Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

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

SOMMARIO

* Contributo non sottoposto a referaggio ai sensi dell'art. 2.2, lett. c), del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 306 del 21.12.2023.

ISSN 2239-8570

9. L'avvio da parte dell'AGCOM di una consultazione pubblica sulle modalità tecniche e di processo per l'obbligatoria verifica della maggiore età da parte dei gestori di siti web e dei fornitori delle piattaforme di condivisione video in attuazione della nuova normativa in materia di verifica della maggiore età per l'accesso ai siti pornografici [2024/1(9)SGh]
10. Il documento di indirizzo del Garante privacy italiano del 21.12.2023 sulla conservazione dei metadati della posta elettronica dei dipendenti e la successiva apertura di una consultazione pubblica con provvedimento del 22.2.2024 [2024/1(10)EG]
11. La notifica ad OpenAI da parte del Garante privacy italiano di un atto di contestazione di violazione del GDPR per il servizio ChatGPT [2024/1(11)SO]
12. Il Garante privacy Italiano apre una procedura istruttoria a carico di OpenAI per il servizio Sora [2024/1(12)SO]
13. Il provvedimento del Garante privacy italiano contro il Comune di Trento in materia di videosorveglianza e sicurezza urbana [2024/1(13)VR]
14. Il provvedimento dell'AGCM del 14.3.2024 contro TikTok per pratiche commerciali scorrette per il caso della 'cicatrice francese' [2024/1(14)LC]
15. Avviata indagine dell'AGCM contro Booking.com per presunto abuso di posizione dominante [2024/1(15)GD]
16. Il Garante privacy francese irroga una sanzione da 32 milioni di euro ad Amazon per monitoraggio invasivo delle prestazioni lavorative [2024/1(16)RM]
17. I Garanti privacy spagnolo e italiano si esprimono in senso contrario al progetto Worldcoin (la criptovaluta di Sam Altman) per il dispositivo "Orb" di scansione dell'iride [2024/1(17)CAT]
18. "Protecting Americans": le due leggi americane contenute nel National Security Act 2024 contro le applicazioni controllate da Cina, Russia, Iran e Corea del Nord (la legge contro TikTok) e contro qualunque trasferimento di dati sensibili in questi paesi [2024/1(18)SM]
19. Il Dipartimento di Giustizia USA contro Apple per pratiche anticoncorrenziali legate agli smartphone [2024/1(19)VH]
20. La sentenza del British Columbia Civil Resolution Tribunal del 14.2.2024 nel caso Moffatt vs Air Canada per informazione errata fornita dal chatbot del sito web della compagnia aerea [2024/1(20)SB]
21. La dichiarazione 'Artificial Intelligence and Society' firmata durante il G7 Italia 2024 [2024/1(21)VP]

ISSN 2239-8570

2024/1(1)SO

1. Il parere 8/2024 dell'EDPB del 17.4.2024 sulla validità del consenso al trattamento dei dati personali nel contesto dei modelli «acconsenti o paga» implementati sulle «piattaforme online di grande dimensioni»

Il 17.4.2024 il Comitato europeo per la protezione dei dati (**EDPB**) – che riunisce le Autorità nazionali per la protezione dei dati personali (o Autorità nazionali di controllo) dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS) - ha adottato un parere da tempo atteso, sollecitato dalle autorità di controllo olandese, norvegese e di Amburgo (Germania) a proposito dei c.d. modelli «acconsenti o paga» (in inglese «*consent or pay*», o anche «*Pay or Ok*») (**Parere 8/2024** o il **Parere**). Le predette autorità avevano chiesto all'EDPB di rendere un parere, ai sensi dell'art. 64(2) del Regolamento (UE) 2016/679 (**GDPR**), sulle circostanze e condizioni ricorrendo le quali debba ritenersi che i modelli «acconsenti o paga» relativi alla pubblicità comportamentale possano essere implementati in modo da consentire la prestazione di un consenso valido, in particolare sotto il necessario profilo della libertà dell'interessato di esprimere il consenso, anche tenendo conto del pronunciamento della Corte di Giustizia dell'Unione europea (**CGUE** o la **Corte**) nel caso C-252/2021 (su cui v. in questa Rubrica notizia n. 7 nel numero 3/2023 [2023/3(7)CAT].

È opportuno ricordare in proposito che, in quella occasione, nell'ambito di una controversia tra *Meta Platforms Inc*. e il *Bundeskartellamt* (Autorità federale garante della concorrenza, Germania) con sentenza del 4.7.2023, la CGUE aveva dichiarato che l'articolo 6(1)(b) GDPR - che prevede la base giuridica del contratto - debba essere interpretato nel senso che il trattamento di dati personali effettuato da Meta a proposito di Facebook, 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. In quella sentenza, la Corte ulteriormente negava di per sé rilevanza al fatto che un simile trattamento dei dati personali sia menzionato nel contratto oppure che esso sia soltanto utile per la sua esecuzione. Infatti – così statuiva la CGUE in quella sentenza - l'elemento determinante ai fini dell'applicazione della base giuridica del contratto è che il trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra quest'ultimo e l'interessato e che,

ISSN 2239-8570

pertanto, non esistano altre soluzioni percorribili e meno invasive. Quanto alla base giuridica del legittimo interesse, la CGUE dichiarava (sempre in quella sentenza) che la base prevista dall'articolo 6(1)(f) GDPR può essere considerata idonea per la pubblicità profilata solo se: *(i)* il titolare del trattamento abbia precisamente informato gli interessati in merito al legittimo interesse; *(ii)* tale trattamento sia effettuato entro i limiti di quanto strettamente necessario alla realizzazione di suddetto interesse; e *(iii)* 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. Riferendosi al caso concreto che formava oggetto dei quesiti rivoltile in quel giudizio, la CGUE concludeva dichiarando che, in conseguenza di quanto sopra, né il contratto, né il legittimo interesse (né tantomeno l'obbligo legale o l'interesse vitale) potessero essere considerati basi giuridiche idonee ai fini della pubblicità personalizzata operata da Meta.

Tornando al Parere 8/2024 in commento, l'EDPB ha ritenuto innanzitutto di limitarlo al campo dei modelli «acconsenti o paga» (attraverso i quali gli utenti sono richiesti di acconsentire al trattamento dei loro dati personali per finalità di pubblicità comportamentale) implementati da «piattaforme online di grandi dimensioni».

La definizione di «piattaforme online di grandi dimensioni» è stata resa dall'EDPB nel Parere al fine di circoscriverne il campo di applicazione. In particolare, si trova ivi scritto, al punto 23, che «il concetto di 'piattaforme online' può comprendere le 'piattaforme online' come definite nell'Articolo 3(i) del Digital Services Act», ma non è limitato da tale definizione. Ai sensi del Digital Services Act (**DSA**) (ossia il Regolamento UE 2022/2065), la piattaforma online è definita come un servizio di memorizzazione o *hosting* (come definito a sua volta nel DSA) che, su richiesta di un destinatario del servizio (come anche definito a sua volta nel DSA) immagazzina e diffonde informazioni al pubblico, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio o funzionalità minore del servizio principale e, per ragioni oggettive e tecniche, non possa essere utilizzata senza tale altro servizio e a condizione che l'integrazione di tale funzione o funzionalità nell'altro servizio non sia un mezzo per eludere l'applicabilità del DSA.

Si deve aggiungere che nel DSA non si trova la nozione di «piattaforma online di grandi dimensioni», cui si riferisce l'EDPB nel Parere, bensì (cfr. art. 33 DSA), quella, diversa, di «piattaforme online di dimensioni *molto* grandi» (**VLOPs**) [su cui v. in questa Rubrica le notizie 2023/2(5)RA e 2023/4(12)RA].

