesso.

Il rispetto dei principi di minimizzazione, proporzionalità e necessità è poi nuovamente richiamato dall'EDPS nell'invocazione dell'inserimento di uno specifico riferimento alla necessità per gli utilizzatori dei dati di operare in conformità con le norme e linee guida applicabili in materia di accesso ed utilizzo dei dati personali: in questa prospettiva, l'Autorità raccomanda fortemente una consultazione formale dell'EDPB da parte dell'EBA (European Banking Authority) e dell'EIOPA (European Insurance and Occupational Pensions Authority), ossia le autorità cui la Proposta assegna la competenza a redigere le linee guida per l'applicazione della stessa.

In particolare, secondo l'EDPS, tali linee guida dovrebbero non soltanto concentrarsi sull'utilizzo dei dati ricompresi nel perimetro di applicazione della Proposta, ma prevedere altresì limiti e

modalità di combinazione tra essi e dati personali ottenuti da altre fonti, come quelli generati dall'utilizzo di nuove tecnologie, o condivisi da terze parti.

Per quanto concerne gli altri soggetti coinvolti dalla Proposta, l'EDPS si sofferma sugli obblighi posti a carico dei prestatori di servizi di informazione finanziaria ("**FISP**"), che – a seconda dei casi – possono agire come detentori o come utilizzatori dei dati. Il testo attuale della Proposta prevede che essi, prima di poter accedere ai dati dei clienti, debbano ottenere un'autorizzazione preventiva da parte dell'autorità competente; sul punto, l'EDPS raccomanda l'inclusione di una previsione che tale autorizzazione possa essere revocata qualora il FISP che l'abbia ottenuta sia destinatario di un provvedimento di una *data protection authority* che accerti la violazione di obblighi in materia di protezione dei dati personali da parte dello stesso FISP.

Sotto diverso profilo, alla luce dell'obbligo imposto dalla Proposta in capo a detentori ed utilizzatori dei dati di aderire a specifici sistemi di condivisione dei dati finanziari ("**FDSS**") (Art. 9, par. 1 della Proposta), l'Autorità raccomanda di inserire un obbligo di specificazione delle misure tecniche ed organizzative minime che i FDSS devono prevedere allo scopo di assicurare un livello appropriato di sicurezza per gli scambi di dati personali.

L'EDPS invita infine ad una stretta collaborazione tra tutte le autorità e le istituzioni coinvolte nel processo legislativo della Proposta e nell'emissione delle linee guida ad essa relative, specificando che le autorità di protezione dei dati personali ai sensi del GDPR vanno considerate tra le autorità pubbliche rilevanti che devono essere consultate nel contesto dell'elaborazione di tali linee guida.

TIMOTEO BUCCI

https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-08-22-edps-opinion-382023-regulation-framework-financial-data-access_en

2023/3(6)FDA

Le Linee guida AGID del 4.8.2023 sui dati aperti nel settore pubblico versione 1.0

Con la determinazione n. 183 del 4 agosto 2023 l'Agenzia per l'Italia Digitale ("**AgID**") – supportata da alcune regioni, enti di ricerca e amministrazioni centrali dello Stato – ha pubblicato la prima versione delle "*Linee Guida recanti regole tecniche per l'apertura dei dati e il riutilizzo dell'informazione del settore pubblico*" ai sensi dell'art. 12 del d.lgs. n. 36/2006 come modificato dal d.lgs. n. 200/2021 che ha recepito nell'ordinamento italiano la direttiva (UE) 2019/1024, cd. direttiva 'Open Data' (sul recepimento v. in questa Rubrica la notizia 2 del numero 1/2022: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf [2022/1(2)RA]).

Il documento intende supportare le pubbliche amministrazioni e gli altri soggetti interessati nel "*processo di apertura dei dati e di riutilizzo dell'informazione del settore pubblico*" attraverso indicazioni dirette ad attuare sul piano operativo le disposizioni di legge (p. 10). Esso introduce "*requisiti*" da "*implementare obbligatoriamente*" (p. 9) – in particolare quelli che attengono ai formati e alle modalità di pubblicazione dei dati di tipo aperto, alle richieste di riutilizzo, alle licenze, agli strumenti di ricerca – e altri aspetti di dettaglio qualificati come "*raccomandazioni*", ossia come "*forte suggerimento*" rivolto agli operatori di settore (p. 21).

Sul piano soggettivo le linee guida sono indirizzate alle seguenti categorie di enti: alle "*pubbliche amministrazioni*" incluse nell'art. 1, co. 2 del d.lgs. n. 165/2001; agli "*organismi di diritto pubblico*" di cui all'art. 3, co. 1, lett. d) del d.lgs. n. 50/2016; alle "*imprese pubbliche*" che operano nei settori speciali del codice degli appalti; alle "*imprese private*" incaricate di pubblici servizi (pp. 13-15). Invece sul piano oggettivo riguardano: tutti i dati e i documenti pubblici; i dati e i documenti intellettuali detenuti da biblioteche anche universitarie, musei e archivi; i dati della ricerca; i dati territoriali ai quali si applica il D.Lgs. 32/2010 di recepimento della direttiva 'INSPIRE' 2007/2/CE. Le esenzioni sono dettagliate al § 1.2 del medesimo documento.

È richiesto dall'AgID che tutti i dati pubblici coperti dalle linee guida siano leggibili meccanicamente; siano pubblicati in formato aperto e in modalità accessibile a costi marginali o gratuiti (cfr. anche § 6.2); siano provvisti di licenze standard e metadati (p. 29). La pubblicazione deve avvenire nel rispetto della normativa sulla privacy e può essere ritardata o esclusa solo in casi eccezionali e adeguatamente motivati dall'ente pubblico che implicherebbero "*difficoltà sproporzionate*" sul piano tecnico ed economico (p. 34). Regole specifiche sono dettate per la pubblicazione dei dati dinamici (§ 4.2); dei dati di elevato valore (§ 4.3); dei dati della ricerca (§ 4.4); dei dati territoriali (§ 4.5); dei metadati (§ 4.6).

Sul piano organizzativo le linee guida dell'AgID precisano che l'apertura dei dati pubblici deve

seguire un processo completo che non si deve limitare alla sola fase di pubblicazione, ma deve includere "*momenti continui di aggiornamento, monitoraggio e coinvolgimento degli utenti finali*" per saggiare l'impatto economico e sociale dei dati divulgati (p. 55). A tal fine spetta a ogni ente interessato individuare al proprio interno una singola figura o un gruppo di lavoro incaricato di curare le attività di apertura e di aggiornamento dei dati (p. 58).

I §§ 5.1.2 e seguenti delle linee guida descrivono il processo di apertura dei dati che può iniziare anche su impulso di soggetti esterni all'organizzazione dell'ente pubblico interessato. Esso comincia con la preliminare "*ricognizione dei dati detenuti e trattati dall'ente*" (p. 60); prosegue con la "*analisi giuridica delle fonti del dato*" volta ad accertare l'esistenza di eventuali limiti d'uso e di circolazione (p. 62); continua con le necessarie operazioni di manutenzione qualitativa e di modellazione del dato per migliorarne la fruizione (pp. 67-70); termina con la validazione del contenuto del dato e con la sua pubblicazione (p. 74). Ciascuna delle fasi descritte concorre a garantire il rispetto di quattro principi basilari che sono l'accuratezza, la coerenza, la completezza e l'attualità del dato divulgato (p. 80).

La diffusione dei dati al pubblico deve avvenire senza restrizioni di sorta (salvo quelle giustificate da oggettive e non sproporzionate ragioni di interesse generale), utilizzando licenze riconosciute e validate a livello internazionale da organismi tecnici di certificazione (p. 91; all. B). Opportunamente le linee guida precisano che l'apertura dei dati pubblici deve osservare il principio di non discriminazione e di regola devono essere esclusi o comunque fortemente limitati nel tempo eventuali "*accordi di esclusiva*" che conferiscano diritti speciali di utilizzo dei dati a determinate categorie di soggetti privati (§ 6.4).

Da ultimo le linee guida dell'AgID hanno cura di precisare che ciascun soggetto tenuto ad applicare la normativa di settore sull'apertura dei dati pubblici deve "*pubblicare e aggiornare annualmente nei propri siti istituzionali gli elenchi delle categorie di dati detenuti ai fini del riutilizzo attraverso collegamenti ipertestuali al portale nazionale dati.gov.it*" (p. 118).

FILIPPO D'ANGELO

https://www.agid.gov.it/sites/default/files/repository_files/lg-open-data_v.1.0_1.pdf

2023/3(**7**)CAT

La sentenza CGUE del 4.7.2023 nel caso C-252/21 sui rapporti tra privacy e antitrust, sulla pubblicità dei dati sensibili e sulla inadeguatezza della base del legittimo interesse per il trattamento dei dati inerenti la pubblicità comportamentale di Meta (sentenza Meta abuso di posizione dominante)

Il 4 Luglio 2023, la Corte di Giustizia dell'Unione Europea (CGUE), riunita in Grande Sezione nella causa C-252/21 si è pronunciata sul rinvio pregiudiziale presentato nell'ambito di una controversia tra *Meta Platforms Inc*. e il *Bundeskartellamt* (Autorità federale garante della concorrenza, Germania) in merito alla decisione di quest'ultimo di vietare a Meta di subordinare, tramite le condizioni generali, l'utilizzo di Facebook da parte di utenti privati residenti in Germania al trattamento dei loro dati personali per finalità di pubblicità personalizzata, procedendo a tali operazioni senza il loro consenso. Inoltre, tale Autorità ha sottolineato che un siffatto consenso non sarebbe comunque valido, in quanto costituirebbe uno sfruttamento abusivo della posizione dominante di Meta sul mercato tedesco.

Meta ha presentato un ricorso dinanzi all'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf, Germania), sollevando alcune questioni inerenti, da un lato, la possibilità per le Autorità garanti della concorrenza di verificare e pronunciarsi sulla conformità di un trattamento di dati personali ai requisiti stabiliti nel Regolamento (UE) 679/2016 (GDPR) e, dall'altro, l'interpretazione e l'applicazione di talune disposizioni di detto regolamento.

Allo scopo di dirimere tali questioni, Il Tribunale superiore ha adito la CGUE in via pregiudiziale. In particolare, sono state rinviate alla CGUE le seguenti questioni:

a) se sia compatibile con gli articoli 51 e ss. del GDPR il fatto che un'Autorità diversa da quella competente a garantire un controllo sulla liceità e correttezza dei trattamenti di dati personali rilevi, nell'ambito di una verifica sull'eventuale abuso di posizione dominante di un operatore, che le condizioni contrattuali applicate dallo stesso violino il GDPR, imponendo la conseguente regolarizzazione di tali violazioni.
b) se debbano considerarsi categorie particolari di dati personali ai sensi dell'articolo 9 del GDPR quelli raccolti da Meta all'accesso e durante l'utilizzo, da parte dell'interessato, di siti e app (ad esempio, di incontri, di partiti politici o

relativi alla salute) e successivamente ricollegati all'account di quest'ultimo, nonché, in caso affermativo, se l'accesso a tali siti e app e/o l'inserimento di dati e/o l'attivazione di pulsanti ("plug-in social" come "Mi piace", "Condividi" o "Facebook Login" o "Account Kit") costituiscano una modalità di rendere manifestamente pubblici i dati relativi all'accesso di per sé e/o i dati immessi da parte dell'utente, ai sensi dell'articolo 9, paragrafo 2, lettera e), del GDPR e, pertanto, rendano ex se lecito tale trattamento;

c) se Meta possa utilizzare le basi giuridiche del contratto (articolo 6, par. 1, lett. b) GDPR) o del legittimo interesse (articolo 6, par. 1, lett. f) GDPR), dell'obbligo di legge articolo 6, par. 1, lett. c) GDPR e della salvaguardia di un interesse vitale o pubblico (articolo 6, par. 1, lett. d) ed e) GDPR) per effettuare pubblicità personalizzata sui propri utenti;

d) se, accertato l'abuso di posizione dominante di un'impresa, possa essere considerato valido, e in particolare libero, il consenso al trattamento dei propri dati personali espresso da un utente nei confronti di tale titolare.

La CGUE si è pronunciata sulle suddette questioni come segue

a) Con riferimento al riparto di competenze tra Autorità privacy e antitrust, fermo restando il rispetto dell'obbligo di leale cooperazione, un Garante della concorrenza di uno Stato membro può constatare, nell'ambito dell'esame di un abuso di posizione dominante da parte di un'impresa, ai sensi dell'art. 102 TFUE, che le condizioni generali d'uso di tale impresa relative al trattamento dei dati personali e la loro applicazione non sono conformi al GDPR, qualora la constatazione sia necessaria per accertare l'esistenza dell'abuso, dunque della violazione di sua competenza.

Tuttavia, l'Autorità della concorrenza non può discostarsi da una decisione di quella privacy che riguardi tali condizioni generali e, in ogni caso, anche in assenza di un'indagine o di una decisione di detta Autorità, qualora ritenga che le condizioni in questione non siano conformi al GDPR, ha il dovere di consultare l'Autorità di controllo privacy e chiederne la cooperazione, al fine di determinare se si debba attendere l'adozione di una sua decisione prima di iniziare la propria valutazione. In assenza di obiezioni o di risposta entro un termine ragionevole, l'Autorità antitrust può proseguire la propria indagine.

b) L'articolo 9, paragrafo 1, del GDPR deve essere interpretato nel senso che: nel caso in cui un utente di un social network consulti siti o applicazioni correlati a una o più delle categorie menzionate da tale disposizione e, se del caso, inserisca in essi dati, iscrivendosi oppure effettuando ordini online, il trattamento di tali dati deve essere considerato un «trattamento di categorie particolari di dati personali», il quale è in linea di principio vietato, fatte salve le deroghe previste dal paragrafo 2 dello stesso articolo 9 del GDPR.

Inoltre, la semplice consultazione di siti o applicazioni correlati a una o più categorie particolari non equivale a rendere manifestamente pubblici i relativi dati. Infine, quando inserisce informazioni in tali siti o applicazioni nonché quando attiva pulsanti di selezione integrati in questi ultimi (es. «Mi piace» o «Condividi»), tale utente rende manifestamente pubblici, ai sensi di detto articolo 9, paragrafo 2, lettera e), del GDPR, i dati così inseriti o risultanti dall'attivazione di tali pulsanti soltanto se abbia esplicitamente espresso preliminarmente la sua scelta di rendere i dati che lo riguardano pubblicamente accessibili a un numero illimitato di persone.

c) L'articolo 6, paragrafo 1, primo comma, lettera b) (base giuridica del contratto) del GDPR deve essere interpretato nel senso che: il trattamento di dati personali effettuato da Meta, consistente nella profilazione a fini pubblicitari dell'utente, può essere considerato necessario per l'esecuzione di un contratto del quale gli interessati sono parti solo a condizione che detto trattamento sia oggettivamente indispensabile per realizzare una finalità che costituisce parte integrante della prestazione contrattuale destinata a quegli stessi utenti, cosicché l'oggetto principale del contratto non potrebbe essere conseguito in assenza di tale trattamento.

Il fatto che il trattamento sia menzionato nel contratto oppure che esso sia soltanto utile per la sua esecuzione è, di per sé, irrilevante. Infatti, l'elemento determinante ai fini dell'applicazione di tale base giuridica è che il trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra quest'ultimo e l'interessato e, pertanto, che non esistano altre soluzioni percorribili e meno invasive.

L'articolo 6, paragrafo 1, primo comma, lettera f) (base giuridica del legittimo interesse) del GDPR può essere considerata una base giuridica idonea per la pubblicità profilata solo se: il titolare del trattamento abbia precisamente informato gli interessati in merito al legittimo interesse, tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di suddetto interesse e il contemperamento delle

contrapposte pretese non comporti una prevalenza delle libertà e dei diritti fondamentali di tali utenti che richiedano la protezione dei dati personali, sul legittimo interesse del titolare.

Ne deriva che, nel caso concreto, né il contratto, né il legittimo interesse (né tantomeno l'obbligo legale o l'interesse vitale) possano essere considerati basi giuridiche idonee ai fini della pubblicità personalizzata operata da Meta.

d) L'articolo 6, paragrafo 1, primo comma, lettera a), e l'articolo 9, paragrafo 2, lettera a) (consenso dell'interessato) del GDPR devono essere interpretati nel senso che: la circostanza che l'operatore di un social network occupi una posizione dominante sul mercato non osta, di per sé, a che gli utenti di tale social possano validamente acconsentire al trattamento dei loro dati personali. Tale circostanza costituisce nondimeno un elemento importante per determinare se il consenso sia stato effettivamente prestato validamente e, in particolare, liberamente, circostanza che spetta a detto operatore dimostrare.