Ai fini del Parere 8/2024, l'EDPB ha dichiarato di ritenere necessario verificare, caso per caso, la ricorrenza di alcuni elementi per stabilire se il titolare di un trattamento debba essere considerato una «piattaforma online di grandi dimensioni», e ne ha indicato alcuni, in modo dichiaratamente non esaustivo, precisando che si tratta di elementi o requisiti non tutti necessariamente cumulativi. In primo luogo si afferma che, per essere tale, la «piattaforma online di grandi dimensioni» deve attrarre una «grande quantità di interessati come suoi utenti» (punto 25, Parere 8/2024). In

ISSN 2239-8570

secondo luogo, si chiede di esaminare quale sia la «posizione della società nel mercato» (punto 26, Parere 8/2024) e se essa tratti dati personali su 'larga scala', nel senso inteso dal Considerando 91 GDPR e chiarito dall'*Article 29 Working Party* a proposito del trattamento dei dati personali nel contesto dell'art. 37(1)(b) e (c) GDPR (punto 27, Parere 8/2024). Si specifica, infine (punto 28, Parere 8/2024), che questa nozione può comprendere, tra gli altri, certi titolari di trattamento dei dati personali delle VLOPs e dei «*gatekeepers*», questi ultimi come definiti dal Digital Markets Act [ossia dall'Art. 3(1) Regolamento (UE) 2022/1925, su cui v. in questa Rubrica notizia n. 3 nel numero 3/2023, [2023/3(3)RA].

Il Parere 8/2024 non si applica perciò a tutte le piattaforme online e in particolare non dovrebbe applicarsi alle testate giornalistiche online, molte delle quali hanno da tempo adottato modelli «*Pay or Ok*», tanto che il Garante privacy italiano ha aperto una istruttoria ormai più di un anno e mezzo fa per valutarne la compatibilità con il GDPR (sui comunicati del Garante privacy italiano del 18.10.2022, del 21.10.2022 e del 12.11.2022 di avvio di istruttorie a carico di testate editoriali online per iniziative di cookie wall e monetizzazione di dati personali v. in questa Rubrica notizia n. 11 del numero 4/2022 [2022/4(11)SO].

Venendo alla questione sottopostale, nel Parere si afferma che, «nella maggior parte dei casi», le «piattaforme online di grandi dimensioni» non saranno in grado di soddisfare i requisiti stabiliti dal GDPR per un consenso valido se sottopongono ai loro utenti un'alternativa secca tra acconsentire al trattamento dei dati personali per finalità di pubblicità comportamentale e pagare una somma di denaro. Secondo l'EDPB, le «piattaforme online di grandi dimensioni» dovrebbero offrire agli interessati una «alternativa equivalente» che non comporta un pagamento in denaro, eventualmente all'interno di un'opzione che non comporta pubblicità comportamentale, ad es. con forme di pubblicità che comportano il trattamento di un minor numero di dati personali o che non contemplano affatto il trattamento di dati personali. In questo modo, l'eventuale consenso (al trattamento dei dati personali, inerente all'opzione alternativa che comporta la pubblicità comportamentale) sarebbe valido, avuto riguardo ai requisiti del relativo giudizio, ed in particolare all'aspetto del 'detrimento'. L'EDPB fa riferimento in proposito alla tesi per la quale il consenso per essere prestato liberamente non deve causare un detrimento all'interessato, ciò che occorrerebbe – secondo l'EDPB – se l'unica alternativa al consenso fosse il pagamento di una somma di denaro, specialmente nei casi in cui il servizio reso dalla «piattaforma online di grandi dimensioni» abbia un ruolo di primo piano, o risulti decisivo per la partecipazione alla vita sociale o per l'accesso a reti professionali, ed ancor di più in costanza di formule che condizionano la partecipazione a gruppi di partecipanti ("*lock-in or network effects*").

Nel Parere si aggiunge essere necessario verificare caso per caso la presenza di uno squilibrio di potere tra interessato e titolare del trattamento dei dati, avuto riguardo a fattori quali la posizione della «piattaforma online di grandi dimensioni» nel mercato, l'esistenza di formule che condizionano la partecipazione a gruppi di partecipanti, l'affidamento che l'interessato ripone nel servizio e l'*audience* del medesimo servizio.

ISSN 2239-8570

Si dice essere altresì necessario verificare se l'«alternativa equivalente», eventualmente offerta all'interessato, possa considerarsi «genuinamente equivalente», e si offrono elementi da impiegare per il relativo giudizio (punti 120 ss. del Parere).

Il Parere sottolinea che i dati personali non possono considerarsi alla stregua di beni commerciabili e che i titolari del trattamento dovrebbero sempre valutare attentamente se sia necessario contemplare la richiesta di una somma di denaro (in alternativa alla richiesta del consenso al trattamento dei dati personali, per usufruire del servizio della «piattaforma online di grandi dimensioni»), e, in caso affermativo, l'adeguatezza del relativo importo nelle circostanze del caso concreto. In ogni caso, i titolari del trattamento dovrebbero evitare di applicare tariffe di importi tali da impedire agli interessati di compiere una scelta genuina, alla luce dei requisiti per un valido consenso e dei principi di cui all'art. 5 GDP, in particolare quello della correttezza. Nel Parere si sottolinea che le autorità di controllo dei vari Stati membri hanno il compito di valutare l'impatto di simili tariffe sulla libertà di scelta degli interessati, ai fini della corretta applicazione del GDPR.

Nel Parere si aggiunge che altri requisiti giuridici ai sensi del GDPR sono la granularità e la specificità (tale per cui l'interessato deve essere libero di decidere la finalità di trattamento per cui presta il consenso, e deve poter specificare di conseguenza il proprio consenso: in proposito, il Parere ricorda che gli utenti non devono essere sottoposti a modelli ingannevoli di interfacce sulle piattaforme online, c.d. *deceptive design patterns*) nonché l'informazione (tale per cui il consenso deve essere informato, e l'interessato deve essere messo in grado dal titolare del trattamento di avere una completa e chiara comprensione del valore, della portata e delle conseguenze delle possibili scelte alternative).

Infine, nel Parere si offrono chiarimenti sulla revoca del consenso (punti 169-177, Parere 8/2024) e sulla tempistica di riottenimento del consenso (punti 177-178, Parere 8/2024). Quanto alla revoca – richiamandosi anche i punti 46, 49, 110, 114, 116 e 117 delle linee guida EDPB sul consenso (Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1, adottate il 4 maggio 2020, su cui v. anche in questa Rubrica la notizia n. 5 del n. 2/2020 [2020/2(5)EMI]) nel Parere si ricorda innanzitutto che, ai sensi dell'art. 7(3) GDPR, è obbligatorio che il titolare del trattamento informi l'interessato del suo diritto di revocare il consenso, prima che il consenso sia effettivamente espresso. Si aggiunge che l'interessato debba essere messo nelle condizioni di esercitare il diritto di revoca senza detrimento (Considerando 42 GDPR), e che, in caso contrario, si debba concludere che il consenso non sia stato validamente ottenuto, con conseguente obbligo del titolare del trattamento di cancellare tutti i dati personali.

Nel contesto dei modelli «acconsenti o paga», come considerati nel Parere, viene in proposito operata una distinzione tra la volontà di esercitare il diritto di revoca, come tale, e l'eventuale volontà dell'utente del servizio (della «piattaforma online di grandi dimensioni») di continuare ad usufruire del servizio dopo la revoca del consenso. Al riguardo, nel Parere si afferma

ISSN 2239-8570

che la «piattaforma online di grandi dimensioni» debba evitare di dare all'utente l'impressione che la revoca del consenso abbia come conseguenza automatica la nascita del dovere di pagare una somma in denaro per il servizio. Al contrario, in questi casi, secondo il Parere, è necessario che, dopo l'eventuale esercizio del diritto di revoca del consenso da parte dell'utente, la «piattaforma online di grandi dimensioni» presenti nuovamente all'utente la scelta tra le varie opzioni alternative a disposizione dell'utente, secondo le modalità iniziali, che devono – nel senso indicato nel Parere – consentire sempre la libertà nella prestazione del consenso. Senza di ciò, dovrà ritenersi che non esisteva una possibilità di libera scelta nemmeno per la revoca del consenso, con la conseguenza di ritenere che nemmeno il consenso iniziale era stato prestato validamente.

Si chiarisce inoltre che mentre la decisione dell'utente di sottoscrivere la versione a pagamento del servizio quando egli aveva inizialmente optato per la prestazione del consenso al trattamento dei dati personali per la pubblicità comportamentale, costituisce una revoca del consenso, non è vero il contrario, ossia si specifica che il recesso dalla sottoscrizione della versione a pagamento del servizio non comporta automaticamente né equivale alla prestazione del consenso al trattamento dei dati personali.