La pronuncia della CGUE ha statuito una serie di principi di grande importanza e, a parere di chi scrive, non privi di criticità. Se da un lato, infatti, la Corte ha affrontato in modo deciso il riparto di competenze tra Autorità indipendenti, adottando una soluzione flessibile che non impedisce, da parte dell'antitrust, l'analisi in sede di istruttoria di questioni utili alla risoluzione del caso concreto imponendo tuttavia una cooperazione con l'Autorità privacy, dall'altro ha finito, seppur indirettamente, per delineare un vero e proprio modello di business che Meta avrebbe dovuto adottare, quello del consenso, salvo poi affermare che lo stesso non può, nel caso concreto, ritenersi liberamente prestato e, dunque, valido. In tal senso, permangono alcuni dubbi sul contemperamento effettuato dall'organo giudicante tra principi fondamentali e, in particolare, su quanto sia stato salvaguardato il diritto alla libertà d'impresa sancito dall'articolo 16 della Carta di Nizza. Merita, peraltro, di essere osservato che la CGUE sembra riproporre una visione "consenso-centrica" (parzialmente anacronistica) tenendo in scarsa considerazione le altre basi giuridiche (paragrafi 91 e 92 della sentenza).

Fatta questa premessa, va ricordato che, perlomeno per quanto riguarda la pronuncia di non idoneità della base giuridica del contratto ai fini della pubblicità personalizzata nel caso di specie, la CGUE si è limitata, come dovuto, ad esprimere un giudizio sul caso concreto analizzando le argomentazioni fornite dal titolare del trattamento. Meta si è difesa affermando che la pubblicità personalizzata era necessaria per offrire il servizio di social network. Come noto, l'articolo 6, paragrafo 1, lett. b) del GDPR prevede che il trattamento è lecito se "*è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*". La CGUE ha rilevato, come precedentemente fatto sia dall'EDPB che dall'Autorità privacy irlandese (sulle relative pronunce v. in questa Rubrica la notizia 6 nel numero 2023/1 [2023/1(6)GDI]: http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf), che il servizio di social network è autonomo e può essere materialmente fruito indipendentemente dalla pubblicità personalizzata. Tutt'al più, secondo la CGUE l'attività promozionale potrà dirsi utile, ma non oggettivamente indispensabile per l'erogazione del servizio. Ne consegue che il contratto non si configura come idonea base giuridica per la pubblicità personalizzata nel caso oggetto di trattazione. Resta, ad oggi, la curiosità sull'esito di questa e di altre controversie laddove Meta fosse stata più coraggiosa e avesse sostenuto che la pubblicità personalizzata non era tanto necessaria a rendere il servizio di social network, bensì (come in realtà è evidente) a finanziarlo grazie agli introiti che riceve da chi paga la pubblicità, configurandosi in sostanza come vera e propria controprestazione del sinallagma contrattuale. È chiaro che ciò non sia avvenuto in quanto il colosso statunitense non ha voluto mettersi nella posizione di autoproporre il mutamento del proprio modello di business. In tal caso, infatti, nella migliore delle ipotesi e sul modello dei *pay-wall*, avrebbe dovuto quantomeno offrire un'alternativa di fruizione del social a pagamento oltre a quella surrettiziamente gratuita e finanziata tramite la pubblicità personalizzata. In tal senso, tuttavia, non si registra una chiusura di principio da parte del giudice europeo al contratto quale base giuridica per la pubblicità personalizzata.

CARMINE ANDREA TROVATO

CURIA - Documenti (europa.eu)

2023/3(8)GDI

Il provvedimento del 14.7.2023 del Garante norvegese per la protezione dei dati personali sulla base del legittimo interesse per la pubblicità comportamentale di Meta

Con provvedimento d'urgenza del 14 luglio 2023, l'Autorità di controllo norvegese in materia di protezione dei dati personali (**Datatilsynet**) ha temporaneamente vietato a Meta di profilare gli utenti dei suoi servizi Facebook e Instagram per fini di pubblicità comportamentale (*behavioural advertising*).

È, questa, solo l'ultima tappa di un contenzioso che ha visto contrapposta la nota piattaforma digitale americana alle istituzioni europee con riferimento al corretto trattamento di dati personali per finalità di pubblicità personalizzata.

Infatti, con due provvedimenti del 31 dicembre 2022, contro i servizi Facebook e Instagram, e uno del 12 gennaio 2023, contro il servizio WhatsApp, l'Autorità di controllo irlandese (**DPC**), su parere vincolante del 5 dicembre 2022 del Comitato europeo per la protezione dei dati personali (**EDPB**), aveva censurato la scelta di Meta di sostituire il consenso dell'interessato *ex* art. 6(1)(a) del Regolamento UE 2016/679 (**GDPR**, in seguito anche il "**Regolamento**") con il contratto *ex* art. 6(1)(b) dello stesso Regolamento quale base giuridica della pubblicità comportamentale. Conseguentemente aveva sanzionato Meta per un totale di 396 milioni di euro per la violazione degli artt. 5(1)(a), 6(1)(b), 12(1) e 13(1)(c) del Regolamento (sul punto v. in questa Rubrica la notizia 6 nel numero 2023/1 [2023/1(6)GDI]: http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf).

La pronuncia si era subito imposta all'attenzione dei fornitori di servizi digitali per le conclusioni che se ne traevano in materia di pubblicità personalizzata online, ossia la principale fonte di remunerazione per le piattaforme digitali, centrale nei modelli di business per l'offerta dei servizi cc.dd. "a prezzo zero". L'aver dichiarato illecito il ricorso al contratto quale base giuridica della profilazione degli utenti per fini commerciali, infatti, è suscettibile di mettere in crisi tale modello di business nella misura in cui rende meno sicura o certa la possibilità di abilitare la forma più remunerativa (e invasiva) di pubblicità personalizzata: la pubblicità comportamentale.

In altre parole, la scelta della base giuridica contrattuale per la profilazione per fini pubblicitari è strategica, non solo per Meta ma per la gran parte delle piattaforme digitali, perché permette di inserire tale trattamento tra le condizioni negoziali del servizio, sottraendo così all'utente la possibilità di esprimere il proprio consenso (e la relativa, eventuale, revoca) in merito. La pronuncia della DPC ha rimosso l'automatismo sotteso al considerare la pubblicità comportamentale un elemento necessario alla fornitura del servizio, in quanto tale oggetto di una clausola contrattuale non negoziabile.

La DPC aveva inoltre concesso a Meta tre mesi di tempo per adeguare i suoi trattamenti alle norme del GDPR e comunicare come intendesse applicare l'art. 6 del Regolamento. Si chiedeva, dunque, a Meta di individuare un'altra base giuridica, tra quelle previste dall'art. 6 GDPR, per la pubblicità comportamentale.

In considerazione di tale pronuncia, Meta ha informato che, a partire dal 5 aprile 2023, avrebbe svolto la pubblicità comportamentale non più sulla base del contratto *ex* art. 6(1)(b) GDPR ma sulla base di un proprio legittimo interesse *ex* art. 6(1)(f) GDPR. Il risultato pratico di questa scelta è che, anche in questo caso, nessun consenso è chiesto all'utente sulla profilazione per fini pubblicitari ma a questo è riconosciuta la sola possibilità di esercitare il diritto di opporsi al trattamento, *ex* art. 21 del Regolamento, in un secondo momento, ossia solo dopo che è iniziato il trattamento (c.d. opt-out).

Nel ritenere tale proposta non in linea con la normativa, in data 5 maggio 2023, la Datatilsynet aveva formalmente chiesto alla DPC di vietare a Meta il trattamento di dati personali degli utenti per finalità di pubblicità comportamentale ma l'autorità irlandese, in data 2 giugno 2023, ha ritenuto di non poter aderire a tale richiesta.

Successivamente, con sentenza del 4 luglio 2023, la Corte di Giustizia dell'Unione Europea, nel caso C-252/21 *Facebook Inc. and Others v. Bundeskartellamnt*, in sede di rinvio pregiudiziale, nel riconoscere la possibilità per le autorità nazionali per la concorrenza di applicare, in via incidentale, il GDPR, si è espressa anche su alcuni istituti del medesimo Regolamento. Per quanto qui di interesse, la Corte ha ritenuto che Meta non potesse ricorrere al legittimo interesse di cui all'art. 6(1)(f) GDPR quale base giuridica per la pubblicità personalizzata (v. *amplius* la notizia 8 qui sopra in questo numero della Rubrica [2023/3(8)CAT]).

Proprio questa sentenza è stata interpretata dall'Autorità di controllo norvegese come un ulteriore elemento a sostegno del perdurante mancato adempimento di Meta alla normativa in materia di *data protection*.

Nel considerare rilevanti e serie le violazioni attribuite a Meta dalla decisione della DPC, la Datatilsynet ha ritenuto che il persistente stato di non conformità dei servizi di Meta richiedesse un'azione immediata a tutela dei diritti degli interessati, spesso ignari della presenza, delle caratteristiche e dell'intrusività di simili trattamenti.

La Datatilsynet è così intervenuta in via d'urgenza *ex* art. 66(1) del Regolamento, derogando alla procedura di cooperazione tra Autorità capofila e

Autorità interessate di cui agli artt. 60 e ss del Regolamento.
Nel merito, anche in considerazione delle evidenze contenute nella citata sentenza della Corte di giustizia del 4 luglio 2023, la Datatilsynet ha giudicato errate le valutazioni di Meta sulla possibilità di ricorrere al legittimo interesse. In presenza di altri e meno invasivi sistemi per generare profitto, non si è ritenuto soddisfatto il criterio della necessità del trattamento. Soprattutto, in considerazione delle circostanze concrete e della scarsa consapevolezza fornita agli interessati su tali trattamenti, ha ritenuto non soddisfatto il requisito del c.d. "*balancing test*": l'interesse di Meta a svolgere quel trattamento non è superiore agli interessi e ai diritti degli utenti a non subire trattamenti così invasivi. Secondo l'autorità norvegese: «è responsabilità di Meta progettare un modello di business che sia, al tempo stesso, lecito e sostenibile».
Infine, ulteriore elemento di illiceità è rinvenuto nella non adeguata attuazione e riconoscimento agli interessati del diritto all'opposizione. Secondo l'autorità norvegese Meta ha introdotto restrizioni illecite alla possibilità dell'utente di opporsi alla pubblicità comportamentale.
In conclusione, oltre al mancato adeguamento alla pronuncia della DPC, la Datatilsynet rileva la violazione degli artt. 6(1) e 21 del Regolamento.
Conseguentemente, ha rivolto a Meta l'ordine, temporaneo e limitato al territorio della Norvegia, di non trattare i dati dei cittadini norvegesi per fini di pubblicità comportamentale ai sensi degli artt. 6(1)(b) e 6(1)(f) del Regolamento, ossia sulla base del contratto e del legittimo interesse.
La Datatilsynet specifica che ad essere vietato è il trattamento dei dati relativi al comportamento degli utenti per fini pubblicitari, non anche la possibilità di Meta di mostrare annunci pubblicitari in generale o annunci pubblicitari basati sulle informazioni direttamente fornite dagli utenti sul proprio profilo, come le informazioni contenute nella biografia quali età, sesso, residenza o studi effettuati.
Meta potrà quindi continuare a offrire i propri servizi e accompagnarli con pubblicità generalista o profilata purché su dati direttamente forniti agli utenti. Quel che Meta non potrà fare sarà continuare a profilare gli utenti sulla base dei loro comportamenti desunti e inferiti dall'utilizzo della piattaforma (per es. dall'interazione coi contenuti sulla piattaforma o dai movimenti dell'utente ricavati della geolocalizzazione) sulla base di fondamenti di liceità dichiarati non adeguati: in particolare il contratto e il legittimo interesse.
Essendo un provvedimento d'urgenza, il divieto è limitato a un periodo di tre mesi, dal 4 agosto 2023 al 3 novembre 2023, salva la possibilità per Meta di attivarsi per rendere lecito il trattamento prima di questo termine con conseguente revoca dell'ordine.
In base all'art. 66(1) del Regolamento, il provvedimento è stato notificato alle altre Autorità di controllo europee, alla Commissione UE, all'EDPB e, ai sensi della normativa interna, all'autorità di sorveglianza EFTA. Conseguentemente, ai sensi dell'art. 66(2) del Regolamento, la Datatilsynet richiede una decisione urgente e vincolante da parte dell'EDPB per l'adozione di misure definitive e riguardanti l'intero territorio europeo.
Infine, la Datatilsynet ha disposto una sanzione amministrativa di 1.000.000 NOK per ogni giorno di ritardo di Meta nel conformarsi all'ordine imposto.

GUIDO D'IPPOLITO

https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/temporary-ban-of-behavioural-advertising-on-facebook-and-instagram/

2023/3(9)EB

La sentenza CEDU del 4.7.2023 sul diritto all'oblio (caso 57292/16 Hurbain c. Belgio)

Il 4 luglio 2023 la Grande Camera della Corte europea dei diritti dell'uomo, si è pronunciata sull'annosa questione del diritto all'oblio e del suo bilanciamento con il diritto alla libertà di espressione e di informazione, confermando quanto deciso sullo stesso ricorso (n. 57292/16 Hurbain contro Belgio) dalla Terza sezione il 22 giugno 2021.
Il caso trae origine dal ricorso alla Corte EDU, ai sensi dell'articolo 34 della Convenzione e.d.u. (di seguito anche, "**Convenzione**"), da parte di Patrick Hurbain, editore del quotidiano belga Le Soir, contro il Belgio.
Nel merito, la controversia origina dalla pubblicazione, nel 1994, di un articolo sulla versione cartacea del giornale Le Soir, riportante la notizia di un incidente automobilistico che aveva causato la morte di due persone e il ferimento di altre tre. L'articolo menzionava il nome completo del conducente, che era stato condannato nel 2000. Questi aveva scontato la pena ed aveva ottenuto la riabilitazione nel 2006.

Nel 2008 il giornale aveva creato una versione elettronica dei suoi archivi dal 1989 in poi - tra cui era inserito l'articolo sopra citato -, che era diventato disponibile gratuitamente sul sito web del quotidiano. Nel 2010 il conducente dell'auto si era rivolto a Le Soir, chiedendo la cancellazione dell'articolo dagli archivi elettronici del quotidiano o quantomeno la sua anonimizzazione. La richiesta originava dal fatto che digitando sui diversi motori di ricerca il nome del conducente, il link all'articolo appariva in primo piano, creando un vero e proprio "registro penale virtuale", particolarmente pregiudizievole per il cittadino che aveva ormai da molti anni scontato la pena e ottenuto la riabilitazione.

L'interessato aveva dunque adito le competenti autorità giudiziarie per ottenere la tutela del suo "diritto ad essere dimenticato", contro il rifiuto del quotidiano ad adempiere spontaneamente. Tale adempimento fu imposto dalle sentenze di condanna pronunciate in tutti i gradi di giudizio, che hanno intimato l'anonimizzazione del nome dell'Interessato dalla versione online dell'articolo. In particolare, è stato ritenuto che la sostituzione del nome dell'interessato con la lettera "X" dalla sola versione online del giornale, restando impregiudicata sia la notizia che la versione cartacea dell'articolo, garantisse un equo bilanciamento tra diritti parimenti meritevoli di tutela: diritto all'oblio e libertà di espressione ed informazione.

Avverso tale decisione aveva presentato ricorso alla Corte EDU l'editore del giornale, il sig. Hurbain, per violazione dell'articolo 10 della Convezione, ottenendo però una sostanziale conferma delle decisioni delle autorità giudiziarie nazionali e dunque la legittimità della misura disposta, conforme ai principi di cui all'articolo 10 della Convenzione.

La Grande Camera ha ritenuto legittima la decisione delle autorità giudiziarie belghe, prima e della Terza sezione, poi, di richiedere all'editore di rendere anonimo l'articolo in questione.

La Corte osserva che i tribunali nazionali hanno preso in considerazione in modo coerente la natura e la gravità dei fatti giudiziari riportati nell'articolo cui si aggiunge il fatto che quanto riportato non aveva alcun interesse attuale, storico o scientifico e il fatto che l'interessato non fosse una persona nota. Inoltre, è stata data importanza al grave danno subito all'onore e alla reputazione dell'interessato a causa della continuata disponibilità online dell'articolo con accesso illimitato, il che poteva creare un "registro penale virtuale", specialmente alla luce del tempo trascorso dalla pubblicazione originale dell'articolo. In ultimo, dopo aver esaminato le misure che potevano essere prese in considerazione al fine di bilanciare i diritti in gioco, ha riconosciuto come l'anonimizzazione dell'articolo non impone un onere eccessivo ed impraticabile per il richiedente, costituendo nel contempo il mezzo più efficace per proteggere la privacy dell'interessato.

In tali circostanze, e tenuto conto del margine di apprezzamento degli Stati, la Corte ha ritenuto che i tribunali nazionali abbiano bilanciato attentamente i diritti in gioco in conformità ai requisiti della Convenzione, in modo tale che l'interferenza con il diritto garantito dall'articolo 10 della Convenzione a causa dell'anonimizzazione della versione elettronica dell'articolo sul sito web del giornale Le Soir sia stata limitata a quanto strettamente necessario e possa quindi, nelle circostanze del caso, essere considerata adeguata e proporzionata in una società democratica. Pertanto, la Corte non vede ragioni valide per sostituire la propria opinione con quella dei tribunali nazionali e per ignorare l'esito dell'esercizio di bilanciamento da loro effettuato.