Per quanto riguarda le conseguenze della revoca del consenso al trattamento dei dati personali per finalità di pubblicità comportamentale, si trova illustrato nel Parere che esse riguardano tutte le attività di trattamento autorizzate attraverso il consenso, ossia non solo la conservazione e/o l'accesso ai dati attraverso il dispositivo terminale per finalità di pubblicità comportamentale, ma anche l'ulteriore trattamento dei dati raccolti a tali fini, ciò che è particolarmente rilevante quando il titolare usi una grande rete di *marketing* per individuare le persone da assoggettare a pubblicità comportamentale attraverso una pluralità di siti web. In proposito, nel Parere si richiama la sentenza della CGUE nel caso C-129/21, c.d. sentenza *Proximus* (su cui v., in questa Rubrica, la notizia n. del numero 4/2022 [2022/4(9)CAT] nella quale la CGUE ha statuito che, allorquando più titolari del trattamento si basano su un singolo atto di consenso dell'interessato, è sufficiente per l'interessato dichiarare la propria revoca del consenso ad uno solo dei titolari, il quale è poi obbligato a comunicare tale revoca a tutte le persone ai quali il titolare abbia inoltrato i dati personali, con conseguente obbligo dei titolari così informati di inoltrare a loro volta tale informazione agli ulteriori eventuali titolari ai quali essi hanno comunicato i dati personali dell'interessato.

Per quanto riguarda il riottenimento del consenso, nel Parere si ricorda innanzitutto come il GDPR non stabilisca uno specifico periodo di tempo oltre il quale il titolare debba riottenere il consenso dell'interessato, e si afferma come appaia corretto, di conseguenza, affermare in linea generale che il relativo accertamento debba effettuarsi sulla base di un'analisi casistica. Tanto premesso, relativamente alla finalità di trattamento consistente nella pubblicità comportamentale, nel Parere si afferma che un termine congruo (decorso il quale debba riottenersi il consenso) sia pari ad un anno (1 anno), attesa la particolare invasività del trattamento condotto per tale finalità.

ISSN 2239-8570

SALVATORE ORLANDO

Parere 8/2024 dell'EDPB del 17.4.2024

2024/1(2)BG

2. La decisione dell'EDPS dell'8.3.2024 sull'uso di Microsoft 365 da parte della Commissione europea

La decisione del Garante europeo della protezione dei dati (**EDPS** o **Garante europeo**) dell'8.3.2024 sull'uso di Microsoft 365 da parte della Commissione europea (la **Commissione** e la **Decisione**) propone considerazioni di portata generale in relazione alle criticità e ai rischi derivanti dall'impiego di servizi di *internet communication technologies* (**ICT**) offerti da grandi fornitori operanti in paesi terzi, specialmente in termini di misure di sicurezza, trasferimento e garanzie adeguate, per il trattamento dei dati personali.

La Decisione, che consta di ben 180 pagine, è il punto di arrivo di un lungo percorso di confronto e valutazione svolto dall'EDPS di concerto con tutti i soggetti coinvolti, nonché di un contesto giuridico complesso e dinamico.

A seguito della sentenza della Corte di giustizia dell'Unione europea (**CGUE**) del 16.7.2020 nel caso C-311/18 a proposito della decisione di adeguatezza relativa al c.d. *Privacy Shield* per il trasferimento di dati personali negli Stati Uniti d'America (**sentenza *Schrems II***) - su cui v. in questa Rubrica la notizia n. 1 del numero 3/2020 [2020/3(1)CR] - che ha fissato e ribadito i principi per cui il trasferimento di dati personali verso paesi terzi deve essere subordinato al rispetto di un livello di protezione sostanzialmente equivalente a quello garantito dall'ordinamento dell'UE, e che le clausole contrattuali standard (**SCC**) adottate dalla Commissione sono valide solo fintantoché assicurano effettivamente tali garanzie, l'EDPS ha avviato diverse iniziative affinché le istituzioni, gli organi e gli organismi dell'UE si conformassero al dettato della medesima sentenza.

Difatti, nell'interesse di un approccio coerente alla protezione dei dati personali in tutta l'Unione il Regolamento (UE) 2018/1725 (**EUDPR** o **Regolamento**), che stabilisce le norme per la protezione dei dati nelle istituzioni, negli organi e negli organismi dell'UE, deve essere allineato ed armonizzato alle norme sulla protezione dei dati del Regolamento (UE) 2016/679 (**GDPR**). Di conseguenza, ogni volta che le disposizioni dell'EUDPR seguono gli stessi principi delle disposizioni del GDPR, le norme debbono, secondo la giurisprudenza della CGUE, essere interpretate in modo omogeneo.

In un'ottica di adeguamento graduale, l'EDPS ha innanzi tutto identificato, di concerto con le istituzioni europee, le più rilevanti operazioni di trattamento poste in essere attraverso *software* basati su *cloud* e servizi di infrastruttura o piattaforma *cloud* di grandi fornitori di ICT (quali i servizi

ISSN 2239-8570

cloud di Amazon e Microsoft 365, che erano già all'attenzione del Garante europeo, nonché dei singoli garanti nazionali).

In questo contesto, la "Strategia *Schrems II*" dell'EDPS, pubblicata il 29 ottobre 2020, mira a garantire e monitorare la conformità delle istituzioni dell'UE alla sentenza *Schrems II*, alla luce della crescente dipendenza delle organizzazioni istituzionali dai *software* e dalle infrastrutture *cloud*, e, di conseguenza, dai grandi fornitori di servizi IT, alcuni dei quali hanno sede negli Stati Uniti e sono pertanto soggetti a una legislazione che, secondo la sentenza *Schrems II*, consente attività di sorveglianza sproporzionate da parte delle autorità statunitensi.

L'indagine è stata avviata il 27 maggio 2021 sull'uso di Microsoft Office 365 fatto da parte della Commissione sulla base dell'accordo di licenza tra Microsoft e le istituzioni dell'UE, lo *Inter-institutional Licensing Agreement*, firmato il 7 maggio 2021 (il **2021 ILA**). L'obiettivo dell'indagine è stato quello di appurare se l'uso di Microsoft 365 da parte della Commissione, ivi inclusa ogni attività di trattamento di dati personali svolta per suo conto, fosse conforme al Regolamento.

Tale indagine ha seguito una precedente valutazione. In particolare, nel 2019 e nel 2020, l'EDPS aveva già condotto un'indagine sull'uso dei prodotti e dei servizi Microsoft da parte di organi ed istituzioni UE sulla base dello *Inter-institutional Licensing Agreement* firmato nel 2018 (il **2018 ILA**). In quella occasione, l'EDPS aveva verificato una serie di violazioni del Regolamento. Nel 2020, pertanto, l'EDPS aveva emesso un documento contenente le risultanze di quella prima indagine e le raccomandazioni del caso, queste ultime elaborate per aiutare le istituzioni e gli organi UE a rimediare alle violazioni allora riscontrate. La nuova indagine, culminata con la Decisione, è stata avviata dall'EDPS dopo aver ricevuto l'indicazione che molte delle più significative preoccupazioni emerse in quella occasione non erano state affrontate in modo efficace.

L'8 marzo 2024, l'EDPS ha concluso la propria indagine ed ha emesso la Decisione che ha accertato diverse violazioni dell'EUDPR ed ha imposto l'adozione di misure correttive entro il termine del 9 dicembre 2024. La fissazione di un termine piuttosto ampio è dovuta alla necessità di assicurare che la Commissione, in quanto istituzione fondamentale dell'Unione europea, non si trovi, a seguito della Decisione, a non poter eseguire i propri compiti istituzionali, e disponga di tempo per rimodellare e rendere conformi alla normativa i propri processi.

Le violazioni riscontrate sono essenzialmente riconducibili a tre macroaree principali: *(i)* limitazione delle finalità del trattamento, *(ii)* trasferimenti di dati personali al di fuori dell'UE, e *(iii)* divulgazione non autorizzata di dati personali.