Questa pronuncia risulta rilevante per le sue ricadute nell'ordinamento italiano ed europeo, la cui giurisprudenza spesso si occupa di diritto all'oblio e il suo bilanciamento con il diritto di informazione, concludendo però per la diversa misura della deindicizzazione.

A ben vedere, le conclusioni della Gran Camera, nell'interpretazione dei principi della Convenzione, non si pongono necessariamente in contrasto con la giurisprudenza eurounitaria consolidata. Difatti, a norma dell'art. 17, comma 3, lett. a) GDPR, l'esercizio della libertà di espressione e di informazione costituisce una delle eccezioni che consentono di escludere l'esercizio del diritto all'oblio, rendendo necessaria un'analisi svolta caso per caso e volta a valutare la prevalenza dell'uno o dell'altro nelle circostanze concrete (es. l'interessato è un personaggio pubblico, i fatti riportati sono inaccurati etc.). Questa valutazione *ad hoc*, anche alla luce dell'interpretazione datane dalla giurisprudenza, ammette, fra le misure che ne permettono la piena attuazione, oltre alla deindicizzazione, l'anonimizzazione dei dati e la loro esatta contestualizzazione.

Inoltre la Gran Camera nel bilanciamento tra diritti meritevoli di tutela, prende in considerazione grosso modo dei parametri non dissimili da quelli che la CGUE ha riconosciuto nella sentenza Costeja (Causa C-131/12) e ha ripetuto nella sentenza Google 2 (Causa C-136/17): (i) la natura dell'informazione o il suo carattere sensibile; (ii) l'interesse degli utenti di Internet ad avere accesso

all'informazione; (iii) il ruolo che l'interessato riveste nella vita pubblica.
Infine, ed è una precisazione rilevante, la Gran Camera ha sottolineato come non sussista un obbligo automatico di sorveglianza per i media, di controllare sistematicamente e permanentemente i propri archivi, ma tale obbligo di attivarsi per garantire un giusto equilibrio degli interessi in gioco conseguirebbe solo ad una espressa richiesta dell'interessato.
Incidenter tantum, giova ricordare come in Italia la recente Riforma Cartabia (D.lgs. 150 del 2022) abbia introdotto tra le disposizioni di attuazione del codice di procedura penale l'art. 64-*ter*, rubricato «Diritto all'oblio degli imputati e delle persone sottoposte ad indagini», sul cui schema si era pronunciato il Garante per la protezione dei dati personali con parere del 1 settembre 2022. Sul punto v. in questa Rubrica la notizia 2 nel numero 2023/1 [2023/1(6)SM]: http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf.

EMANUELA BURGIO

https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%224%20luglio%2057292/16,%20Hurbain%20contro%20Belgio%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-225546%22]}

2023/3(10)IG

La decisione vincolante EDPB 2/2023 del 2.8.2023 e la conseguente decisione finale del Garante irlandese per la protezione dei dati personali del 1.9.2023 su c.d. dark (o deceptive design) patterns e altre pratiche riguardanti i bambini e la verifica dell'età poste in essere da TikTok

Il 1 settembre 2023, la Commissione per la Protezione dei dati irlandese (**DPC**), ha disposto nei confronti di TikTok Technology Limited (**TTL**) – la cui sede europea è situata in Irlanda - sanzioni amministrative per un totale di 345 milioni di euro, unitamente ad una nota di biasimo, ai sensi dell'articolo 58, paragrafo 2, lettera b), del Regolamento (UE) 679/2016 (**GDPR**), e all'ordine di adottare, entro tre mesi dalla notifica della decisione, le misure per garantire la conformità del trattamento dei dati personali al GDPR, come indicate nella decisione.

Il provvedimento, ai sensi dell'art. 111 del Data Protection Act irlandese del 2018 e degli artt. 60 e 65 del GDPR, riflette la decisione vincolante dello European Data Protection Board (**EDPB**), adottata in conformità all'art. 65(1) lett. a) GDPR, per la risoluzione della controversia sorta in merito a una bozza di decisione della stessa DPC, che aveva suscitato obiezioni da parte di altre autorità europee per la privacy, fra le quali l'autorità di controllo italiana. La (bozza di) decisione era stata adottata a seguito di un'indagine avviata dalla stessa autorità irlandese per esaminare il trattamento da parte di TTL dei dati personali degli utenti minori (di età compresa fra i 13 e i 17 anni) registrati sulla piattaforma Tik Tok, nel periodo compreso fra il 31 luglio e il 31 dicembre 2020 e per valutare se TTL avesse o meno rispettato gli obblighi previsti dal GDPR, in qualità di titolare del trattamento.
Durante l'indagine, sono emerse problematiche riguardanti la chiarezza e la trasparenza delle informazioni fornite da TTL agli utenti minorenni riguardo alle impostazioni predefinite dell'account e alla visibilità dei contenuti pubblicati, che, secondo l'Autorità irlandese avrebbero condotto a una presunta violazione del GDPR sotto vari profili di cui si è dato atto nella bozza di decisione.
Le questioni principali successivamente analizzate da EDPB, chiamata a valutare il merito delle obiezioni sollevate dalle autorità di controllo alla bozza di decisione della DPC, si sono incentrate essenzialmente su: 1) la possibile ulteriore violazione del principio di correttezza ai sensi dell'art. 5, par. 1, lett. a) del GDPR; 2) la possibile violazione dell'art 24, paragrafo 1, e dell'articolo 25, par 1 e 2, GDPR in relazione alle misure di verifica dell'età dei minori di 13 anni e alla valutazione dei rischi per questa specifica categoria di interessati.
In relazione alla prima questione, l'EDPB ha esaminato le pratiche relative alla registrazione degli utenti e alla pubblicazione dei video. Durante il periodo preso in considerazione, sono emerse carenze significative in termini di trasparenza e di fornitura di informazioni adeguate riguardo alla visibilità dei contenuti pubblicati e alla loro accessibilità a un pubblico più ampio. In particolare, durante la fase di registrazione, agli utenti veniva presentato un pop-up di notifica che, nonostante spiegasse la possibilità di impostare l'account come privato, consentiva loro effettivamente di "saltare" questa opzione, rendendo l'account pubblico per impostazione predefinita, con evidenti gravi implicazioni per la privacy dei minori sulla piattaforma. Inoltre, nella 'Notifica di Pubblicazione' dei video, i minori venivano

incoraggiati a pubblicare i video 'pubblicamente'. L'opzione 'Pubblica ora' era posizionata in modo prominente a destra e presentata in grassetto più scuro, aumentando così la probabilità che l'utente optasse per questa scelta.
Inoltre, accogliendo le obiezioni presentate dalle altre autorità di controllo, l'EDPB ha anche individuato una violazione da parte di TTL del principio di correttezza, ai sensi dell'art. 5(1) lett. a) GDPR per aver utilizzato, sia nei pop-up di registrazione, sia nei pop-up di pubblicazione, modelli c.d. oscuri ("*dark patterns*" o "*deceptive design patterns*") al fine di influenzare le decisioni degli utenti minorenni. Di conseguenza, l'EDPB ha incaricato l'Autorità irlandese di includere nella sua decisione finale una constatazione di violazione del principio di correttezza, ai sensi dell'art. 5(1) lett. a) GDPR, da parte di TTL, al fine di eliminare i modelli di progettazione ingannevoli come identificati nella decisione vincolante dello EDPB.
Con riguardo alla questione relativa alla possibile violazione degli artt. 24 e 25 GDPR in relazione alle misure di verifica dell'età dei minori di 13 anni e alla valutazione dei rischi per questa specifica categoria di interessati, l'EDPB ritiene che l'obiezione dell'autorità di controllo italiana in merito all'esistenza della violazione dell'art. 25 GDPR sia pertinente e motivata ai sensi della definizione di cui all'art. 4, n. 24 GDPR, esprimendo seri dubbi sull'efficacia delle misure di verifica dell'età messe in atto da TikTok durante questo periodo; in particolare i dubbi sono giustificati dalla gravità dei rischi di violazione dei diritti fondamentali delle persone, per l'elevato numero di minori di età inferiore ai 13 anni coinvolti, nonché dalla mancata identificazione da parte di TTL, nella valutazione di impatto (come viene rilevato nella bozza di decisione) del rischio che i minori di età inferiore ai 13 anni accedano alla piattaforma TikTok.
Tuttavia, nella decisione vincolante, l'EDPB non prende posizione in merito alla questione della verifica materiale dell'età. Nella decisione infatti si legge che non disponendosi di informazioni sufficienti, in particolare in relazione all'elemento dello stato dell'arte, per valutare in modo definitivo la conformità di TTL all'art. 25(1) GDPR, non sia possibile concludere che la società in questione abbia, sotto tale profilo, violato la disposizione del medesimo articolo.
Nella decisione finale, l'Autorità irlandese ribadisce la conclusione a cui era già giunta nella bozza di decisione. Specificamente, sottolinea che le misure tecniche e organizzative adottate da TTL per verificare l'età nel periodo di riferimento non possono essere considerate in contrasto con l'art. 25 GDPR. L'Autorità osserva inoltre che gli artt. 24 e 25 GDPR non specificano in modo esplicito le misure particolari da utilizzare per garantire la verifica dell'età. Inoltre, sottolinea che il settore della verifica dell'età è ancora in fase di sviluppo e che al momento non esistono standard industriali o normativi ampiamente accettati in questo contesto.
Nel predisporre la decisione finale, con le valutazioni giuridiche espresse nella decisione vincolante dell'EDPB, il DPC ha dichiarato di aver tenuto conto di tutte le osservazioni presentate da TTL nell'esercizio del suo diritto di essere ascoltata, nonché di altre informazioni pertinenti ricevute e ha quindi modificato la bozza di decisione, nell'esercizio dei suoi poteri correttivi, disponendo nel modo sopra riassunto.

ILARIA GARACI

https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_it

https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en

2023/3(11)RMo

I provvedimenti dei Garanti per la protezione dei dati personali austriaco e della Bassa Sassonia, dell'aprile e del maggio 2023, in materia di cookie paywall impiegati da testate di giornali online

Con provvedimento dell'aprile scorso (2023) l'Autorità austriaca per la protezione dei dati personali (d'ora in poi "**Garante austriaco**" e "**decisione del Garante Austriaco**") si è pronunciata in merito ai requisiti di liceità dell'impiego di cookie paywall da parte della testata giornalistica austriaca www.derstandard.at, alla luce della Direttiva del Parlamento europeo e del Consiglio, 2002/58/CE del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (d'ora in poi, "**direttiva e-privacy**") e del Regolamento del Parlamento europeo e del Consiglio, 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (**GDPR**).
Nello scorso maggio (2023), invece, l'Autorità per la protezione dei dati personali della Bassa Sassonia ha adottato una decisione relativa ai cookie paywall impiegati dal sito web www.heise.de (d'ora in poi

"**Garante Bassa Sassonia**" e "**decisione del Garante Bassa Sassonia**"), parimenti volta ad accertarne la conformità alle suddette normative.

Un cookie wall preclude l'accesso agli utenti di un sito web, a meno che costoro acconsentano all'uso dei cookie presenti nel medesimo, che non siano necessari per prestare il servizio di comunicazione elettronica agli utenti. Invece, i cookie paywall offrono all'utente di un sito web di notizie una duplice scelta: 1) acconsentire all'uso dei cookie, inclusi quelli di profilazione e analitici di terze parti (cfr., per una classificazione funzionale dei cookie, Garante per la protezione dei dati personali, Linee guida cookie e altri strumenti di tracciamento - n. 231 del 10 giugno 2021 (su cui v. in questa Rubrica la notizia 6 del numero 2021/3 [2021/3(6)CR]: http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf), ovvero 2) pagare un prezzo per accedere al sito o, più di frequente, sottoscrivere un abbonamento a pagamento, potendo così usufruire dei contenuti ivi presenti in assenza di tracciamento.

L'associazione "None of Your Business" (di seguito "NOYB"), creata per tutelare i diritti degli utenti della rete Internet, ha proposto i reclami che hanno dato origine alle due citate decisioni dei Garanti austriaco e della Bassa Sassonia, unitamente a una serie di reclami presso molteplici autorità nazionali per la protezione dei dati personali, tutti relativi all'impiego di cookie paywall, anche di profilazione e analitici di terze parti, da parte di giornali online europei (si vedano https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price, nonché https://noyb.eu/en/pay-or-okay-beginning-end, relativi a ricorsi concernenti giornali online austriaci e tedeschi).

Per far fronte all'elevato numero di reclami concernenti cookie wall e cookie paywall, l'European Data Protection Board (d'ora in poi "EDPB") ha costituito un'apposita *Task force* (Cfr. https://edpb.europa.eu/news/news/2021/edpb-establishes-cookie-banner-taskforce_en, nonché https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf).

Anche la nostra autorità garante per la protezione dei dati personali (d'ora in poi, il "Garante italiano") ha avviato nell'ottobre 2022 alcune istruttorie tutt'ora pendenti sull'uso di cookie paywall da parte delle testate giornalistiche online italiane (v. in questa Rubrica la notizia 11 del numero 4/2022 [2022/4(11)SO]: http://www.personaemercato.it/wp-content/uploads/2023/01/Osservatorio.pdf).

Secondo le linee guida del Garante italiano sui cookie, un cookie wall rischia di porre l'interessato nella posizione di "prendere o lasciare" (c.d. "*take it or leave it*"), di rinunciare cioè al servizio o, viceversa, di usufruirne, acconsentendo però al trattamento dei propri dati non necessari per la prestazione del servizio di comunicazione elettronica. Il consenso dell'utente rischia dunque di formarsi in modo non libero. La valutazione in merito alla presenza di un consenso libero deve compiersi, secondo il Garante italiano, caso per caso. La illiceità cioè non sussiste *in re ipsa*, non potendo escludersi che, in concreto, "il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di cookie o altri strumenti di tracciamento".

In linea di principio, l'accesso ai contenuti giornalistici a pagamento nel quadro di un cookie paywall può corrispondere al "servizio equivalente" di cui alle Linee guida del Garante italiano sui cookie, purché l'impiego di tale meccanismo sia conforme all'art. 5 GDPR.

Nel reclamo proposto al Garante austriaco, NOYB ha dedotto che il consenso degli utenti del sito web non è stato liberamente manifestato, rilevando che, nella pratica oggetto di istruttoria: i) i dati personali degli utenti sono trattati illecitamente, per carenza di una valida base giuridica (in considerazione del contrasto del trattamento con gli artt. 4(1), (2) e (11), art. 6(1)(a), art. 7, Art. 51(1), art. 57(1)(f), art. 58(2) e art. 77(1) GDPR), ii) va dunque disposta la inibizione del trattamento e la cancellazione dei dati raccolti, iii) nonché la irrogazione di una sanzione pecuniaria. Il Garante austriaco ha ritenuto fondate le deduzioni di NOYB, ma non ha disposto l'irrogazione di una sanzione pecuniaria.

Con proprie linee guida del 30/11/2018 il Garante austriaco aveva già indicato le condizioni in presenza delle quali i cookie paywall sono conformi a direttiva e-privacy e GDPR (GZ: DSB-D122.931/0003-DSB/2018, https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies- and-data-protection.html): i) i gestori dei siti che utilizzano cookie paywall non devono avere una posizione di monopolio o quasi monopolio; ii) deve essere offerto un prezzo ragionevole ed equo per l'alternativa a pagamento (per accedere al sito web tramite l'alternativa a pagamento, all'utente non deve essere cioè prospettato pro forma un prezzo del tutto sproporzionato); se si sceglie l'opzione a pagamento, non possono essere trattati dati personali degli utenti a scopo di tracciamento e

pubblicità personalizzata (salvo valido consenso degli utenti stessi).

Non diversamente, il Garante per la protezione dei dati personali francese (CNIL, Cookie walls: la CNIL publie des premiers critères d'évaluation (16 maggio 2022,), in https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation. 16 maggio 2022. Cfr. anche Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019, https://www.cnil.fr/sites/cnil/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf.) ha stabilito i seguenti requisiti: i) che il prezzo richiesto per la sottoscrizione sia ragionevole; ii) che i cookie paywall siano previsti limitatamente agli scopi del trattamento che permettano agli editori di conseguire un'equa remunerazione del servizio offerto; iii) che vi sia trasparenza in ordine ai criteri impiegati per valutare sia la ragionevolezza del prezzo fissato per l'alternativa a pagamento, sia l'equità della remunerazione conseguibile grazie al consenso all'uso dei cookie.

Nella propria decisione sul reclamo proposto da NOYB, il Garante austriaco, a partire dalla posizione espressa dall'EDPB (Linee guida dell'EDPB n. 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 adottate il 4 maggio 2020, para 43 f: sulle Linee guida dell'EDPB v. in questa Rubrica la notizia 5 del numero 2020/2 [2020/2(5)EMI]: http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf), ha rilevato quanto segue:

i) i cookie, come gli altri identificatori online, permetto di accedere ad informazioni qualificabili come dati personali ai sensi dell'art. 4 (1) GDPR, pertanto, il trattamento di tali dati per finalità di pubblicità online e di data analytics deve basarsi sul consenso dell'interessato secondo l'art. 6 (1) GDPR;

ii) tale consenso può dirsi validamente prestato a condizione che (art. 4 (11) e 7 GDPR) vi sia una inequivoca manifestazione di volontà, espressa liberamente, specifica e informata, nonché revocabile;

iii) il consenso si considera liberamente espresso se viene osservato il principio di granularità, per il quale (considerando 32 e 43 GDPR), quando il trattamento dei dati persegue più finalità o si articola in una pluralità di operazioni, occorre mettere gli interessati in condizione di acconsentire separatamente alle diverse finalità e operazioni di trattamento dei dati personali. Se il responsabile del trattamento "aggrega" diverse finalità/operazioni di trattamento e non cerca di ottenere consensi separati per ciascuna di esse, manca la libertà del consenso;

iv) le testate giornalistiche austriache hanno richiesto il consenso per una pluralità di finalità indicate nella propria dichiarazione sulla privacy, incluso il consenso al tracciamento e alla pubblicità personalizzata; le modalità adottate per acquisire il consenso sono tali da stabilire un "prendere o lasciare" tra l'opzione consistente nell'abbonarsi a pagamento, da un lato, e l'alternativa di fornire un "consenso generalizzato" alla installazione e uso dei cookie, dall'altro lato. Gli utenti per conseguenza non possono che acconsentire a tutti i diversi trattamenti (anziché a ciascuno di essi in modo granulare) o scegliere di abbonarsi a pagamento.

Ad analoghe conclusioni è giunta anche la Risoluzione della Conferenza dei Garanti della Federazione e dei Länder tedeschi del 22 marzo 2023 (d'ora in poi "Conferenza dei Garanti della Federazione e dei Länder" https://datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf) e, prima ancora il Garante per la protezione dei dati personali francese (CNIL), secondo cui: "La creazione di un account deve perseguire scopi specifici e trasparenti per gli utenti […]. I cookie paywall non possono imporre l'accettazione di tutti i marcatori presenti in un sito web. I siti web possono richiedere il consenso dell'utente, caso per caso" (cfr. CNIL, Cookie walls: la CNIL publie des premiers critères d'évaluation (16 maggio 2022), in https://www.cnil.fr/fr/cookie-walls-la-cnil-publie-des-premiers-criteres-devaluation).

L'istruttoria del Garante della Bassa Sassonia è anch'essa pervenuta all'accertamento di talune violazioni del GDPR.

Più in particolare, una prima violazione dell'art. 6 (1) GDPR è consistita nel fatto che, già al momento

del primo accesso al sito web oggetto di istruttoria, ha luogo un trattamento di dati personali degli utenti (come indirizzi IP e informazioni sulla navigazione online), non necessari per il funzionamento del sito medesimo e senza previo consenso degli utenti. Il requisito del carattere preventivo del consenso, necessario ai sensi delle suddette normative, non viene dunque rispettato nel caso di specie.

Inoltre, nelle informazioni rese agli utenti, alcuni cookie di terze parti vengono indicati come funzionali (non richiedenti quindi il consenso degli interessati), in contrasto con gli esiti degli accertamenti tecnici compiuti dal Garante.

In aggiunta, secondo il Garante della Bassa Sassonia, i requisiti per manifestare un valido consenso secondo gli art. 4 (11) e 7 GDPR non vengono osservati, per le seguenti ragioni:

i) alcune informazioni da fornirsi già al "primo livello" di interazione dell'utente con il sito web (nel cookie banner grazie al quale l'utente può esprimere il consenso) e, tra esse, quelle concernenti gli scopi del trattamento, la costituzione di profili degli utenti, i terzi a cui i dati degli utenti vengono trasferiti e la facoltà di revocare il consenso, appaiono disponibili per gli utenti soltanto accedendo ad una pagina successiva, con la conseguenza che il requisito della completezza della informazione viene rispettato tardivamente, quando è possibile che l'utente abbia già acconsentito al collocamento e uso dei cookie;

ii) il sito web ottiene dagli utenti un consenso generico e dunque invalido, giacché non vengono ivi elencate le finalità specifiche del trattamento, né fornite informazioni sul fatto che si fa luogo a trattamento di dati personali, che profili individuali degli utenti vengono creati e arricchiti con dati provenienti da altri siti web, e che i dati sono trasmessi a terzi (il cui numero e identità non vengono dichiarati). Per via delle informazioni insufficienti e dell'elevata complessità del trattamento dei dati personali, dovuto all'elevato numero di dati e di partecipanti, nel caso concreto il consenso non viene dunque espresso in modo specifico;

iii) il consenso dell'utente non è libero, secondo il GDPR, se dal rifiuto o revoca del consenso possa derivare all'utente un pregiudizio. Per interpretare il requisito del pregiudizio, il GDPR prende in considerazione l'eventuale "squilibrio" tra il titolare del trattamento e l'interessato. Nel caso di specie, nota il Garante della Bassa Sassonia, per via del modo in cui il sito web è concepito, e, in particolare, del fatto che occorre accedere ad un secondo livello per ottenere un quadro più chiaro dell'ambito del trattamento e, soprattutto, dell'enorme numero di terzi aventi accesso ai dati, l'utente deve compiere un notevole sforzo aggiuntivo per informarsi adeguatamente prima di dare il proprio consenso. Questo sforzo aggiuntivo – dovuto al design del banner del consenso - rappresenta un pregiudizio per gli utenti che acconsentono ai cookie, rispetto agli utenti abbonati;

iv) per giunta, il design del sito web integra la pratica del *nudging*, giacché in tale sito il banner del consenso reca un primo pulsante "accetta", più appariscente perché colorato in un blu brillante con scritte bianche, e un secondo pulsante per abbonarsi, ma in bianco con scritte nere, appena distinguibile dallo sfondo del banner, anch'esso bianco. Il *nudging* – osserva il Garante – costituisce una pratica idonea a influenzare il comportamento degli utenti;

v) infine, l'articolo 7 (3) n. 4 GDPR richiede che la revoca del consenso sia altrettanto semplice del suo rilascio. Tale requisito non viene rispettato per via del modo in cui il sito web è concepito: il consenso, infatti, può ivi essere dato immediatamente nel primo livello, non appena si inizia ad utilizzare il sito, mentre la revoca del consenso non è resa possibile in questa stessa fase, ma soltanto accedendo ad un livello successivo, con conseguente maggiore aggravio per l'utente.

ROBERTA MONTINARO

https://noyb.eu/sites/default/files/2023-04/Standard_Bescheid_geschwärzt.pdf

https://noyb.eu/sites/default/files/2023-07/11VerwarnungPurAboModellfinalgeschwrztp_Redacted.pdf

2023/3(12)AAM

Emessa in Cile il 9.8.2023 la prima sentenza al mondo sui neurodiritti (a proposito di 'Insight' un dispositivo neurotecnologico non terapeutico e non invasivo in commercio del tipo

elettroencefalogramma mobile progettato per ottenere informazioni sull'attività cerebrale)

Il Cile con la "Ley n. 21.383 *Modifica La Carta Fundamental, Para Establecer El Desarrollo Científico Y Tecnológico Al Servicio De Las Personas*", del 25 ottobre 2021 è stato il primo paese al mondo ad intervenire con una modifica legislativa per tutelare la mente umana da uno sviluppo tecnologico in grado di incidere negativamente sull'integrità psicofisica delle persone. Tale legge, infatti, ha modificato il primo comma, ultima parte dell'art. 19 della Costituzione cilena (*Constitucion politica de la Republica de Chile*) che così attualmente prevede espressamente quanto segue: "*El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella*". Nella Commissione che ha presentato la proposta di modifica del testo costituzionale (con il progetto di legge dal titolo *Modifica el artículo 19, número 1°, de la Carta Fundamental, para proteger la integridad y la indemnidad mental con relación al avance de las neurotecnologías* del 7 ottobre 2020) vi era anche il parlamentare Guido Girardi Lavín, che ha poi dato impulso al processo che si è concluso con la prima sentenza in tema di tutela dei dati neurali e sviluppo e commercializzazione di dispostivi neurotecnologici conformi ai principi fondamentali di salvaguardia della persona umana. Si tratta di una decisione assunta il 9 agosto 2023 dalla Corte Suprema del Cile (Rol n. 105.065-2023) contro la società Emotiv Inc., un'azienda bioinformatica e tecnologica che sviluppa e produce prodotti di elettroencefalografia indossabili con sede a San Francisco, negli Stati Uniti. La società veniva chiamata in giudizio a causa della vendita e commercializzazione in Cile di '*Insight*', dispositivo *wireless* che funziona come una fascia per capelli, con sensori che raccolgono informazioni sull'attività cerebrale, ottenendo dati su gesti, movimenti, preferenze, tempi di reazione e attività cognitiva dell'utente che lo indossa. Il ricorrente sosteneva che "*Insight*" non protegge adeguatamente la *privacy* delle informazioni cerebrali dei suoi utenti, ciò in violazione delle garanzie costituzionali contenute nei numeri 1, 4, 6 e 24 dell'articolo 19 della Costituzione politica della Repubblica del Cile.

Il ricorrente, infatti, dopo aver acquistato un dispositivo '*Insight*' attraverso il sito web della società convenuta, seguiva le istruzioni sul dispositivo al fine di registrare e accedere ai suoi dati cerebrali, creando a tale scopo un account sul *cloud* di dati di Emotiv Inc., accettando i termini e le condizioni della società. Successivamente, installava sul proprio computer il *software* denominato '*Emotiv Launcher'*, che consiste in un punto di accesso a tutte le informazioni, gli strumenti e la gestione dei dispositivi *Emotiv*, associando il proprio *account* al dispositivo *Insight* ed accettando nuovamente i termini e le condizioni della società. Il ricorrente, tuttavia, sosteneva che, avendo utilizzato la licenza gratuita e non quella 'PRO', non ha potuto esportare o importare alcuna registrazione dei propri dati cerebrali, che erano stati registrati e archiviati nel *cloud* della società Emotiv Inc. Il ricorrente affermava in giudizio, pertanto, di essere stato esposto ai seguenti rischi: (i) re-identificazione; (ii) *hacking* dei dati (iii) riutilizzo non autorizzato dei dati cerebrali; (iv) commercializzazione dei dati cerebrali; (v) sorveglianza digitale; (vi) raccolta di dati cerebrali per scopi non consentiti, a tal fine riferendo la violazione degli articoli 11 (responsabilità del titolare del trattamento per la corretta conservazione dei dati) e 13 (diritto alla cancellazione dei dati) della legge cilena sulla privacy (Ley n. 19.628) oltre che dell'articolo 19 della Costituzione.

La convenuta società si difendeva sostenendo che "*Insight*" è un dispositivo neurotecnologico non terapeutico e non invasivo del tipo elettroencefalogramma mobile, concepito per l'autovalutazione e la ricerca sul campo, non venduto, pertanto, come dispositivo medico. Sosteneva ancora la società americana che i termini e le condizioni del prodotto accettate dal ricorrente contenessero precise e chiare indicazioni sul trattamento dei dati personali - e quindi anche dei dati neurali - rilevati dal dispositivo, trattamento per il quale era stato espresso il consenso da parte dell'utente. Emotiv Inc. riferiva, pertanto, di non aver commesso alcuna violazione, né della Ley n. 19.628, né del più rigoroso Regolamento (UE) 2017/679 sulla protezione dei dati personali (GDPR). Con specifico riferimento al diritto alla cancellazione dei dati registrati (art. 13 Ley n. 19.628), infatti, la società affermava che il ricorrente non aveva mai avanzato alcuna richiesta in tal senso, né mai aveva risposto alle e-mail inviategli a tal fine.

Preso atto dei fatti illustrati, nella sentenza in commento, la Corte Suprema cilena in primo luogo fornisce una dettagliata ricostruzione della fattispecie oggetto di giudizio facendo espresso richiamo alla citata legge di modifica della Costituzione cilena, inquadrando in tal modo i fatti

di causa in un preciso dibattito internazionale che ha coinvolto diversi organismi sovranazionali (Unesco, OCSE, Organizzazione delle Nazioni Unite) preoccupati dello sviluppo non regolamentato di alcuni dispositivi – c.d. neurotecnologici – in grado di dare accesso all'attività cerebrale della persona. La Corte ribadisce pertanto la *ratio* della legge di modifica costituzionale - Ley n. 21.383 - diretta a tutelare la persona da uno sviluppo tecnologico incontrollato e lesivo dei diritti fondamentali, richiamando altri importanti testi internazionali che riconoscono il rapporto tra scienza e diritti umani (Patto internazionale sui diritti economici, sociali e culturali; Dichiarazione dell'Unesco sulla scienza e l'uso della conoscenza scientifica; Dichiarazione delle Nazioni Unite sul Genoma Umano; Convenzione sulla Diversità Biologica; Dichiarazione universale sulla bioetica e i diritti umani dell'Unesco).

Fatta tale premessa, la Corte afferma due importanti principi di diritto. In primo luogo, viene precisato che, in relazione alla tutela della *privacy* del dato neurale – ovvero collegato all'attività cerebrale rilevata e registrata dal dispositivo – la tecnica dell'anonimizzazione degli stessi non legittima il titolare del trattamento a considerarli alla stregua di mere informazioni statistiche liberamente utilizzabili. Rigetta, pertanto, la Corte la posizione assunta dalla società Emotiv Inc. per cui una volta anonimizzati, i dati neurali diventano informazioni statistiche liberamente utilizzabili. Al contrario, la Corte precisa che a tal fine occorre il consenso esplicito dell'utente, che deve essere informato che i suoi dati possono essere utilizzati anche per finalità diverse, per le quali occorre un consenso espresso appunto. Diversamente, i dati non sono utilizzabili, non potendosi affermare che tale consenso possa essere considerato come tacitamente dato attraverso altri consensi o approvazioni date dalla persona in qualità di cliente o consumatore. Tale diverso trattamento dei dati, infatti, richiede un consenso specifico, oltre che espresso, che indichi anche lo scopo e l'obiettivo della ricerca corrispondente.

Tuttavia, il principio che appare di maggiore interesse – dalla portata dirompente rispetto al mercato dei prodotti neurotecnologici – è quello che va direttamente ad incidere sulla fase precedente la commercializzazione dei dispositivi in parola.

La Corte, infatti, afferma che lo sviluppo di nuove tecnologie che coinvolgono aspetti della persona umana, che fino a pochi anni fa era impensabile che potessero essere conosciuti, deve imporre una diversa valutazione dei dispositivi da parte delle autorità statuali, ciò anche laddove questi non siano destinati all'utilizzo medico ma al mercato dei prodotti di consumo.

L'obiettivo, infatti, deve essere quello di prevenire e anticipare i possibili effetti negativi delle neurotecnologie sui diritti delle persone, andando queste ad invadere una dimensione un tempo assolutamente privata e personale, riservata all'ambito sanitario ovvero l'attività cerebrale, oggi aperta al mercato e alle sue logiche.

Nelle valutazioni operate dalla Suprema Corte, pertanto, ciò che appare assolutamente necessario è un controllo preventivo operato dalle competenti autorità sanitarie (la Corte fa riferimento per il Cile all'*Istituto di sanità pubblico*), provvedano ad operare gli opportuni controlli di dispositivi potenzialmente lesivi, prima della loro commercializzazione. In altre parole, le più ampie e rafforzate garanzie - e controlli – previsti per i dispositivi medici, devono essere estese anche ai dispositivi destinati al mercato dei prodotti di consumo. A tale controllo, precisa la Corte, deve aggiungersi anche quello dell'autorità doganale cilena, competente ad emettere il relativo Certificato di Destinazione Doganale.

Per tutti questi motivi, la Suprema Corte cilena, in applicazione dell'articolo 19, numeri 1, 4 e 6, della Costituzione accoglie il ricorso e ordina alla società Emotiv Inc. di cancellare tutte le informazioni memorizzate nel suo *cloud* o nei suoi portali in relazione all'uso del dispositivo da parte del ricorrente.

L'importanza di tale sentenza, pertanto, rileva non solo perché destinata ad orientare la giurisprudenza ben oltre i confini cileni, se si considera che in nessun altro ordinamento giuridico è allo stato entrata in vigore una specifica disciplina normativa che tuteli la persona da intrusioni non autorizzate nella propria attività cerebrale e sui relativi dati che la rappresentano. La sentenza in parola rappresenta, altresì, un importante stimolo per l'interprete, per riflettere sul modo in cui la tecnologia deve essere regolamentata dal legislatore.