Con riferimento al punto *sub (i)*, l'EDPS ha ritenuto che la Commissione abbia violato: la disposizione di cui all'art. 4(1)(b) del Regolamento, non avendo sufficientemente determinato i tipi di dati personali raccolti in relazione a ciascuna delle finalità del trattamento, né garantito che le finalità per cui Microsoft era autorizzata a raccogliere dati personali ai sensi del contratto fossero sufficientemente specifiche ed esplicite; la disposizione dell'art. 29(3)(a) del Regolamento non avendo fornito istruzioni

ISSN 2239-8570

documentate sufficientemente chiare per il trattamento; le disposizioni di cui agli artt. 4(2) e 26(1), in combinato disposto con quella dell'art. 30 del Regolamento, non avendo garantito che Microsoft trattasse i dati personali solo su istruzioni documentate della Commissione; la disposizione dell'art. 6 del Regolamento, non avendo valutato se le finalità dei trattamenti ulteriori operati fossero compatibili con gli scopi per cui i dati personali erano stati inizialmente raccolti; ed infine la disposizione dell'art. 9 del Regolamento, non avendo valutato se fosse necessario e proporzionato trasmettere i dati personali a Microsoft Irlanda e ai suoi sub-responsabili (inclusi gli affiliati) situati nello spazio economico europeo (**SEE**) per uno scopo specifico nell'interesse pubblico.

Con riferimento al punto *sub (ii)*, l'EDPS ha ritenuto che la Commissione abbia violato: la disposizione di cui all'art. 29(3)(a) del Regolamento, non avendo chiaramente previsto nel contratto di riferimento quali tipi di dati personali potessero essere trasferiti a quali destinatari in quale paese terzo e per quali scopi, e non avendo fornito a Microsoft istruzioni documentate a tal riguardo; le disposizioni di cui agli artt. 4(2), 46 e 48 del Regolamento, non avendo fornito garanzie adeguate affinché i dati trasferiti godessero di un livello di protezione sostanzialmente equivalente a quello nello SEE, poiché: innanzi tutto non aveva effettuato alcuna valutazione dell'impatto dei trasferimenti (**TIA**), né prima dell'avvio dei trasferimenti né successivamente, non ottenendo quindi le informazioni minime necessarie per determinare se fossero necessarie misure supplementari per garantire il livello di protezione sostanzialmente equivalente a quello goduto nell'UE, inoltre, non aveva attuato misure supplementari efficaci per i trasferimenti verso gli Stati Uniti che avevano luogo prima dell'entrata in vigore della decisione di adeguatezza degli Stati Uniti, alla luce della sentenza Schrems II. Inoltre, l'EDPS ha ritenuto che la Commissione abbia violato le disposizioni di cui agli artt. 4(2), 46 e 48(1) e (3)(a), del Regolamento vincolandosi alle SCC per i trasferimenti dalla Commissione a Microsoft Corporation senza aver chiaramente mappato i trasferimenti proposti, senza aver realizzato una valutazione d'impatto sui trasferimenti, senza aver incluso garanzie adeguate in tali SCC e non avendo ottenuto l'autorizzazione di tali SCC per i trasferimenti dalla Commissione a Microsoft Corporation dall'EDPS ai sensi dell'art. 48(3)(a) del Regolamento; la disposizione dell'articolo 47(1) del Regolamento, letto alla luce degli artt. 4, 5, 6, 9 e 46 del Regolamento, non avendo garantito che i trasferimenti avvenissero "esclusivamente per consentire l'esecuzione di compiti di competenza del titolare del trattamento".

Infine, con riferimento al punto *sub (iii)*, l'EDPS ha ritenuto che la Commissione abbia violato: la disposizione dell'art. 29(3)(a) del Regolamento, in particolare come interpretato alla luce della sentenza Schrems II, non avendo garantito che, per i dati personali trattati nello SEE, solo il diritto dell'UE o degli Stati membri vieti la notifica alla Commissione di una richiesta di divulgazione, e che, per i dati personali trattati al di fuori dello SEE, qualsiasi divieto di tale notifica non costituisca una misura necessaria e proporzionata in una società democratica che rispetta l'essenza dei diritti e delle libertà fondamentali riconosciuti dalla Carta; le

ISSN 2239-8570

disposizioni degli artt. 4(1)(f), 33(1) e (2), e 36 del Regolamento, non avendo valutato la legislazione di tutti i paesi terzi in cui si prevede di trasferire i dati personali e quindi non avendo garantito che Microsoft e i suoi sub-responsabili non effettuassero divulgazioni di dati personali che non sono autorizzate dal diritto dell'UE, e non avendo attuato misure tecniche e organizzative efficaci che garantissero il trattamento in conformità al principio di integrità e riservatezza all'interno dello SEE e, come parte di una equivalenza essenziale del livello di protezione, anche al di fuori dello SEE.

L'EDPS ha pertanto imposto alla Commissione, a partire dal 9 dicembre 2024, di sospendere tutti i flussi di dati, derivanti dall'utilizzo di Microsoft 365, a Microsoft e ai suoi affiliati e sub-responsabili situati in paesi al di fuori dell'UE/SEE non coperti da una decisione di adeguatezza.

In proposito, deve ricordarsi che – relativamente agli USA – dopo la sentenza *Schrems II*, la Commissione ha adottato il 10 luglio 2023 una decisione di adeguatezza sul nuovo piano di trasferimento dei dati personali UE-USA, cd. *Privacy Framework* (su cui v. in questa Rubrica la notizia n. 2 del numero 3/2023 [2023/3(2)CR].

Nella Decisione (punto 411, nota 716), si sottolinea che il 2021 ILA prevede trasferimenti di dati personali in ben 12 paesi non coperti da una decisione di adeguatezza, precisamente: Australia, Brasile, Cile, Cina, Egitto, Hong Kong, India, Malesia, Serbia, Singapore, Sud Africa, Emirati Arabi Uniti, nonché, prima dell'entrata in vigore della sopra menzionata decisione di adeguatezza del 10 luglio 2023, gli Stati Uniti d'America.

L'EDPS ha inoltre imposto, entro lo stesso termine, l'adozione di una serie di misure correttive, volte a portare le operazioni di trattamento derivanti dal suo utilizzo di Microsoft 365 in conformità con l'EUDPR. Innanzitutto, dovrà essere realizzata una mappatura completa dei trasferimenti, e la Commissione dovrà identificare nello specifico quali dati personali siano trasferiti a quali destinatari in quali paesi terzi, per quali scopi e con quali garanzie, con particolare attenzione agli ulteriori trasferimenti ("*onward transfers*"). La Commissione dovrà accertarsi che tutti i trasferimenti verso paesi terzi avvengano esclusivamente per consentire lo svolgimento di compiti nell'ambito di quanto richiesto dal titolare del trattamento, garantendo, attraverso vincoli contrattuali apposti ai sensi dell'articolo 29(3) del Regolamento ed attraverso altre misure organizzative e tecniche, che: tutti i dati personali siano raccolti per scopi espliciti e specificati; i tipi di dati personali siano sufficientemente determinati in relazione agli scopi per i quali sono trattati; qualsiasi trattamento da parte di Microsoft o delle sue affiliate o sub-responsabili sia effettuato solo su istruzioni documentate della Commissione; nessun dato personale venga ulteriormente trattato in modo non compatibile con gli scopi per i quali i dati sono stati raccolti, in conformità ai criteri stabiliti dall'articolo 6 del Regolamento; qualsiasi trasmissione a Microsoft Irlanda o alle sue affiliate e sub-responsabili situati nello SEE sia conforme all'articolo 9 del Regolamento; non avvenga alcuna divulgazione di dati personali da parte di Microsoft o dei suoi sub-responsabili, a meno che, per i dati personali trattati all'interno del SEE, la divulgazione sia richiesta dal

ISSN 2239-8570

diritto dell'UE o degli Stati membri, o, per i dati personali trattati al di fuori del SEE, la divulgazione sia richiesta dal diritto di un paese terzo che garantisca un livello di protezione sostanzialmente equivalente a quello del SEE, a cui Microsoft o i suoi sub-responsabili sono soggetti.