Il secondo principio espresso dalla Corte, infatti, mette in guardia dai pericoli insiti in dispositivi tecnologici le cui funzionalità spesso sfuggono non solo agli utenti finali ma agli stessi progettisti e produttori. Ciò sembra confermato dallo stesso legislatore europeo che nella Proposta di Regolamento Europeo che stabilisce regole armonizzate sull'intelligenza artificiale (c.d. AI Act) nel testo di compromesso con relativi emendamenti del Parlamento europeo, approvati il 14 giugno 2023 (COM(2021)0206 – C9-0146/2021 – 2021/0106 (COD)), prevede un'articolata disciplina dei sistemi di IA di riconoscimento delle

emozioni, che prevede, nell'art. 5, il divieto di commercializzazione e di uso in determinati casi (nella bozza attuale si tratta dei seguenti 4 campi: applicazione della legge, gestione delle frontiere, istituti di insegnamento e luoghi di lavoro) e nella generalità degli altri casi li assoggetta al test previsto dall'articolo 6, paragrafo 2 che qualifica come sistemi "ad alto rischio" quei sistemi di IA rientranti tra le previsioni dell'Allegato III che "***presentano un rischio significativo di danno per la salute umana, la sicurezza e i diritti fondamentali delle persone fisiche***". Nell'Allegato III sono espressamente previsti i "*sistemi di AI destinati ad essere utilizzati per trarre conclusioni sulle caratteristiche personali delle persone fisiche sulla base di dati biometrici o basati su elementi biometrici, compreso i* ***sistemi di riconoscimento delle emozioni****, ad eccezione di quelli di cui all'articolo 5*". Nel testo della bozza di AI Act in commento, i sistemi di IA di rilevamento delle emozioni sono così definiti: "un sistema di IA finalizzato all'identificazione o alla deduzione di emozioni, pensieri, stati d'animo o intenzioni di individui o gruppi sulla base dei loro dati biometrici e basati su elementi biometrici".

I dispositivi neurotecnologici del tipo di quelli oggetto della sentenza in parola, commercializzati sul territorio dell'Unione Europea, laddove rientranti nella definizione di sistemi di IA, potrebbero ragionevolmente includersi tra i "*sistemi ad alto rischio*" laddove il Regolamento Europeo entrasse in vigore nella sua attuale formulazione. Ciò in considerazione del forte impatto negativo di tali sistemi sui diritti fondamentali delle persone e, nella specie, sulla *privacy* e integrità della sfera mentale dell'utilizzatore. Inoltre, la loro commercializzazione ed uso sarebbe vietata nei sopradetti quattro ambiti di applicazione.

Su tale considerazione si innesta la possibilità di mettere in evidenza la parte più rilevante della sentenza della Suprema Corte del Cile. Questa, infatti, sembra accendere un faro sulla tutela della persona che deve necessariamente costruirsi con interventi *ex ante* e non *ex post*. È necessario, in tale ambito, infatti, pensare a sistemi di controllo preventivi delle tecnologie che non siano autoreferenziali, mere dichiarazioni provenienti dalle stesse aziende produttrici il cui unico interesse è quello di immettere il prodotto sul mercato per finalità sicuramente differenti dalla (o comunque non esclusivamente coincidenti con la) tutela della persona. Il controllo deve, pertanto, essere operato da organismi di valutazione autonomi ed indipendenti, con l'obiettivo di valutare nel lungo periodo – non soltanto nel momento in cui il prodotto viene immesso sul mercato – quali potranno essere prospetticamente i rischi prodotti dal dispositivo, in modo da poterli eliminare. Tali valutazioni, inoltre, dovrebbero essere operate durante la fase di progettazione e non a processo ultimato, per evitare che in caso di esito negativo dei controlli si crei un diverso problema di gestione di dispositivi che devono necessariamente essere dismessi, ponendo un evidente questione di sostenibilità della tecnologia prodotta.

Su questo punto, si tratterà di vedere quale sarà il testo finale dell'AI Act (se sarà alla fine emanato, in esito ai triloghi ancora da svolgersi in questo ultimo scorcio di anno) posto che sarebbe certamente insufficiente un sistema di gestione e mitigazione del rischio derivante dai sistemi di IA che lasciasse ai fornitori (soggetti che sviluppano o fanno sviluppare un sistema di AI al fine di immetterlo sul mercato) la libertà di scegliere le misure più adeguate a far fronte ai rischi. La fattispecie oggetto del giudizio innanzi alla Suprema Corte del Cile, sopra riassunto, stimola perciò senz'altro verso la creazione di una disciplina legislativa e l'elaborazione di soluzioni ermeneutiche, idonee a garantire, anche in Europa, adeguate tutele nei confronti del fenomeno del 'dominio della mente', nel senso della elaborazione di: (a) norme e soluzioni applicative che assicurino una tutela dell'individuo-utente finale nel caso di utilizzo di dispositivi neurotecnologici progettati per usi anche al di fuori del contesto medico: (b) una disciplina normativa in grado di orientare la progettazione e produzione di dispositivi neurotecnologici con efficienti misure di controllo e certificazione da parte di soggetti indipendenti.

In questo senso, i principi espressi dalla Corte cilena, e dalla riferita legge cilena di riforma costituzionale, in quanto orientati alla protezione dell'integrità psicofisica della persona, e al divieto di utilizzo non consentito dei dati neurali connessi all'attività cerebrale, sono senz'altro di stimolo anche per la riflessione e l'elaborazione dell'erigendo diritto dei dati nel contesto europeo.

ANNA ANITA MOLLO

https://www.bcn.cl/leychile/navegar?idNorma=242302

https://www.diarioconstitucional.cl/wp-content/uploads/2023/08/GIRARDICONEMOTIVSUPREMA.pdf105.065-2023.pdf

2023/3(13)EWDM

La sentenza della Corte Costituzionale del 27.7.2023 sul valore di corrispondenza dei messaggi whatsapp e email

La Corte costituzionale, con la sentenza n. 170 del 27 luglio 2023, ha dichiarato che la Procura di Firenze non poteva acquisire, senza preventiva autorizzazione del Senato, messaggi di posta elettronica e whatsapp di un noto parlamentare, o a lui diretti, conservati in dispositivi elettronici appartenenti a terzi, oggetto di provvedimenti di sequestro nell'àmbito di un procedimento penale a carico dello stesso parlamentare e di terzi.

Esclusa l'ipotesi di considerare tali messaggi all'interno della disciplina delle intercettazioni per carenza dei requisiti, la Corte è convinta che lo scambio di messaggi elettronici – mail, sms, whatsapp e simili – rappresenti una "forma di corrispondenza" e, pertanto, tutelabile ai sensi e per gli effetti degli artt. 15 e 68, co. 3, cost.

Movendo dalla convinzione che il concetto di "corrispondenza" sia "ampiamente comprensivo", «atto ad includere ogni comunicazione di pensiero umano (idee, propositi, sentimenti, dati) tra due o più persone, attuato in modo diverso dalla conversazione in presenza», ritiene che la tutela contenuta nell'art. 15 cost., che assicura a tutti i consociati la libertà e la segretezza "della corrispondenza e di ogni altra forma di comunicazione", consentendo limitazioni solo "per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge", prescinda dai mezzi tecnici utilizzati.

Ne consegue che, secondo il giudice delle leggi, i messaggi di posta elettronica e quelli whatsapp (appartenenti ai sistemi di "messaggistica istantanea"), sono del tutto simili a lettere e biglietti chiusi, tutelabili *ex* art. 15 cost. La riservatezza della comunicazione, che tradizionalmente è garantita nell'inserimento del plico cartaceo o del biglietto in una busta chiusa, sarebbe assicurata, per la posta elettronica, dal fatto che "viene inviata a una specifica casella di posta, accessibile solo dal destinatario tramite codici personali di accesso", e, per i messaggi whatsapp, dal fatto che rimangono accessibili "solo al soggetto che abbia concretamente la disponibilità del dispositivo elettronico di destinazione, protetto anch'esso da codici di accesso o altri meccanismi di identificazione".

Nonostante l'art. 15 cost. si riferisca anche alle "altre forme di comunicazione", oltre alla corrispondenza, e l'art. 68, comma 3, cost., invece, si riferisca solo alla corrispondenza, la corte ritiene che i due concetti si relazionino in termini di *species ad genus*, per orientamento costante.

Pertanto, la nozione di "corrispondenza", utilizzata dal testo costituzionale senza alcuna ulteriore specificazione, appare "sufficientemente ampia" da ricomprendere anche le forme di scambio del pensiero tramite la messaggistica istantanea e la posta elettronica, che altro non sono se non «"versioni contemporanee" della classica corrispondenza epistolare e telegrafica».

Diversamente, si determinerebbe una forte compressione della libertà di espressione di una persona, parlamentare o meno, poiché, in tale momento storico, la corrispondenza cartacea è di fatto relegata ad un ruolo del tutto marginale.

Il giudice delle leggi ritiene, altresì, che simili messaggi mantengano la natura di "corrispondenza" anche dopo che siano stati ricevuti e/o conservati nella memoria dei dispositivi elettronici, purché conservino carattere di "attualità" e "interesse" per i corrispondenti.

Soltanto «quando il decorso del tempo o altra causa abbia trasformato il messaggio in un documento "storico", cui possa attribuirsi esclusivamente un valore retrospettivo, affettivo, collezionistico, artistico, scientifico e probatorio», allora si perderebbe l'attualità e quindi la natura di corrispondenza.

Del resto, la Corte europea dei diritti dell'uomo ha da tempo ricondotto, all'interno dell'art. 8 CEDU, sia i messaggi di posta elettronica e whatsapp inviati, ma non ancora letti sia quelli già ricevuti, letti ed archiviati nella memoria dei dispositivi elettronici.

Alla critica che tale soluzione potrebbe determinare "incertezze applicative", non potendo l'autorità giudiziaria conoscere *a priori* se il messaggio conservi attualità o meno, la Corte costituzionale precisa che tale carattere «deve sempre presumersi fino a prova contraria», ossia fino a quando i messaggi siano scambiati ad una distanza di tempo non particolarmente significativa rispetto al momento in cui l'autorità giudiziaria dovesse procedere ad acquisirli.

ETTORE WILLIAM DI MAURO

https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:2023:170

2023/3(14)FG

Le modifiche alla legge italiana sul diritto d'autore per il contrasto della pirateria online (L. 93/2023)

L'Italia ha adottato misure di contrasto alla pirateria online con l'approvazione della L. 14 luglio 2023, n. 93 - pubblicata sulla Gazzetta Ufficiale n. 171 del 24 luglio 2023 ed entrata in vigore l'8 agosto u.s. - avente ad oggetto 'Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica'.

La legge è costituita da sette articoli che si pongono l'obiettivo di rafforzare la tutela del diritto d'autore sulle piattaforme digitali, cercando di prevenire e limitare la distribuzione illegale di contenuti protetti sia con l'introduzione di disposizioni cogenti sia con l'attribuzione di nuovi poteri all'Autorità Garante per le Comunicazioni (**AGCOM**). Le nuove azioni di contrasto alla pirateria introdotte dal legislatore italiano dovranno essere lette in combinato disposto con le disposizioni europee, relative all'operato degli intermediari digitali, introdotte col Regolamento (UE) 2022/2065 (**Digital Services Act**).

La lotta alla pirateria online prevede il coinvolgimento di tutti gli stakeholder della filiera (i.e. titolari dei diritti, licenziatari, AGCOM, Internet Service Providers) che dovranno collaborare per contrastare un fenomeno che solo nel 2022 ha fatto registrare circa 345 milioni di atti illeciti, anche grazie all'Internet Protocol Television (IPTV) e al cd. camcording (ossia la distribuzione online di contenuti cinematografici registrati all'interno di una sala cinematografica), con un incremento di 30 milioni rispetto all'anno precedente (sport live + 26%; programmi tv + 20%; serie/fiction + 15%, dati Fapav-Ipsos, 'Report sulla Pirateria Audiovisiva in Italia 2022').

L'art. 1 della Legge elenca i "Princìpi" che permeano le nuove disposizioni normative, giustificando l'ampliamento dei poteri di AGCOM nonché l'irrigidimento delle sanzioni, e previsti in attuazione degli articoli 41 e 42 della Costituzione, dell'art. 17 della Carta dei diritti fondamentali dell'Unione europea e della Convenzione sulla protezione e la promozione delle diversità delle espressioni culturali. In particolare, vi è il riconoscimento, la tutela e la promozione della proprietà intellettuale, la tutela del diritto d'autore, l'assicurazione di forme di sostegno alle imprese, agli autori, agli artisti e ai creatori, la individuazione di forme di responsabilizzazione nei confronti degli intermediari di rete.

Sulla base dei Princìpi sopra richiamati, l'art. 2, co. 1, attribuisce all'AGCOM il potere di ordinare ai prestatori di servizi, compresi i prestatori di accesso alla rete, di disabilitare l'accesso a contenuti diffusi in maniera illecita, anche adottando a tal fine provvedimenti cautelari in via d'urgenza. Al fine di rendere la norma immediatamente operativa ed in linea con quanto previsto dall'art. 6, co. 1 della stessa, l'AGCOM ha approvato nella seduta del 26 luglio 2023, con delibera n. 189/23/CONS, le modifiche al Regolamento sul diritto d'autore online (approvato con Delibera n. 680/13/CONS), inserendo la possibilità di emanare le cd. 'ingiunzioni dinamiche'.

Il ricorso all'ingiunzione dinamica trova la sua collocazione nell'ambito della Comunicazione del 29 novembre 2017 della Commissione UE ('Communication from the Commission to the Institutions on Guidance on certain aspects of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights', consultabile al link https://ec.europa.eu/docsroom/documents/26582), contenente le linee guida per l'interpretazione di alcuni aspetti della c.d. Direttiva enforcement (Direttiva 2004/48/CE del Parlamento Europeo e del Consiglio del 29 aprile 2004 sul rispetto dei diritti di proprietà intellettuale, in Gazzetta ufficiale dell'Unione europea L 157 del 30 aprile 2004), i cui artt. 9 e 11 rappresentano la base normativa delle ingiunzioni dinamiche, in quanto ne disciplinano gli aspetti legati alle misure inibitorie, cautelari e non.

Con tali misure, l'Autorità potrà intervenire interrompendo la diffusione pirata di tutti gli eventi trasmessi in diretta, disabilitando l'accesso ai contenuti pirata nei primi 30 minuti della trasmissione dell'evento con il blocco della risoluzione DNS dei nomi di dominio e il blocco dell'instradamento del traffico di rete verso gli indirizzi IP univocamente destinati ad attività illecite. Da sottolineare come l'art. 2 co. 2 preveda che l'Autorità, sempre nell'ambito dello stesso provvedimento e con lo scopo di impedire l'accesso agli stessi contenuti e a contenuti della stessa natura, possa anche ordinare il blocco di ogni altro futuro nome di dominio, sotto dominio o indirizzo IP, a chiunque riconducibili, comprese le variazioni del nome o della semplice declinazione o estensione (cosiddetto top level domain), che consenta l'accesso ai medesimi contenuti diffusi abusivamente e a contenuti della stessa natura. Sempre l'art. 2 (al comma 3), affronta anche le fattispecie in cui i contenuti siano diffusi per la prima volta o trasmessi in diretta: i cd. casi gravi e urgenti. In questi casi, a fronte dell'istanza che deve essere presentata dal titolare o licenziatario del diritto o dalla società di gestione collettiva alla quale sia stato conferito il mandato o, infine, da un

soggetto appartenente alla categoria dei "segnalatori attendibili" (v. art. 22(2) del Digital Services Act), l'AGCOM può emettere un provvedimento cautelare, ordinando ai prestatori di servizi di disabilitare l'accesso ai contenuti illeciti mediante il blocco di dominio e degli indirizzi IP e ciò anche in assenza di un contraddittorio con la controparte: nell'ipotesi di trasmissione in diretta, il suddetto provvedimento deve essere adottato, notificato ed eseguito prima o, al massimo, nel corso della stessa; se invece i contenuti non siano trasmessi in diretta, occorre agire nel corso della loro prima trasmissione. I provvedimenti di disabilitazione sono altresì trasmessi alla Procura della Repubblica che, su richiesta dell'AGCOM, deve ricevere altresì il riscontro delle attività eseguite da parte dei destinatari degli stessi. La mancata osservanza delle disposizioni dell'AGCOM (art. 5) comporterà l'applicazione da parte della stessa Autorità della sanzione amministrativa prevista dall'art.1, co. 31, terzo periodo della l. 31 luglio 1997, n. 249, pari ad euro diecimila fino al 2% del fatturato realizzato nell'ultimo esercizio chiuso anteriormente alla notifica della contestazione.

La nuova normativa (art. 3) al fine di individuare alcune misure per combattere la pirateria cinematografica, audiovisiva e editoriale, introduce sia alcune modifiche agli articoli 171-*ter* e 174-*ter* della legge 641/1933 (LDA) sia all'articolo 131-*bis* del codice penale. Con tali modifiche viene previsto un nuovo reato per coloro che, a fini di lucro, effettuino in maniera abusiva la fissazione dei contenuti digitali, audio, video o audiovisivi, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale (anche secondo il dettato dell'art. 85-*bis*, co. 1, del R.D. 773/1931 - Testo unico delle leggi di pubblica sicurezza), ovvero, riproducano, eseguano o comunichino al pubblico della fissazione eseguita in maniera illecita. A sostegno di tali modifiche, la sanzione amministrativa, prevista dall'art. 174-*ter*, co. 2 LDA, a carico degli utenti che usufruiscono dei contenuti trasmessi sui siti-pirata, viene aumentata fino a 5.000 euro.

A sostegno degli interventi previsti ed al fine di sensibilizzare gli utenti sul valore della proprietà intellettuale e con l'obiettivo di contrastare l'abusivismo, la diffusione illecita e la contraffazione dei contenuti tutelati dal diritto d'autore, l'articolo 4 prevede la collaborazione fra il Ministero della Cultura, la Presidenza del Consiglio dei Ministri e l'AGCOM, per organizzare delle specifiche campagne di informazione, comunicazione e sensibilizzazione.

A carico dell'AGCOM (art. 6), oltre alle modifiche al regolamento in materia di tutela al diritto d'autore (già approvato nella seduta del 26 luglio 2023: si veda sopra), è prevista altresì la convocazione di un tavolo tecnico con gli operatori del settore per definire quali siano i requisiti tecnici per consentire la disabilitazione dei nomi di dominio e degli indirizzi IP, attraverso un'unica piattaforma (da realizzare entro sei mesi dalla convocazione del tavolo tecnico) ed i cui costi di realizzazione (art. 7) saranno a carico dei titolari di diritti delle opere cinematografiche, audiovisive e musicali, programmi televisivi ed eventi sportivi, dei fornitori di servizi di media e degli organismi di gestione collettiva e delle entità di gestione indipendenti di cui all'articolo 2 del decreto legislativo 15 marzo 2017, n. 35.

In data 7 settembre 2023 si è tenuta la riunione di insediamento del tavolo tecnico convocato da AGCOM, in collaborazione con l'Agenzia per la cybersicurezza nazionale, e con la partecipazione delle rappresentanze della Guardia di Finanza e della Polizia Postale presso l'Autorità, del Ministero delle Imprese e del Made in Italy, degli Internet Service Provider e dei titolari dei diritti.

Nel corso dell'incontro, è stato anche discusso il calendario delle attività finalizzate alla conclusiva messa in opera della piattaforma tecnologica unica ("Piracy Shield") che consentirà ai titolari di segnalare le violazioni e agli ISP di provvedere al blocco delle risorse pirata.

FRANCESCO GROSSI

https://www.gazzettaufficiale.it/eli/gu/2023/07/24/171/sg/pdf

2023/3(15)RA

Il provvedimento dell'AGCM del 18.7.2023 sugli impegni di Google relativi alla portabilità dei dati personali

Nella sua adunanza del 18 luglio 2023, l'Autorità Garante della Concorrenza e del Mercato (l'"**Autorità**" o "**AGCM**") ha deliberato di rendere obbligatori per Alphabet Inc., Google LLC, Google Ireland Ltd e Google Italy S.r.l., taluni impegni presentati da tali società (collettivamente "**Google**") ai sensi dell'art. 14-*ter*, comma 1 della legge n. 287/1990, chiudendo il procedimento da essa avviato senza accertare alcuna infrazione dell'art. 102 TFUE da parte loro.

Il provvedimento dell'Autorità trae origine dalla vicenda che segue.

Il 5 luglio 2022, l'AGCM ha avviato – su segnalazione di Hoda S.r.l. (società, con sede a Milano, attiva nell'intermediazione di dati personali attraverso l'App denominata "Weople") – un'istruttoria ai sensi dell'articolo 14 della legge n. 287/1990 nei confronti di Google, per accertare eventuali violazioni dell'articolo 102 del TFUE, consistenti in ostacoli frapposti dalla società che controlla il noto motore di ricerca all'individuazione di adeguati meccanismi di interoperabilità volti a rendere disponibili i dati presenti su Google a piattaforme alternative. In particolare, Hoda ha rappresentato di aver avviato, fin dal 2019, contatti con Google per l'individuazione di meccanismi di interoperabilità che consentissero agli utenti della piattaforma "Weople" di trasferire su tale piattaforma, ai sensi dell'articolo 20 del GDPR (dedicato al "Diritto alla portabilità dei dati"), i dati presenti nell'ecosistema Google. Tuttavia, a fronte di tali richieste, Google avrebbe rappresentato che l'unico servizio che essa rende disponibile ai propri utenti per richiedere e ottenere una copia dei loro dati è rappresentato da "Takeout": una procedura che, risultando estremamente articolata e complicata, scoraggerebbe l'esercizio da parte degli utenti della portabilità dei dati.

Secondo Hoda, la condotta di Google, nel pregiudicare l'esercizio da parte dell'utente finale del diritto alla portabilità dei dati stabilito dal menzionato art. 20 del GDPR, si risolverebbe in un indebito sfruttamento da parte della stessa Google dei consumatori finali nella misura in cui determina una limitazione dei benefici che i consumatori potrebbero trarre dalla valorizzazione dei loro dati personali, ciò tenuto conto che Google detiene una posizione dominante nel mercato della pubblicità *search* radicata proprio sui dati di cui esso dispone, che – per volume e varietà – consentono una profilazione degli utenti così qualificata da rendere irreplicabile la capacità di Google di ritagliare su misura gli spazi pubblicitari in base al *target* degli inserzionisti (v. decisione della Commissione del 20 marzo 2019, caso AT.40411 – *Google Search-Ad Sense* – https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020AT40411%2803%29). Basti pensare che, nel mercato per la offerta di servizi generali di ricerca, Google detiene una quota di mercato – a livello italiano – pari al 95%.

A seguito delle ispezioni dell'Autorità, della presentazione delle osservazioni delle Parti e delle relative audizioni, il 28 febbraio 2023 Google ha presentato taluni impegni ai sensi dell'art. 14-*ter* della legge n. 287/1990 e l'AGCM, verificata la loro non manifesta infondatezza, ne ha disposto la pubblicazione.

In particolare, al fine di rispondere alle preoccupazioni concorrenziali rappresentate dall'Autorità, Google ha presentato un pacchetto di tre impegni: due di tali impegni prospettano soluzioni integrative del servizio "Takeout" volte a facilitare l'esportazione dei dati verso operatori terzi; il terzo impegno offre la possibilità di iniziare a testare – prima del rilascio ufficiale – una nuova soluzione di portabilità diretta dei dati da servizio a servizio, che Google metterà a disposizione di operatori terzi, autorizzati da un utente finale i cui dati sono stati oggetto della richiesta di portabilità relativa a taluni prodotti di Google.

Alla consultazione pubblica su tali impegni, avviata in data 22 marzo 2023, hanno partecipato tre imprese (la società denunciante Hoda, Mediaset ed ErnieApp Ltd) e due associazioni di imprese (il Consorzio Netcomm - e la Computer & Communications Industry Association - CCIA), nonché l'istituto per le Politiche dell'innovazione e la Fondazione Italia Digitale. Tali soggetti hanno fornito un riscontro sostanzialmente positivo rispetto al pacchetto complessivo di impegni presentato da Google, evidenziando solo la necessità di alcuni puntuali miglioramenti e ampliamenti dei medesimi.

Il 22 maggio 2023, Google ha replicato alle osservazioni presentate nella consultazione pubblica, rilevando come i contributi degli *stakeholder* hanno confermato, nel loro complesso, che gli impegni rispondono alle preoccupazioni espresse dall'Autorità e ha provveduto a integrare gli impegni presentati.

Secondo l'Autorità, gli impegni presentati da Google appaiono idonei a far venir meno i profili anticoncorrenziali relativi alle condotte contestate nel provvedimento di avvio dell'istruttoria. Essi, infatti, garantendo un'importante automatizzazione della procedura allo stato disponibile per l'esportazione dei dati ("Takeout"), appaiono idonei a consentire agli utenti l'esercizio del diritto alla portabilità consacrato nell'articolo 20 del GDPR; essi inoltre approssimano al meglio un meccanismo di interoperabilità atto a rendere accessibili a piattaforme terze i dati che sono disponibili nella piattaforma di Google. Di tale meccanismo utenti e operatori terzi potranno avvalersi fino al rilascio da parte di Google di una soluzione di portabilità diretta da servizio a servizio; rilascio che, secondo quanto indicato dalle stesse società Google, avverrà nel primo trimestre del 2024.

RICCARDO ALFONSI

https://www.agcm.it/media/comunicati-stampa/2023/7/A552-

2023/3(16)TDMCDV

L'intesa tra il governo USA e i "giganti" dell'Intelligenza Artificiale del 21.7.2023 e del 12.9.2023 su safety, security e trust della IA generativa

Il 21 luglio 2023 il governo USA ha raggiunto un accordo con i principali sviluppatori di Intelligenza Artificiale (IA), cd. "giganti" dell'IA, con cui questi ultimi hanno assunto un impegno volontario e non giuridicamente vincolante ("*voluntary AI committments*") ad agire in maniera responsabile e ad assicurare che i prodotti che essi mettono a disposizione del pubblico siano sicuri e trasparenti. L'intesa – siglata inizialmente da Amazon, Anthropic, Google, Inflection, Meta, Microsoft e OpenAI, cui il successivo 12 settembre si sono aggiunte le firme di Adobe, Cohere, IBM, Nvidia, Palantir, Salesforce, Scale AI e Stability – rappresenta solo una parte della più ampia politica dell'amministrazione Biden-Harris, la quale ha dichiarato l'impegno a continuare a intraprendere azioni esecutive e a perseguire una legislazione che permetta agli USA di essere leader nell'innovazione responsabile e di sfruttare le potenzialità e, allo stesso tempo, gestire i rischi creati dall'IA. Infatti, il raggiungimento di questo accordo rappresenta – secondo le dichiarazioni ufficiali del Governo USA - solo il primo passo verso la creazione di obblighi giuridicamente vincolanti per gli sviluppatori di IA negli USA, il che richiederà l'adozione di nuove leggi, sistemi di sorveglianza ed *enforcement*.

Con l'adesione all'intesa le imprese assumono l'impegno di incorporare tre principi fondamentali all'interno delle proprie attività di sviluppo e di impiego di tecnologie di IA: *safety*, *security*, *trust*. L'accordo si riferisce in particolare alla cd. IA generativa, cioè quella capace di generare testi, immagini, video, musica o altri contenuti in base alle specifiche richieste. Infatti, l'ambito di applicazione dell'intesa viene esplicitamente circoscritto a tali modelli di IA, precisando che, quando gli specifici impegni menzionano modelli particolari, essi si applicano solo ai modelli generativi che sono complessivamente i più potenti del settore, come GPT-4, Claude 2, PaLM 2, Titan e DALL-E 2.

L'accordo prevede otto categorie di impegni specifici suddivisi in base alle parole chiave sopra riportate.

Il requisito della "*safety*" si riferisce all'obbligo delle imprese di accertarsi della sicurezza dei propri prodotti prima di immetterli sul mercato. La sicurezza, in questo caso, attiene alla necessità di testare le capacità dei sistemi di IA in modo da valutare i loro potenziali rischi biologici, di cybersicurezza e sociali, rendendo pubblici i risultati di tali valutazioni. Rientra nell'ambito dei test sulla sicurezza lo specifico impegno ***(1)*** ad investire nello sviluppo dei cd. *red teaming* interni ed esterni, vale a dire una metodologia di test che implica la simulazione di attacchi informatici, anche da parte di società esterne ed esperte, finalizzati a identificare e colmare le eventuali lacune di cybersicurezza, tenendo in considerazione una serie di rischi come quelli biologici e chimici legati al potenziale impiego di sistemi di IA nella progettazione e nell'uso di armi, ovvero rischi sociali come quelli collegati ai *bias* e alle possibili discriminazioni. Inoltre, la sicurezza dei sistemi di IA generativa include l'impegno ***(2)*** alla condivisione di informazioni tra imprese, amministrazioni, società civile e accademia, in merito ai rischi per la fiducia e la sicurezza, alle capacità pericolose o emergenti dei sistemi e ai tentativi di eludere misure di sicurezza, tanto attraverso la creazione o la partecipazione a forum o ad altri meccanismi attraverso cui sviluppare, adottare e diffondere standard condivisi e *best practices* per la sicurezza dell'IA.

Il requisito della "*security*" – che in questo caso attiene a profili di "protezione" o "difesa" – richiede di salvaguardare i modelli contro le minacce informatiche e interne, nonché di condividere gli standard per prevenire gli abusi, ridurre i rischi per la società e proteggere la sicurezza nazionale. In particolare, le imprese si impegnano ***(3)*** a proteggere la proprietà intellettuale dei propri modelli di IA, con particolare riguardo ai cd. "pesi" dei modelli, ovverosia quei parametri numerici appresi dal modello durante l'addestramento e che sono essenziali per il suo funzionamento in quanto determinano il livello di influenza dell'*input* sull'*output* prodotto. L'accordo prevede, dunque, l'impegno a trattare i modelli non ancora rilasciati come un elemento centrale della proprietà intellettuale dell'impresa, limitando l'accesso a tali modelli solamente al personale le cui funzioni lo richiedono ed elaborando un robusto programma di rilevamento delle minacce interne. Inoltre, tale dimensione di sicurezza richiede di conservare e lavorare con i modelli in un ambiente fornito di adeguata protezione per ridurre il rischio di rilasci non autorizzati. Rientra, ancora, nell'ambito della *security* l'impegno ***(4)*** a incentivare terze parti a

segnalare problemi e vulnerabilità del sistema di IA, anche attraverso l'impiego di programmi cd. "*bug bounty*", ossia accordi tra sviluppatori che prevedono un sistema di ricompense per gli individui che riconoscono e segnalano un *bug* del sistema.

Il requisito della fiducia ("*trust*") include il maggior numero di impegni specifici, tutti volti alla creazione di sistemi di IA che ispirino fiducia nel pubblico tanto con riguardo alla loro trasparenza, quanto rispetto alla qualità dei risultati attesi dal loro utilizzo. In questo senso, i giganti dell'IA si impegnano ***(5)*** a sviluppare e implementare meccanismi che consentano agli utenti di capire se i contenuti audiovisivi sono stati generati dall'IA, anche attraverso sistemi di *provenance* – ossia "provenienza autenticata", modelli di fiducia algoritmici impiegati soprattutto in ambito *blockchain* – e/o di *watermarking* – cioè l'inserimento di una "filigrana" elettronica all'interno di file audiovisivi che permette di distinguere i contenuti reali da quelli realizzati dall'IA – fatta eccezione per quei contenuti facilmente distinguibili da quelli reali o progettati proprio per essere distinti da questi ultimi, come nel caso delle voci degli assistenti vocali. A tale scopo, i dati di *provenance* e di *watermark* dovrebbero includere un identificativo del servizio o del modello che ha creato il contenuto, ma non le informazioni che permettono di identificare il suo utente. La fiducia nei sistemi di IA include, poi, l'impegno ***(6)*** a pubblicare report contenenti le valutazioni sulle capacità e i limiti dei modelli, così come i loro ambiti di utilizzo appropriati e non, includendo discussioni circa i loro rischi sociali, al fine di garantire agli utenti interazioni consapevoli con i sistemi. In questo senso, le imprese si impegnano anche ***(7)*** a dare la priorità alla ricerca finalizzata a ridurre i rischi sociali generati dall'IA, in modo da evitare gli effetti di *bias* dannosi e discriminazioni, nonché proteggere la privacy degli individui e tutelare soggetti vulnerabili, come i bambini. Infine, l'intesa prevede l'impegno ***(8)*** a sviluppare e diffondere sistemi di IA all'avanguardia per contribuire ad affrontare le sfide più importanti della società, tra cui il cambiamento climatico, la diagnosi tempestiva e la prevenzione del cancro e le minacce informatiche. In aggiunta, le imprese si impegnano a sostenere iniziative che promuovano l'istruzione e la formazione di studenti e lavoratori per trarre concreto vantaggio dai benefici dell'IA e aiutare i cittadini a comprendere la natura, le capacità, i limiti e l'impatto di questa tecnologia.

TOMMASO DE MARI CASARETO DAL VERME

https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ (21 luglio 2023);

https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ (12 settembre 2023)

2023/3(17)FG

L'opinion del 18.8.2023 (e il collegato provvedimento) del Giudice Howell del District of Columbia nel caso Thaler su IA generativa e copyright

In data 18 agosto 2023 il giudice Beryl A. Howell della corte distrettuale della Columbia ha confermato il provvedimento di rigetto dello United States Copyright Office (**USCO**) relativamente a una domanda di registrazione di un'opera figurativa ('A Recent Entrance to Paradise') creata interamente con un sistema di intelligenza artificiale generativa.

La domanda di registrazione era stata depositata dal dr. Stephen Thaler, proprietario del software, presso l'USCO, in data 3 novembre 2018.

L'USCO si è pronunciata in senso negativo in data 12 agosto 2019 e 23 settembre 2019 e il suo Review Board (responsabile dell'esame dei ricorsi amministrativi presentati da un richiedente in caso di doppio rifiuto di registrazione dell'opera dell'Ufficio) è intervenuto in tal senso in data 14 febbraio 2022 - tale approccio è stato successivamente confermato in data 21 febbraio 2023 relativamente alla registrazione di una graphic novel ("Zarya of the Dawn") creata dal sistema di IA 'Midjourney'.