Come dichiarato da Wojciech Wiewiórowski, in occasione del comunicato stampa dell'11 marzo 2024: "*è responsabilità delle istituzioni, degli organi, degli uffici e delle agenzie dell'UE garantire che qualsiasi trattamento di dati personali al di fuori e all'interno dell'UE/SEE, anche nel contesto dei servizi basati su cloud, sia accompagnato da solide garanzie e misure di protezione dei dati. Questo è imperativo per garantire che le informazioni degli individui siano protette, come richiesto dal Regolamento (UE) 2018/1725, ogni volta che i loro dati sono trattati da, o per conto delle, istituzioni, degli organi, degli uffici e delle agenzie dell'UE* ".

BEATRICE GALLUCCI

Decisione dell'EDPS dell'8.3.2024

2024/1(3)RA

3. Digital Markets Act: la Commissione europea apre un'indagine contro Google, Apple e Meta

Il 25 marzo 2024 la Commissione europea (la **Commissione**) ha avviato un procedimento – ai sensi dell'art. 20 del Regolamento (UE) 2022/1925 relativo a mercati equi e contendibili nel settore digitale (**Digital Markets Act** o **DMA**) – al fine di verificare un'eventuale inosservanza delle disposizioni racchiuse nel Digital Markets Act da parte di Alphabet (con riguardo alle relative regole in materia di "*steering*" di Google Play e di "*self-preferencing*" di Google Search), di Apple (con riguardo alle relative regole in materia di "*steering*" dell'App Store e di "*choice screen*" di Safari) e di Meta (con riguardo al modello "*pay or consent*" adottato dalla società).

In particolare, la Commissione ha il sospetto che le misure adottate da questi tre *gatekeeper* (sulla cui nomina v. in questa Rubrica notizia n. 3 nel numero 3/2023, [2023/3(3)RA] non siano rispettose degli obblighi imposti a tali figure dal DMA. Segnatamente, la Commissione intende:

- valutare se le misure attuate da Alphabet e Apple in relazione ai loro *app store* – che impongono diverse restrizioni e limitazioni ai consumatori – violino l'art. 5(4) del DMA, il quale impone ai *gatekeeper* di consentire agli sviluppatori di app di consentire, a titolo gratuito, ai consumatori di accedere a offerte che si trovino al di fuori degli *app store* dei *gatekeeper*;
- stabilire se la visualizzazione dei risultati di Google Search fornita da Alphabet possa portare a un "*self-preferencing*" degli ulteriori servizi di Google (quali, ad esempio: Google Shopping, Google Flights e Google Hotels) rispetto ad analoghi servizi concorrenti. Ciò comporterebbe una violazione dell'art. 6(5) DMA,

ISSN 2239-8570

nella misura in cui produrrebbe un trattamento dei servizi offerti dai terzi non equo e discriminatorio rispetto a quelli offerti da Alphabet;

- comprendere se le misure adottate da Apple al fine di *(i)* consentire agli utenti finali di disinstallare facilmente qualsiasi applicazione *software* su iOS, *(ii)* modificare facilmente le impostazioni predefinite su iOS, e *(iii)* proporre agli utenti schermate di scelta che consentano agli utenti di selezionare facilmente un servizio predefinito alternativo come *browser* o motore di ricerca, siano pienamente conformi all'art. 6 (3) DMA, che impone ai *gatekeeper* di consentire "anche *a livello tecnico, agli utenti finali, di disinstallare con facilità qualsiasi applicazione software presente nel sistema operativo del gatekeeper*" e "*di modificare facilmente le impostazioni predefinite del sistema operativo, assistente virtuale e browser web del gatekeeper*";
- valutare se il modello "*pay or consent*" recentemente introdotto da Meta sia conforme all'art. 5(2) DMA, che richiede ai *gatekeeper* di ottenere il consenso (in conformità alle previsioni del GDPR) degli utenti qualora i medesimi *gatekeeper* intendano combinare o comunque utilizzare "*in modo incrociato*" i dati personali degli utenti per altri servizi forniti separatamente dal *gatekeeper*. In particolare, la Commissione ha il timore che la scelta imposta da tale modello possa non fornire una reale alternativa agli utenti. Peraltro, relativamente alla conformità alle previsioni del GDPR del modello "*pay or consent*" adottato da piattaforme online di gradi dimensioni, è sopraggiunto il Parere dell'EDPB del 17.4.2024, (su cui v. in questo numero della Rubrica la notizia n. 1 *supra* [2024/1(1)SO]).

La Commissione sta inoltre adottando altre misure investigative per raccogliere talune informazioni al fine di chiarire se: *(i)* Amazon possa lecitamente privilegiare i prodotti di marca propria sull'Amazon Store in conformità al già richiamato art. 6(5) DMA; *(ii)* la nuova struttura tariffaria di Apple e i nuovi termini e condizioni applicabili in relazione ad *app stores* alternativi (o alla distribuzione di *app* dal *web*) possa vanificare gli obiettivi posti dall'art. 6(4) DMA, secondo cui – tra l'altro – il "*gatekeeper consente, anche a livello tecnico, l'installazione e l'uso effettivo di applicazioni software o di negozi di applicazioni software di terzi che utilizzano il suo sistema operativo o che sono interoperabili con esso e consente l'accesso a tali applicazioni software o negozi di applicazioni software con mezzi diversi dai pertinenti servizi di piattaforma di base di tale gatekeeper*" e comunque "*non impedisce che le applicazioni software scaricate o i negozi di applicazioni software di terzi chiedano agli utenti finali di decidere se desiderano impostare come predefiniti tale applicazione software scaricata o tale negozio di applicazioni software*" e, ancora, il "*gatekeeper consente, a livello tecnico, agli utenti finali che decidono di impostare come predefiniti tale applicazione software scaricata o tale negozio di applicazioni software di effettuare facilmente tale modifica*".

Inoltre, ai sensi dell'art. 26 DMA, la Commissione ha imposto ad Alphabet, Amazon, Apple, Meta e Microsoft di conservare alcuni

ISSN 2239-8570

documenti che potrebbero essere utilizzati per valutare la loro conformità agli obblighi previsti dal DMA, in modo da preservare le prove disponibili e garantire l'applicazione della normativa.

Infine, la Commissione ha concesso a Meta una proroga di 6 mesi per conformarsi all'obbligo di interoperabilità previsto dall'art. 7 DMA con riguardo a Facebook Messenger.

L'obiettivo della Commissione è quello di concludere entro 12 mesi il procedimento avviato. Se il procedimento lo giustificherà, la Commissione informerà i *gatekeeper* interessati delle sue conclusioni preliminari e delle misure che intende adottare (o che il *gatekeeper* dovrebbe adottare per rispondere efficacemente alle preoccupazioni della Commissione). In caso di accertamento di una violazione della normativa prevista dal DMA, la Commissione potrà imporre multe per un importo pari a sino il 10% (e, in caso di reiterazione della violazione, sino al 20%) del fatturato mondiale totale della società. Inoltre, in caso di violazioni c.d. sistematiche, la Commissione potrà adottare ulteriori misure correttive, quali – ad esempio – l'obbligo per il *gatekeeper* di vendere un'attività, o parti di essa, ovvero il divieto per il *gatekeeper* di acquisire ulteriori servizi connessi all'inosservanza sistematica rilevata.

RICCARDO ALFONSI

Comunicato stampa della Commissione sull'apertura dell'indagine

2024/1(4)GDI

4. La sentenza della CGUE del 7.3.2024 nel caso C-604/22 sul *Real Time Bidding* della pubblicità online e sulle nozioni di 'titolare del trattamento' e di 'dato personale' a proposito della 'stringa del consenso' (*TC String*)

Come noto, gli annunci pubblicitari che vengono mostrati nei banner ai lati dei siti web o nelle app sono spesso frutto di diverse attività di profilazione dirette a confezionare il messaggio pubblicitario più in linea con gli interessi dell'utente.

Tra i tanti meccanismi che rendono possibile la pubblicità personalizzata o targettizzata, il sistema di "Real-Time Bidding" (**RTB**) è quello che mira ad abbinare ogni utente all'inserzione più in linea con i suoi interessi sulla base di un'asta competitiva. Tale sistema ha questo nome perché basato sulla vendita online, tramite asta istantanea ed automatizzata, di spazi pubblicitari su Internet destinati a specifici utenti. Nel momento in cui l'utente accede a un sito internet si mette in moto un sistema automatizzato che svolge, istantaneamente e in tempo reale, un numero enorme di aste per vendere gli spazi pubblicitari disponibili. Nell'asta si "offre" il profilo dell'utente agli inserzionisti e quello tra di loro che sarà in grado di offrire il prezzo più alto per l'annuncio pubblicitario più pertinente rispetto a tale profilo, si aggiudicherà l'asta, ossia la possibilità di mostrare il suo annuncio

ISSN 2239-8570

a quell'utente. In altre parole, quando gli utenti accedono a un sito Web o aprono un'applicazione che contiene uno spazio pubblicitario, le società tecnologiche che rappresentano migliaia di inserzionisti possono istantaneamente ("in tempo reale") fare offerte dietro le quinte per quello spazio pubblicitario attraverso un sistema di aste automatizzato gestito da algoritmi. Il sistema ha lo scopo di far visualizzare all'utente pubblicità di suo interesse e si basa sull'attività interamente automatizzata e coordinata di più soggetti tra i quali un particolare soggetto intermediario, l'Ad Exchange che si pone tra l'editore, ossia il titolare del sito internet o app che ha a disposizione degli spazi liberi che vuole monetizzare, e gli inserzionisti che, al contrario, hanno interesse ad occupare non solo quanti più spazi possibile ma, soprattutto, quelli nei siti raggiungibili dai soggetti che costituiscono i loro utenti di riferimento (target).

Fatta questa sintetica ma necessaria premessa, si può rilevare che all'interno del progetto o consorzio denominato "OpenRTB" l'associazione *IAB Europe* – la sezione europea, con sede in Belgio, della più grande associazione al mondo degli operatori di pubblicità online: *IAB* – ha sviluppato, diffuso e gestito un protocollo definito "*Transparency & Consent Framework*" (in seguito **TCF**), per risolvere uno specifico problema: registrare le preferenze e i consensi degli utenti ad essere profilati per finalità pubblicitarie e poi comunicare queste informazioni all'Ad Exchange che a sua volta lo gestirà nell'ambito delle sue aste. Tutto questo con la "promessa" che il trattamento dei dati personali sottesi a tali processi avvenga nel rispetto delle norme del Regolamento UE 2016/679 (**GDPR**) e riconoscendo agli utenti il più ampio potere di controllo sui propri dati.

In estrema sintesi, il TCF funziona nel seguente modo.

Quando gli utenti visitano un sito web o un'applicazione per la prima volta, apparirà un banner o altra interfaccia con la richiesta di consenso alla raccolta e condivisione dei propri dati o l'opposizione ai vari tipi di trattamento. Dietro queste interfacce c'è un altro soggetto, una piattaforma di gestione del consenso (*Consent Management platform* o **CMP**). Il TCF altro non è che un insieme di istruzioni che aiutano e indicano alla CMP come registrare e gestire le preferenze degli utenti. Tramite il TCF le preferenze vengono raccolte e poi codificate e memorizzate in una "stringa TC", (*TC String* in inglese, da *Transparency and Consent String*: di seguito **Stringa TC** o **Stringa di Consenso e Trasparenza** o **stringa di consenso**) che subito dopo sarà condivisa con le organizzazioni partecipanti al sistema RTB in modo che sappiano a cosa l'utente ha acconsentito/obiettato. La CMP inserisce inoltre un cookie -chiamato "**euconsent-v2**" - sul dispositivo dell'utente. La Stringa TC e il cookie euconsent-v2 vengono poi collegati all'indirizzo IP dell'utente rendendo quindi identificabile l'autore delle preferenze.

Dunque, il TCF svolge un ruolo fondamentale nell'architettura del sistema OpenRTB, poiché registra e manifesta le preferenze degli utenti riguardo a potenziali fornitori ai fini dell'offerta di pubblicità mirata.

Proprio il RTB e in particolare il TCF ha però ricevuto diverse segnalazioni e l'Autorità di controllo belga (*Gegevensbeschermingsautoriteit*, in seguito, **APD** o anche **BE DPA**),

ISSN 2239-8570

autorità competente nei confronti di IAB Europe che ha sede in Belgio, ha avviato una complessa istruttoria per verificare che davvero tale protocollo applicasse correttamente i principi del GDPR.

All'esito della sua istruttoria, con decisione n. 21 del 2.2.2022, l'APD ha ritenuto che IAB Europe agisca in qualità di titolare del trattamento per quanto riguarda la registrazione del consenso, delle obiezioni e delle preferenze dei singoli utenti come riassunti nella Stringa TC, e come contitolare con gli altri operatori del RTB per la raccolta e la diffusione delle preferenze, delle obiezioni e del consenso degli utenti e per il successivo trattamento dei loro dati personali (su questa decisione v. in questa Rubrica notizia n. 11 nel numero 1/2022 [2022/1(11)VR].

Pertanto, IAB Europe può essere ritenuta responsabile di eventuali violazioni del GDPR. Cosa di fatto avvenuta laddove l'autorità Belga ha poi accertato che IAB non ha: individuato una base giuridica adeguata per l'elaborazione delle Stringhe TC e il loro successivo trattamento da parte dei fornitori di *adtech*; investito in adeguata trasparenza e informazione agli utenti; adottato misure organizzative e tecniche adeguate, anche per garantire l'effettivo esercizio dei diritti dell'interessato e per monitorare la validità e integrità delle scelte degli utenti; redatto il registro delle attività di trattamento; nominato un DPO; né svolto alcuna valutazione d'impatto sulla protezione dei dati.

Sicché, ritenendo il TCF non rispettoso del GDPR tanto da determinare una perdita di controllo sui propri dati da parte degli utenti, l'APD ha inflitto a IAB Europe una sanzione amministrativa di 250.000 euro e una serie di misure correttive volte a rendere il TCF conforme al GDPR, come: individuare una base giuridica valida per il trattamento e la diffusione delle preferenze degli utenti, il divieto di utilizzare l'interesse legittimo come base per il trattamento dei dati personali da parte delle organizzazioni partecipanti al TCF, un più rigoroso controllo delle organizzazioni partecipanti.

Tale decisione è stata impugnata da IAB Europe dinanzi alla Corte d'appello di Bruxelles che, a sua volta, ha deciso di sottoporre una serie di questioni pregiudiziali alla Corte di Giustizia dell'UE (di seguito **CGUE** o la **Corte di giustizia**), vertenti, in particolare sulla natura di titolare o contitolare di IAB e sulla natura di dato personale della Stringa TC.

Con la sentenza del 7 marzo 2024 (la **Sentenza**), la CGUE si è quindi espressa sulle questioni sottopostele, in parte confermando l'operato dell'Autorità belga.

Con riferimento alla natura della Stringa TC – che di per sé già contiene le preferenze di un utente relative al suo consenso al trattamento, da parte di terzi, di dati personali che lo riguardano o relative alla sua eventuale opposizione a tale trattamento fondato su un asserito interesse legittimo – la Corte rileva che quando associata a dati supplementari, come l'indirizzo IP del dispositivo di un utente o ad altri identificatori, consente di individuare tale utente e, quindi, la Stringa TC contiene informazioni riguardanti un utente identificabile e costituisce così un dato personale. La CGUE ha aggiunto che, in tale contesto, la circostanza che, senza un contributo esterno, un'organizzazione di settore non possa né accedere ai dati trattati

ISSN 2239-8570

dai suoi membri né combinare detta stringa con altri elementi identificatori (quali in particolare l'indirizzo IP del dispositivo di un utente) non osta a che la stessa stringa costituisca un dato personale ai sensi della disposizione in parola. Nel fare quest'ultima precisazione, la Corte di Giustizia teneva conto dello specifico contesto nel quale l'associazione IAB Europe agisce ed in particolare la circostanza acclarata in giudizio per la quale la medesima associazione aveva contrattualmente il diritto di richiedere ed ottenere, ossia di esigere, dai suoi membri quel contributo esterno, e cioè «tutte le informazioni che le consentano di identificare gli utenti i cui dati sono oggetto di una TC String» (punto 48 della Sentenza).