A differenza di quanto accaduto per 'Zarya of the Dawn', il richiedente ha però rivelato immediatamente nella domanda, che l'immagine era il risultato di un sistema di intelligenza artificiale ('The Creativity Machine'); il dr. Thaler ha indicato 'The Creativity Machine' quale autore dell'opera e indicato se stesso come richiedente, chiarendo di essere autorizzato a presentare la domanda in qualità di proprietario del sistema di IA.

La richiesta di registrazione del dr. Thaler si inserisce nell'ambito della campagna internazionale

di depositi di brevetto e ricorsi ("Artificial Inventor Project") avviata dallo stesso Thaler a partire dal 2018, per sostenere la tesi che un sistema di intelligenza artificiale debba poter essere designato come inventore in una domanda di brevetto e, nel caso, della Creativity Machine quale autore.
A seguito del rigetto della domanda, il dr. Thaler ha impugnato la decisione di fronte alla Corte Distrettuale Territoriale Federale per il Distretto della Columbia, citando in giudizio sia l'USCO sia Shira Perlmutter, in qualità di direttrice dell'USCO stessa.
Thaler ha chiesto alla Corte distrettuale di adottare un provvedimento che imponesse all'USCO sia di annullare la decisione del Review Board e sia di ripristinare la domanda di registrazione dell'opera, ritenendo il rigetto dell'agenzia "*arbitrario, capriccioso, un abuso di discrezionalità, non conforme alla legge, non supportato da prove sostanziali*".
Thaler ha affermato che la normativa americana sul Copyright consente di proteggere le opere generate dall'intelligenza artificiale come avviene per le società e le altre persone giuridiche e non esiste giurisprudenza che giustifichi il diniego dell'USCO; Thaler ha sostenuto, inoltre, che che il requisito dell'originalità abbia una soglia generalmente bassa.
Un'altra argomentazione avanzata da Thaler è che l'opera potrebbe essere classificata secondo la dottrina del 'work for hire'. Nel Complaint, Thaler riconosce la correttezza dell'argomentazione di risposta del Review Board secondo cui un'IA non è un dipendente o un appaltatore indipendente che può stipulare un contratto; tuttavia, Thaler sostiene che il sistema di IA si comporti funzionalmente come tale, e quindi le dovrebbe essere riconosciuto uno status simile.
La Corte Distrettuale ha precisato che la paternità umana è un requisito fondamentale del copyright negli Stati Uniti ("*Human authorship is a bedrock requirement of copyright*"), confermando quanto già affermato dall'USCO.
La "*fissazione*" dell'opera nel supporto tangibile deve essere effettuata "*dall'autore o sotto la sua autorità*", per poter beneficiare del diritto d'autore, quindi, un'opera deve avere un "*autore*".
Pur non essendo definito il termine "autore" nel Copyright Act, la Corte evidenzia che va inteso nell'accezione di "*colui che è la fonte di una qualche forma di lavoro intellettuale o creativo*".
Secondo il Copyright Act, un'opera tutelabile deve avere un autore con capacità di lavoro intellettuale, creativo o artistico. Tale autore secondo la Corte deve essere un essere umano e il requisito della paternità umana è stato dato per assodato negli scorsi secoli.
La Corte distrettuale richiama giurisprudenza nota per giustificare l'assunto:

- in "*Sarony*", 111 U.S.; "*Mazer v. Stein*", 347 U.S. 201 (1954) e "*Goldstein v. California*", 412 U.S. 546 (1973), la paternità si focalizza su atti della creatività umana.
- In "*Urantia Found. v. Kristen Maaherra*, 114 F.3d 955, 958–59 (9th Cir. 1997); *Penguin Books U.S.A., Inc. v. New Christian Church of Full Endeavor*, 96-cv-4126 (RWS), 2000 WL 1028634, at *2, 10–11 (S.D.N.Y. July 25, 2000); *Oliver v. St. Germain Found.*, 41 F. Supp. 296, 297, 299 (S.D. Cal. 1941); *Kelley v. Chicago Park District* 635 F.3d 290, 304–06 (7th Cir. 2011); "*Naruto v. Slater, 888*", le Corti hanno uniformemente rifiutato di riconoscere il copyright alle opere create senza alcun coinvolgimento umano, anche quando, ad esempio, il presunto autore fosse stato "divino".

Secondo la Corte distrettuale, le diverse teorie legali presentate da Thaler in base alle quali il diritto d'autore sull'opera del computer si trasferirebbe a lui, in quanto proprietario del software (i.e. work for hire) non devono essere analizzate in dettaglio, dato che l'opera in questione non è tutelabile.

FRANCESCO GROSSI

https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2022cv1564-24

2023/3(18)IT

Le raccomandazioni del 17.7.2023 del Financial Stability Board sui Global Stable Coin Arrangements e sui mercati in criptoattività

Il 17 luglio 2023 il *Financial Stability Board* (FSB) ha pubblicato due set di raccomandazioni volte a stabilire un quadro internazionale coerente e completo per la regolamentazione e la vigilanza dei mercati di cripto-attività. L'obiettivo è mitigare i rischi alla stabilità finanziaria, rafforzare la cooperazione tra autorità nazionali e promuovere la convergenza in un settore (per lo più) fuori dal perimetro della disciplina finanziaria. Il lavoro dà seguito alle richieste del G20 di sviluppare regole globalmente condivise e un *framework* di sorveglianza che tenga conto non solo dei profili

antiriciclaggio, ma anche delle implicazioni legate alla diffusione delle *stable coin* e alle turbolenze sui mercati delle cripto-attività.

Le raccomandazioni sono presentate in due rapporti separati, ma complementari.

(i) "*High-level recommendations for the regulation, supervision, and oversight of crypto-asset activities and markets*", contenente nove raccomandazioni applicabili alle diverse tipologie di cripto-attività, compresi i cosiddetti *stable coin* e la finanza decentralizzata. Si prevede, tra l'altro, la necessità che le autorità si coordinino e collaborino anche a livello internazionale per lo scambio di informazioni e che siano applicate regole di *governance*, *recordkeeping*, gestione dei rischi e dei conflitti d'interesse da parte di emittenti *stable coin* e fornitori di cripto-attività.

(ii) "*High-level recommendations for the regulation, supervision, and oversight of global stablecoin arrangements*", contenente dieci raccomandazioni applicabili agli *stable coin* cosiddetti "globali" (GSC), ossia utilizzati in modo diffuso come riserva di valore o mezzo di scambio in operazioni transfrontaliere, in quanto tali sottoposti a regole più stringenti in ragione dei potenziali rischi sistemici e alla sovranità monetaria. Si prevede, tra l'altro, la necessità d'introdurre piani di risoluzione, oltre che meccanismi di stabilizzazione e requisiti prudenziali; ai detentori di *stable coin* globali dovrebbe essere garantito un diritto di rimborso che, in caso di GSC riferite a una singola valuta fiat, dovrebbe intervenire alla pari in modo da mitigare i rischi di corse agli sportelli.

Le raccomandazioni costituiscono una fonte di *soft law* internazionale (da decenni il principale strumento di avvicinamento delle legislazioni finanziarie); esse fanno perno su tre capisaldi tra loro connessi e comuni anche ad altri ambiti della regolamentazione di settore:

1. "Stessa attività, stesso rischio, stessa regolamentazione" (*same activity, same risk, same rule*) - le raccomandazioni del FSB mirano a garantire che le regole applicabili al settore cripto siano proporzionate ai rischi. Attività che svolgono funzioni economiche equivalenti alla finanzia tradizionale devono essere soggette alla stessa regolamentazione o a regolamentazione equivalente, indipendentemente dal modo in cui vengono presentate o promosse.

2. Approccio flessibile - le raccomandazioni del FSB sono "*high level*", ossia offrono margini di adattamento affinché le autorità possano calarle nelle cornici regolatorie già vigenti a livello locale o sviluppare nuovi *framework* nazionali, tenendo conto delle evoluzioni del mercato.

3. Neutralità tecnologica - le raccomandazioni del FSB si concentrano sui rischi alla stabilità finanziaria associati alle attività su stablecoin globali e cripto-attività; esse si applicano a prescindere dalla specifica tecnologia impiegata. Le attività sono, infatti, regolamentate in base alle loro funzioni economiche e ai rischi che comportano, indipendentemente dai mezzi tecnologici utilizzati.

Il lavoro del FSB si affianca alle analisi sugli impatti macroeconomici e le indicazioni di *policy* fornite dal Fondo Monetario Internazionale in materia di cripto-attività e rappresenta un fondamentale tassello di un più ampio ventaglio d'iniziative internazionali finalizzate a supportare uno sviluppo responsabile dell'innovazione digitale. Il FSB, infatti, svolge un ruolo di coordinamento dei cosiddetti *Standard Setter Bodies* (SSBs), consessi in cui riuniscono le autorità di vigilanza o le banche centrali al fine di rafforzare la cooperazione ed emanare standard di regolamentazione finanziaria. Nello specifico, le raccomandazioni del FSB in materia di cripto-attività rappresentano il quadro di riferimento che sarà arricchito e integrato con principi e standard di carattere più tecnico e specifico, quali quelli in corso di elaborazione da parte dello IOSCO per il settore dei mercati dei capitali e pubblicati dal BCBS per il settore bancario (https://www.fsb.org/wp-content/uploads/P170723-1.pdf).

L'aspettativa è che questo insieme di standard e raccomandazioni sia attuato globalmente dai singoli Stati e applicato in modo coerente dalle autorità di vigilanza nazionali. In assenza di regole nazionali convergenti sarà difficile garantire un'adeguata vigilanza dei c.d. cripto-conglomerati, ossia dei complessi gruppi di società attivi in via transfrontaliera (*on-line*) che, come nel caso di FTX, prestano cumulativamente, in modo opaco e in conflitto d'interessi una serie di servizi economicamente equivalenti ad attività finanziarie, che spaziano dall'emissione alla gestione di piattaforme di negoziazione, dal post-trading al cambiavalute e alla custodia, ecc.

Considerato, tuttavia, che gli standard internazionali nel settore cripto sono ancora in corso di definizione, il percorso per addivenire all'applicazione di approcci nazionali convergenti appare ancora lungo e dovrà fare i conti, come di frequente nella finanza, con i rischi di arbitraggi normativi e con i tentativi di alcuni centri finanziari di attrarre *business* mediante regole o pratiche di vigilanza più lasche, ovvero ostacolando la cooperazione internazionale.

L'Unione europea, da parte sua, ha già emanato una disciplina comune sui mercati delle cripto-attività, coerente con le raccomandazioni del FSB. Ci si riferisce al Regolamento MICA (Regolamento (UE) 2023/1114, sulla cui adozione v. in questa Rubrica la notizia 1 nel numero 2023/2 [2023/2(1)AF]: http://www.personaemercato.it/wp-content/uploads/2023/08/Osservatorio.pdf), che sarà applicabile nella sua interezza a partire dal dicembre 2024 (dal giugno 2024 per le emissioni di *stable coin*). Di conseguenza, l'accesso al mercato unico europeo da parte degli operatori cripto attivi globalmente potrà intervenire solo laddove questi siano disposti a adeguare la propria condotta e i propri modelli di business alle regole MICA e sottostare alla vigilanza delle autorità competenti nell'UE. Gli operatori globali possono avere interesse ad applicare un unico set di regole in tutti i vari paesi in cui sono attivi, per contenere i costi di compliance e incrementare le economie di scala.

Il MICA, allora, potrebbe rappresentare un modello di riferimento e innescare un'accelerazione nell'adozione da parte di altri grandi paesi di una regolamentazione convergente nel settore cripto, in linea con le raccomandazioni FSB, sulla falsa riga di quell' "Effetto Bruxelles" già sperimentato nella *data protection* con il GDPR e atteso con la disciplina ESG.

IRENE TAGLIAMONTE
Avvocato, Ufficio Analisi di Impatto della Regolamentazione, Divisione Strategie Regolamentari, Consob

Le idee e le opinioni espresse in questo articolo sono da attribuire unicamente all'autore e non coinvolgono l'istituzione di appartenenza

FSB Global Regulatory Framework for Crypto-Asset Activities

High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final report (fsb.org)

2023/3(19)ES

Le nuove regole della SEC su cybersecurity risk, governance, management e incident disclosure efficaci dal 5.9.2023

Il 26 luglio 2023 la Securities and Exchange Commission statunitense (**SEC**) ha adottato la versione finale delle regole su "*cybersecurity risk management, strategy, governance, and incident disclosure*" per le società quotate (da ora anche le "**Final rules**").

Il testo adottato è frutto dell'approvazione di una proposta presentata nel marzo 2022 dalla SEC con cui questa intendeva riformare le regole esistenti in materia di cibersicurezza consapevole che le minacce e gli incidenti digitali si connotano per un crescente grado di rischiosità "*to public companies, investors, and market participants*". La proposta, a sua volta, era frutto di orientamenti interpretativi emessi dalla SEC nel 2011 e 2018 alla luce dell'assenza di valide regole di settore e si proponeva di consentire agli investitori di valutare adeguatamente l'esposizione delle società quotate (da ora anche gli "**Emittenti**") ai rischi legati alla cibersicurezza e ai relativi incidenti, nonché la loro abilità nel gestire e mitigare i suddetti rischi.

Per quanto qui interessa, in sintesi, le Final rules prevedono quanto segue.

A) Innanzitutto, esse richiedono agli Emittenti di comunicare ogni incidente cibernetico che ritengano, a loro giudizio, rilevante descrivendone la natura, l'obiettivo e la tempistica così come l'impatto materiale, anche potenziale, sull'Emittente.

La valutazione sulla rilevanza dell'incidente deve avvenire senza ritardo affinché questo sia poi comunicato alla SEC entro i successivi quattro giorni lavorativi. La comunicazione può essere dilazionata solo laddove il Procuratore Generale degli Stati Uniti stabilisca che una disclosure immediata causerebbe un rischio sostanziale alla sicurezza nazionale.

B) In secondo luogo, le Final rules impongono agli Emittenti di redigere un report per:

i. descrivere le procedure che essi abbiano eventualmente adottato per valutare, identificare e gestire i rischi materiali derivanti da minacce cibernetiche;
ii. comunicare se i suddetti rischi abbiano impattato materialmente l'Emittente; e
iii. descrivere la sorveglianza svolta dagli amministratori della società, nonché il loro ruolo ed esperienza nella gestione dei rischi derivanti dalle minacce cibernetiche.

C) In terzo luogo, anche le società quotate estere dovranno inviare alla SEC delle comunicazioni periodiche riguardo alla disclosure sugli incidenti cibernetici che rendano nelle giurisdizioni straniere. Tali società, inoltre, saranno tenute a un'informativa simile a quella prevista sub B).

Per concludere, occorre sottolineare che le Final rules entrano in vigore il trentesimo giorno successivo alla loro pubblicazione sul Registro federale. Riguardo gli obblighi di cui al paragrafo B), gli Emittenti dovranno provvedere alla disclosure a partire dai report redatti per l'anno fiscale che termina dal 15 dicembre 2023. Per tutti gli altri obblighi, le società - eccetto quelle di piccole dimensioni - dovranno provvedere entro 90 giorni dalla pubblicazione delle Final rules sul Registro federale o, al più tardi, entro il 18 dicembre 2023. Le società più piccole, invece, avranno a più tempo per adempiere ai suddetti doveri.

EMANUELE STABILE

https://www.sec.gov/files/rules/final/2023/33-11216.pdf

2023/3(20)ES

La seconda fase di sperimentazione Fintech

Con un comunicato stampa del 27 luglio 2023 la Banca d'Italia, la Consob e l'Ivass (da ora anche le "**Autorità di vigilanza**" o le "**Autorità**") e il Ministero dell'Economia e delle Finanze ("**MEF**") informavano dell'apertura della seconda finestra temporale, dal 3 novembre al 5 dicembre 2023, per la presentazione delle inziative di sperimentazione delle attività fintech nell'ambito della sandbox regolamentare.

Analogamente alla prima finestra temporale, apertasi il 15 novembre 2021 (v. in questa rubrica la notizia n. 9 sul numero 2021/4 [2021/4(9)ES]: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf), il fondamento giuridico della sperimentazione è il Decreto del Ministero dell'economia e delle finanze n. 100 del 30 aprile 2021 (da ora anche il "**Regolamento sandbox**") entrato in vigore il 17 luglio 2021 il quale attua la delega conferita con l'art. 36, commi 2 bis e ss. D. L. n. 34/2019 (c.d. "Decreto crescita").

Come noto, la sandbox regolamentare è un ambiente controllato dove gli operatori del settore, come meglio definiti infra, possono sviluppare progetti innovativi in ambito bancario, finanziario e assicurativo sotto la vigilanza e con il supporto delle competenti Autorità. Si tratta, dunque, di uno strumento attraverso cui quest'ultime potranno monitorare le dinamiche dello sviluppo tecnologico e individuare gli interventi normativi migliori per incentivare l'adozione di soluzioni tecnologiche e il loro impiego. Al contempo, la vigilanza delle Autorità aiuta a prevenire i rischi connessi alla sperimentazione.

Le similitudini rispetto alla precedente finestra temporale di candidatura sono numerose.

In particolare, resta fermo che i partecipanti alla sandbox possono essere solo soggetti, pure non vigilati, che svolgano o intendano svolgere attività fintech, anche in misura non prevalente: i c.d. operatori fintech (art. 1). Sono esclusi dalla partecipazione invece coloro i quali siano assoggettati ad una procedura concorsuale o non abbiano depositato il bilancio negli ultimi 5 anni.

La soluzione da sperimentare deve riguardare sempre i settori bancario, finanziario o assicurativo ed essere: i) "*soggetta all'autorizzazione o all'iscrizione in un albo, elenco o registro da parte di almeno una delle autorità di vigilanza*", oppure esentata dalla suddetta iscrizione; ii) prestata "*in favore di un soggetto vigilato o regolamentato da almeno un'autorità di vigilanza … avente in Italia la propria sede legale o una succursale*", ovvero in favore di un ente con sede legale negli Stati membri dell'UE ed operante in Italia in regime di libera prestazione di servizi; iii) "*svolta da un soggetto vigilato o regolamentato da almeno un'autorità di vigilanza … avente in Italia la propria sede legale o una succursale, ovvero da un ente con sede legale negli Stati membri dell'UE ed operante in Italia in regime di libera prestazione di servizi*" (art. 5).

L'attività che si intende svolgere dovrà essere "significativamente innovativa" come meglio specificato dall'art. 6 del Regolamento sandbox.

Ancora, sono immutate la procedura di ammissione alla sandbox, l'istruttoria a tal fine condotta dalle Autorità e le competenze del Comitato fintech il quale si occupa di monitorare l'evoluzione del settore, formulare proposte normative, nonché agevolare l'interlocuzione tra gli operatori di settore e le Autorità che decidono sull'ammissione alla sperimentazione.

L'ammissione alla sperimentazione comporta l'iscrizione in un apposito registro tenuto dal Comitato. Durante la sperimentazione, ciascuna Autorità vigila sulle attività svolte e, soprattutto,

può consentire agli operatori di sperimentare in deroga alla propria regolamentazione.
La sperimentazione non può durare più di diciotto mesi, salvo proroghe concesse dall'Autorità di vigilanza.
L'unica differenza rispetto alla prima finestra di sperimentazione è che non è stato previsto un numero massimo di progetti ammissibili alla sandbox.
Giova ricordare, infine, che ciascuna Autorità ha emanato un regolamento per disciplinare l'adozione da parte sua dei provvedimenti di ammissione alla sandbox. Si tratta rispettivamente: del Regolamento di Banca d'Italia del 3 novembre 2021, pubblicato sulla G.U. del 10 novembre 2021; della delibera Consob n. 22054 del 27 ottobre 2021, pubblicata sulla G.U. del 5 novembre 2021 e del regolamento IVASS n. 49 del 3 novembre 2021 pubblicato sulla G.U. del 13 novembre 2021. Essi sono pressoché equivalenti tra di loro.

EMANUELE STABILE

https://www.bancaditalia.it/media/comunicati/documenti/2023-02/cs-FintechLuglio2023.pdf

2023/3(21)RMa

Le ultime modifiche in materia di obblighi informativi nel rapporto di lavoro relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati (D.L. 48/2023 convertito con modifiche dalla Legge 85/2023) e la sentenza del Tribunale di Torino del 5.8.2023 sulla condotta antisindacale di Glovo

L'utilizzo di applicazioni di intelligenza artificiale nella gestione dei rapporti di lavoro apre a scenari inediti con riferimento all'esercizio dei poteri datoriali e, in particolare, al potere di controllo. Consapevole di ciò il legislatore, nel recepire la direttiva europea 2019/1152 relativa a condizioni di lavoro trasparenti e prevedibili nell'Unione europea, è andato oltre quanto strettamente richiesto dall'ordinamento eurounitario e ha introdotto, nel *corpus* della normativa di recepimento, l'art. 1-*bis* del D.lgs. 152/1997. In particolare, tale articolo è stato introdotto dall'art. 4 del d. lgs. 104/2022, ed è stato successivamente modificato dall'art. 26, co. 2 D.L. 48/2023 (in G.U. n. 103 del 4 maggio 2023) convertito con modifiche dalla legge del 03/07/2023 n. 85. L'art. 1-*bis* del D.lgs. 152/1997 è rubricato "*ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati*".
Il suo nuovo comma 1 così reca: "Il datore di lavoro o il committente pubblico e privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori. Resta fermo quanto disposto dall'articolo 4 [Impianti audiovisivi e altri strumenti di controllo] della legge 20 maggio 1970, n. 300 [Statuto dei lavoratori]".
Il capoverso della disposizione elenca, poi, un *set* analitico di informazioni che devono essere fornite.
Il comma 3 precisa che il lavoratore, direttamente o per il tramite delle rappresentanze sindacali aziendali o territoriali, ha diritto di accedere ai dati e di richiedere ulteriori informazioni, che dovranno essere forniti per iscritto entro trenta giorni. Rileva, poi, ai fini della decisione in commento, il comma 6 della disposizione, in base al quale, le informazioni e i dati di cui ai commi da 1 a 5 devono essere comunicati dal datore di lavoro o dal committente in modo trasparente, in formato strutturato, di uso comune e leggibile da dispositivo automatico non solo ai lavoratori ma anche alle RSA/RSU e, in assenza, alle sedi territoriali delle associazioni sindacali comparativamente più rappresentative sul piano nazionale.
Infine, il nuovo comma 8 dell'art. 1-*bis* del D.lgs. 152/1997 prevede che "Gli obblighi informativi di cui al presente articolo non si applicano ai sistemi protetti da segreto industriale e commerciale".
Il caso deciso dal Tribunale di Torino nel provvedimento del 5 agosto 2023 qui in commento riguarda in particolare l'applicazione delle norme contenute nei riferiti commi da 2 a 6 (non toccati dalle ultime modifiche) dell'art. 1-bis D.lgs. 152/1997.
La società di *food delivery* Foodinho, appartenente al gruppo Glovo, veniva convenuta in giudizio dalle federazioni torinesi della CGIL Filcams, Nidil e Filt con procedimento ex art. 28 della L. 300/1970 in quanto, secondo le OO.SS. ricorrenti, la convenuta non avrebbe fornito alle richiedenti le informazioni sui sistemi automatizzati di gestione dei rapporti di lavoro dei rider ex art. 1-*bis* D.lgs. 152/1997 richieste formalmente con missiva del 20 aprile 2023. La Società resisteva in giudizio con vari argomenti, tra cui, l'asserita cessazione della

materia del contendere per avere la convenuta fornito le informazioni richieste dalle ricorrenti con apposita "*informativa in materia di trasparenza ex d.lgs. 104/2022*" trasmessa alle ricorrenti il 5 luglio 2023.

Particolarmente interessanti appaiono i principi di diritto formulati dal Giudice che, nel dichiarare antisindacale la condotta di Foodinho, ha, anzitutto, avuto modo di chiarire, riprendendo numerosi precedenti di merito e di legittimità sul tema (su Trib. Milano sent. n. 1018/2020 del 20.4.2022 v. in questa rubrica notizia 12 del numero 2022/2 [2022/2(12)VP]: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf), che il rapporto di lavoro dei riders non può essere configurato come lavoro autonomo a causa delle concrete modalità di svolgimento dello stesso e che, in ogni caso, anche se lo si volesse ricondurre alla c.d. collaborazione etero-organizzata ex art. 2 del D.lgs. 81/2015 sarebbe, in ogni caso, esperibile l'azione di repressione della condotta antisindacale ex art. 28 dello Statuto dei Lavoratori in quanto, anche alla luce di Cass. n. 1663/2020, "*la norma (...) rende applicabile a tali collaborazioni etero-organizzate, accompagnate dalla personalità e continuità della prestazione, la disciplina del rapporto di lavoro subordinato, senza operare esclusioni di sorta*".

Fatto questo chiarimento preliminare il Tribunale evidenzia che, in base al tenore letterale della norma, non possono esserci dubbi sul fatto che le informazioni sui sistemi automatizzati di gestione dei rapporti di lavoro dei rider ex art. 1-*bis* D.lgs. 152/1997 debbano essere fornite *sia* al lavoratore *sia* alle rappresentanze sindacali "*senza che l'adempimento dell'obbligo nei confronti di uno dei titolari, possa far ritenere l'obbligo informativo adempiuto anche nei confronti dell'altro*".

La decisione si concentra, infine, sull'idoneità dell'"*informativa in materia di trasparenza ex d.lgs. 104/2022*" trasmessa da Foodinho alle ricorrenti il 5 luglio 2023 a considerare assolti gli obblighi informativi sui sistemi automatizzati di gestione dei rapporti di lavoro previsti dalla richiamata normativa.

Ebbene, all'esito di un esame puntuale del contenuto dell'informativa, il Tribunale giunge a ritenere che la predetta comunicazione, essendo del tutto carente su alcuni punti e, su altri, casi lacunosa e generica, non soddisfa gli obblighi informativi gravanti su Foodinho dal ché deriva la natura antisindacale della condotta datoriale, con conseguente condanna della Società a comunicare alle OO.SS. ricorrenti le informazioni di cui alla citata norma e a pubblicare il dispositivo del provvedimento sul proprio sito web, sezione "corrieri".

RICCARDO MARAGA

https://www.gazzettaufficiale.it/eli/id/2023/07/03/23A03800/sg#:~:text=E'%20istituito%2C%20a%20decorrere%20dal,di%20politica%20attiva%20del%20lavoro.

https://web.uniroma1.it/deap/sites/default/files/allegati/20230807_Trib-Torino.pdf

2023/3(22)EG

Emanato il Decreto 7.9.2023 sul fascicolo sanitario elettronico (FSE) 2.0 dopo i pareri positivi del Garante privacy del 8.6.2023 e della Conferenza Stato-Regioni del 2.8.2023

Con Decreto del 7 settembre 2023 (in GU n.249 del 24-10-2023) è ufficialmente entrato nella fase operativa il Fascicolo Sanitario Elettronico (di seguito "**FSE**") nella versione 2.0. Lo schema di decreto del Ministero della Salute e del Sottosegretario di Stato alla Presidenza del Consiglio dei ministri con delega all'innovazione tecnologica, di concerto con il Ministro dell'Economia e delle finanze ha ricevuto prima il via libera dal Garante per la protezione dei dati personali e, il 2 agosto 2023, ha avuto parere favorevole anche dalla Conferenza Stato – Regioni.

Come si legge dal comunicato del Ministero della Salute del 3 agosto 2023: "*Il decreto individua i contenuti del Fascicolo, i limiti di responsabilità e i compiti dei soggetti che concorrono alla sua implementazione, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali nel rispetto dei diritti dell'assistito, nonché le modalità e i livelli diversificati di accesso e si compone di tre allegati tecnici*".

L'8 giugno 2023 il Garante per la protezione dei dati personali (d'ora in poi "Garante" o "Garante Privacy") aveva dato il suo parere positivo alla prosecuzione del progetto di riforma del FSE. Il progetto, che ha l'obiettivo di consentire ai pazienti e al personale sociosanitario di effettuare con maggior rapidità l'accesso alla propria storia clinica, si pone come obiettivo anche la realizzazione di uno Spazio Europeo di Dati Sanitari.

Il Garante si era già espresso su una prima versione dello schema di decreto di attuazione della nuova disciplina del FSE con parere negativo il 22 agosto 2022. In tale occasione erano state rilevate

numerose carenze strutturali e sostanziali riguardanti la mancanza di garanzie uniformi a livello nazionale per il pieno rispetto dei diritti e delle libertà fondamentali degli interessati. In quell'occasione l'Autorità aveva, pertanto, indicato una serie di aggiustamenti necessari al rilascio del proprio parere favorevole. Tali aggiustamenti riguardavano il potenziamento di diversi aspetti, tra cui, a titolo esemplificativo: i diritti degli interessati, il consenso dell'interessato, il profilo sanitario sintetico ("PSS"), le informazioni da fornire agli interessati e la necessità di svolgere una valutazione di impatto alla luce degli effetti significativi che i trattamenti dei dati sanitari possono avere sulla sfera giuridica degli interessati.

Con il Provvedimento n.256 dell'8 giugno 2023, il Garante ha rilevato che l'assetto risultante dal nuovo schema di decreto risponde alle osservazioni e alle criticità sollevate in precedenza, risultando profondamente modificato rispetto alla versione su cui l'Autorità si era espressa ad agosto 2022.

Nello specifico, con il provvedimento n.256 dell'8 giugno, il Garante passa in rassegna gli interventi correttivi ed integrativi effettuati dal Ministero della salute sullo schema di decreto sul FSE trasmesso il 24 maggio 2023, rilevando, in linea generale, il superamento delle criticità evidenziate in precedenza.

Tuttavia, per il Garante Privacy rimangono alcune perplessità. In primo luogo, in considerazione dell'importanza di garantire un'informativa omogenea e uniforme sul territorio nazionale, lo schema di decreto prevede che il Ministero della salute predisponga, in collaborazione con le Regioni e le Province autonome, un modello di informativa. Tale modello, specifica il Garante, per garantire il pieno rispetto del principio di correttezza e trasparenza, dovrà essere necessariamente aggiornato in base alle eventuali modifiche e previamente sottoposto al parere dell'Autorità Garante stessa.

Ancora, in riferimento allo svolgimento della valutazione di impatto, il Garante ha ritenuto che i trattamenti descritti nello schema di decreto rientrassero senza dubbio tra quelli su cui è necessario effettuare una preventiva valutazione di impatto ai sensi dell'art. 35 del GDPR. Al riguardo l'Autorità reputa "non condivisibile" l'approccio che fa riferimento al cosiddetto "*average case*" che "*corrisponde ad una valutazione media che tiene conto delle differenze tra il modello centralizzato e quello distribuito*", poiché rischia di sottostimare vulnerabilità che, in tema di sicurezza, costituiscono il c.d. "anello debole" della catena e che possono quindi rendere pienamente efficaci le misure adottate. Alla luce di quanto sopra, il Garante invita il Ministero della salute e le Regioni e Province autonome a non utilizzare questa metodologia nella redazione e nell'aggiornamento delle valutazioni di impatto.

Nel Provvedimento in esame è stato anche imposto, in capo al Ministero della Salute, alle Regioni e alle Province autonome, l'obbligo di indicare un termine congruo entro il quale fornire informazioni sui trattamenti dei propri dati personali effettuati attraverso il FSE e avviare campagne di informazione volte a comunicare agli interessati l'integrazione automatica dei propri dati con il FSE comprensiva della loro relativa facoltà di opposizione, da manifestarsi entro 30 giorni.

Da ultimo, l'Autorità richiama l'attenzione del legislatore sulla necessità che le disposizioni attuative della medicina predittiva, dell'interconnessione dei sistemi sanitari e delle funzionalità del Sistema TS, nonché la disciplina della telemedicina, nella parte in cui prevedono la condivisione di dati e documenti con il FSE, siano conformi alla disciplina sulla protezione dei dati personali e coerenti con l'assetto e le misure di garanzia individuate nello schema di decreto sul FSE.

Il Fascicolo Sanitario Elettronico 2.0 ha ricevuto parere positivo anche dalla Conferenza Stato – Regioni il 2 agosto 2023. In tale occasione, la Conferenza delle Regioni e delle Province autonome ha formulato un'unica raccomandazione legata all'importanza di adottare, nel breve periodo, un successivo decreto che ampli i contenuti indicati nell'articolo 3 ("Contenuti del FSE") dello schema di decreto. Tale ampliamento, si specifica, deve tenere conto "*dei documenti clinico – sanitari, ad oggi già resi disponibili da alcune Regioni e Province autonome, per l'erogazione dell'assistenza territoriale e la presa in carico dei pazienti cronici/fragili*" e della *"possibilità anche per altre professioni sanitarie di poter accedere al FSE in consultazione per finalità di cura limitatamente alle informazioni necessarie in relazione allo svolgimento delle rispettive mansioni ed al tempo in cui si articola il processo di cura stesso*".

La Conferenza Stato – Regioni ha espresso la propria approvazione anche in riferimento ai flussi informativi del "*Sistema informativo per il monitoraggio dell'assistenza riabilitativa*" (SIAR), del "*Sistema informativo per il monitoraggio delle attività erogate ai consultori familiari*" (SICOF) e del "*Sistema informativo per il monitoraggio dell'Assistenza Domiciliare*" (SIAD).

Si sottolinea che, in riferimento al c.d. "SICOF", le Regioni e le Province autonome hanno reso l'assenso tecnico a condizione che sia prevista una fase transitoria relativa al primo semestre 2024 nella quale, pur mantenendo l'integrità del tracciato SICOF come definito nel Disciplinare tecnico, alcuni campi siano considerati temporaneamente facoltativi.

ELISA GROSSI

https://www.gazzettaufficiale.it/eli/id/2023/10/24/23A05829/sg

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9900433