Da questo punto di vista – ma non possiamo approfondire il tema in questa sede – può essere utile mettere a raffronto la nozione di dato personale fissata in questa sentenza, soprattutto sul punto della identificabilità, con quella utilizzata e formulata nella sentenza del Tribunale della CGUE del 26.4.2023 nel caso T-557/20 (su cui v. in questa Rubrica la notizia n. 7 nel numero 2/2023 [2023/2(7)GDI]) nonché, con quanto si trova statuito nella sentenza della CGUE resa nello stesso giorno della Sentenza nel caso C-479/22 (v. in particolare ai punti 55 ss.).

Invece, con riferimento alla qualificazione del ruolo di IAB nel sistema di TCF, la CGUE, dopo aver rilevato che la nozione di titolare del trattamento deve essere intesa in senso ampio affinché sia suscettibile di assicurare una tutela efficace e completa agli interessati, ha statuito che, al fine di verificare se uno o più soggetti siano titolari o contitolari del trattamento bisogna analizzare il relativo grado di influenza sul trattamento e in che misura tali soggetti definiscono finalità e mezzi del trattamento. Richiamando la propria giurisprudenza in termini, la Corte di giustizia ha aggiunto che l'esistenza di una situazione di contitolarità non si traduce in una responsabilità equivalente ma il grado di responsabilità di ciascun contitolare deve essere valutato tenendo conto di tutte le circostanze rilevanti del caso di specie.

Ciò premesso, la CGUE ha accertato che IAB Europe influisce, per scopi che gli sono propri (ossia il funzionamento del sistema di TCF) sul trattamento dei dati personali, imponendo ai propri membri di conformarsi alle norme e alle specifiche di funzionamento del TCF. In tal senso, la CGUE ha accertato che IAB Europe descrive con precisione e impone, tramite le istruzioni del TCF, il modo in cui i CMP sono tenuti a raccogliere le preferenze degli utenti nonché il modo in cui tali preferenze devono essere trattate al fine di generare una Stringa TC e poi il suo stoccaggio e la sua condivisione. Per queste attività IAB Europe è astrattamente qualificabile come titolare del trattamento. Contemporaneamente però, IAB Europe determina, congiuntamente con gli altri operatori del sistema di RTB, le finalità e i mezzi di un siffatto trattamento e le reciproche decisioni si integrano di modo che ciascuna di esse abbia un effetto concreto sulla determinazione delle finalità e dei mezzi dall'altro. Ciò ha determinato la CGUE a qualificare in concreto IAB Europe quale contitolare del trattamento di TCF, ossia quel trattamento che ha: come fine il favorire e consentire la vendita e l'acquisto di spazi pubblicitari su Internet da parte di detti operatori; e come mezzo l'individuazione di specifiche che descrivono

ISSN 2239-8570

il modo in cui i CMP sono tenuti a raccogliere le preferenze degli utenti relative al trattamento dei dati personali che li riguardano, nonché la gestione della Stringa TC; il tutto al fine di garantire la conformità al GDPR.

La CGUE ha precisato inoltre che: il fatto che IAB Europe non abbia accesso diretto alle Stringhe TC e, quindi, ai dati personali degli utenti non osta, conformemente alla giurisprudenza della medesima Corte (sentenza del 10.7.2018 nel caso C-25/17, punti 66 e 69, nonché giurisprudenza ivi citata), alla possibilità di qualificarla come «contitolare del trattamento»; è comunque da escludere che la contitolarità di tale organizzazione di settore nel trattamento di TCF si estenda automaticamente ai trattamenti successivi di dati personali effettuati da terzi, quali i fornitori di siti Internet o di applicazioni, per quanto riguarda le preferenze degli utenti ai fini della pubblicità mirata online.

Dunque, nel ritenere la Stringa TC un dato personale, la CGUE riconosce che IAB Europe sia il reale *dominus* del sistema di TCF, dal quale trae vantaggio e del quale stabilisce e impone ai suoi membri le specifiche di funzionamento come se fosse il titolare del trattamento, ma che giuridicamente esso sia da qualificarsi "contitolare" del trattamento insieme agli altri operatori del TCF, come le CMP.

Ciò sembra correggere, in punto di diritto, la ricostruzione dell'Autorità belga ma, di fatto, ne ratifica in parte le valutazioni perché IAB Europe continua a essere ritenuta responsabile di simili trattamenti di dati personali. Trattamenti che l'autorità belga ha ritenuto in violazione del GDPR e dei quali IAB Europe dovrà rispondere sulla base dei principi posti dalla Corte di giustizia: in misura proporzionata al suo grado di influenza e gestione del sistema. Per converso, IAB Europe non potrà essere ritenuta automaticamente responsabile per i trattamenti di dati personali effettuati da altri soggetti, al di fuori del sistema di TCF, per fini di pubblicità personalizzata online a meno che non sia dimostrato che essa abbia esercitato un'influenza sulla determinazione delle finalità e delle modalità di questi ultimi, circostanza che spetta al giudice del rinvio verificare alla luce dell'insieme delle circostanze pertinenti del procedimento principale.

GUIDO D'IPPOLITO

CGUE, 7.3.2024, C-604/22

2024/1(5)FG

5. La sentenza del 21.3.2024 della CGUE nel caso C-10/22 a proposito della 'Direttiva Barnier' (2014/26/UE) e dell'ammissibilità dell'attività di intermediazione delle EGI (entità di gestione indipendenti) in Italia

Il 21.3.2024, è stata pubblicata la sentenza della Corte di Giustizia dell'Unione europea (**CGUE** o la **Corte di giustizia**) in merito al caso C-

ISSN 2239-8570

10/22 Liberi Autori ed Editori (**LEA**) contro JAMENDO SA (**Jamendo**) (la **Sentenza**). Il Tribunale di Roma ha sollevato la questione sulla conformità della legislazione italiana alla direttiva 2014/26/UE (di seguito anche **Direttiva Barnier**), riguardante la gestione collettiva dei diritti d'autore e la concessione di licenze multi-territoriali per l'utilizzo online di opere musicali nel mercato interno. Si è chiesto se tale legislazione impedisca ai tribunali nazionali di escludere le entità di gestione indipendenti (**EGI**) di altri Stati membri dall'operare in Italia nel settore dei diritti d'autore.

Premettiamo brevemente, che, ai sensi della Direttiva Bernier le EGI e gli organismi di gestione collettiva (**OGC**) sono entrambi definiti come organismi autorizzati "per legge o in base a una cessione dei diritti, una licenza o qualsiasi altro accordo contrattuale, a gestire i diritti d'autore o i diritti connessi ai diritti d'autore per conto di più di un titolare dei diritti, a vantaggio collettivo di tali titolari come finalità unica o principale" ma si differenziano perché mentre gli OGC sono detenuti o controllati dai propri membri e/o non hanno scopo di lucro, le EGI sono soggetti giuridici indipendenti dai titolari dei diritti gestiti ed agiscono per scopo di lucro.

La questione sull'ammissibilità delle EGI in Italia è stata sollevata precedentemente, già nel 2014, quando la SIAE ha citato Soundreef Ltd. per concorrenza sleale, affermando che operasse in violazione dell'articolo 180 della l. 633/1941 sul diritto d'autore (**l.d.a.**). Il Tribunale di Roma ha sospeso il procedimento e ha deferito la questione alla CGUE. Il procedimento non è mai giunto a una decisione, poiché SIAE ha rinunciato a tutte le cause pendenti, a seguito dell'accordo raggiunto con Soundreef Ltd. e LEA il 10 aprile 2019.

Nel 2021, LEA, un OGC ai sensi della Direttiva Bernier, ha avviato un procedimento cautelare contro Jamendo, qualificata come EGI ai sensi della Direttiva Barnier, chiedendo di interrompere l'attività di intermediazione dei diritti d'autore in Italia, sostenendo che non fosse iscritta nell'elenco delle entità legittimate, non avesse i requisiti previsti dal decreto legislativo n. 35/2017 di attuazione della Direttiva Barnier (il **D.Lgs. 35/2017**), e non avesse informato il Ministero delle comunicazioni prima di iniziare l'attività.

Jamendo ha eccepito l'errata trasposizione della Direttiva Barnier nella legislazione italiana, affermando che questa non conferisce alle EGI i diritti previsti dalla medesima direttiva. Secondo l'articolo 180 l.d.a., solo la Società Italiana Autori ed Editori (**SIAE**) e gli altri organismi di gestione collettiva di cui al D.Lgs. 35/2017 possono intermediare i diritti d'autore in Italia, pertanto le EGI sono escluse, dovendo concludere accordi di rappresentanza con la SIAE o con altri OGC.

Il Tribunale di Roma ha sospeso il procedimento e ha sottoposto alla CGUE la questione se la Direttiva Barnier osti all'applicazione di una legge nazionale che riservi l'accesso al mercato dell'intermediazione dei diritti d'autore solo alle OGC, escludendo le EGI.

La Corte di giustizia ha stabilito che la legislazione nazionale che impedisce alle EGI di altri Stati membri di operare in Italia costituisce una restrizione alla libera prestazione dei servizi. Tale restrizione può essere giustificata solo per motivi imperativi di interesse generale, purché proporzionata. Tuttavia, nel caso in questione, la CGUE ha ritenuto che la

ISSN 2239-8570

restrizione vada oltre quanto necessario per proteggere il diritto d'autore, contravvenendo al diritto dell'Unione.

La Corte di giustizia ha chiarito che né le norme della direttiva 2000/31/CE sul commercio elettronico (per esclusione espressamente disposta dall'art. 3(3) in combinato con l'allegato della medesima direttiva) né quelle della direttiva 2006/13/CE sui servizi nel mercato interno (per esclusione espressamente disposta dall'art. 17, n. 11) della medesima direttiva) sono applicabili ai servizi di gestione dei diritti d'autore e dei diritti connessi, diversamente da quanto specificato dall'Avvocato Generale nelle sue Conclusioni, presentate il 25 maggio 2023.

Inoltre, nella Sentenza, la CGUE ha osservato che la Direttiva Barnier non armonizza in modo esaustivo le condizioni di accesso delle EGI all'attività di gestione dei diritti d'autore, lasciando agli Stati membri la competenza su questo tema, purché essi la esercitino n modo conforme al Trattato sul Funzionamento dell'Unione europea (**TFUE**). Nella Sentenza si torva statuito che non esiste un obbligo per gli Stati membri di garantire che i titolari dei diritti abbiano il diritto di autorizzare un'entità di gestione indipendente di loro scelta a gestire i loro diritti indipendentemente dallo Stato membro di nazionalità, di residenza o di stabilimento dell'entità di gestione indipendente o del titolare dei diritti di cui trattasi.

La Corte di giustizia ha stabilito che l'articolo 180 l.d.a. deve essere, piuttosto, valutato alla luce dell'articolo 56 TFUE in combinato disposto con la Direttiva Barnier.

In particolare, la CGUE ha statuito che la restrizione può essere legittimata solo se basata su ragioni di interesse pubblico imprescindibili e se adeguata a garantire il conseguimento di tale interesse, senza superare ciò che è strettamente necessario per raggiungere l'obiettivo prefissato. Nel caso in questione, pertanto, la Corte di giustizia ha dichiarato che è importante valutare se il trattamento differenziato tra gli organismi di gestione collettiva (OGC), come SIAE e LEA, e le entità di gestione indipendenti (EGI), come Jamendo, risponda a questo criterio.

A questo riguardo, ha osservato la CGUE, se da un lato è plausibile ritenere in astratto che un trattamento differenziato possa assicurare una protezione coerente e sistematica del diritto d'autore, considerando che la Direttiva Barnier impone alle EGI obblighi meno stringenti rispetto agli OGC, dall'altro deve ritenersi che la restrizione che vieta in modo assoluto alle EGI di svolgere qualsiasi attività di gestione dei diritti d'autore vada oltre ciò che è necessario per raggiungere tale obiettivo, e quindi contrasta con il principio sancito dall'articolo 56 TFUE.

Di conseguenza, la Sentenza ha statuito che una legislazione di uno Stato membro che impedisca, in modo generico e totale, alle EGI di un altro Stato membro di offrire servizi di gestione dei diritti d'autore in detto Stato membro non risulta conforme al diritto dell'Unione europea.

Tuttavia, nella Sentenza la Corte di giustizia ha anche riconosciuto che in simili circostanze uno Stato membro potrebbe introdurre specifici obblighi normativi per proteggere il diritto d'autore, ad esempio subordinando la fornitura di servizi di intermediazione dei diritti d'autore a determinati requisiti giustificati dal bisogno di proteggere il diritto d'autore.

ISSN 2239-8570

FRANCESCO GROSSI

CGUE, 21.3.2024, C-10/22

2024/1(6)FS

6. L'ordinanza del Consiglio di Stato dell'11.3.2024 di rigetto della richiesta cautelare di sospensiva del regolamento AGCOM sull'equo compenso per l'utilizzo online di pubblicazioni di carattere giornalistico.

Con ordinanza pubblicata in data 11 marzo 2024, il Consiglio di Stato in sede giurisdizionale (Sezione Sesta) ha annullato il provvedimento cautelare con cui il TAR Lazio aveva sospeso l'efficacia della delibera AGCOM n. 3/23/CONS del 19 gennaio 2023 (di seguito, la **Delibera**), avente ad oggetto "Regolamento in materia di individuazione dei criteri di riferimento per la determinazione dell'equo compenso per l'utilizzo online di carattere giornalistico di cui all'articolo 43-bis della legge 22 aprile 1941 n. 633" (il **Regolamento**), e degli allegati alla medesima Delibera, nelle more del giudizio rimesso alla Corte di Giustizia UE.

La Delibera, emanata in attuazione dell'art. 43-*bis* della l. 633/1941 sul diritto d'autore (**l.d.a.**), era stata impugnata da Meta Platforms Ireland Limited (**Meta**) sul rilievo che detta disposizione risulterebbe in contrasto con la normativa eurounitaria e con la Costituzione sotto vari profili, nonché in violazione delle indicazioni della legge delega (legge 22 aprile 2021, n. 53) circa il recepimento dell'art. 15 della Direttiva (UE) 2019/790 del Parlamento Europeo e del Consiglio del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale (**Direttiva Copyright nel Mercato Unico Digitale**). Condividendo i rilievi della ricorrente, con sentenza n. 18790/2023 del 12 dicembre 2023 il TAR Lazio ha rimesso alla Corte di Giustizia UE una serie di questioni pregiudiziali relative alle modalità di recepimento dell'art. 15 della Direttiva Copyright nel Mercato Unico Digitale e ha sospeso in via cautelare, nelle more del giudizio rimesso alla Corte, l'esecuzione degli atti impugnati.

La sospensiva è stata quindi impugnata da AGCOM dinanzi al Consiglio di Stato, lamentando la carenza di motivazione della decisione cautelare in ordine alla sussistenza dei relativi presupposti. In particolare, l'Autorità ha evidenziato come il TAR non abbia specificato quale sarebbe il danno grave ed irreparabile derivante dall'efficacia della Delibera (e, quindi, dal Regolamento) nelle more della decisione sulle questioni pregiudiziali, né abbia dato conto del bilanciamento effettuato tra i contrapposti interessi. Ha aggiunto che, contrariamente a quanto sostenuto da Meta, il Regolamento impugnato non introduce alcun obbligo di negoziazione in capo ai prestatori di servizi della società dell'informazione, né un obbligo di partecipare alla procedura delineata nel Regolamento stesso, limitandosi a disciplinare un procedimento amministrativo da attivare in caso di mancato accordo tra le

ISSN 2239-8570

parti e il cui provvedimento finale non ha alcuna valenza vincolante né per le parti, né tantomeno per il giudice ordinario cui le parti possono rivolgersi senza che sia obbligatorio un preliminare "passaggio" dinanzi all'Autorità. Ha evidenziato, inoltre, l'insussistenza del *periculum in mora* ove fondato su un ipotetico danno di natura meramente patrimoniale, in quanto tale sicuramente non irreparabile, a maggior ragione per un operatore economico di notevoli dimensioni come Meta.

Nel giudizio così instaurato, si è costituita Meta, contestando la fondatezza delle argomentazioni dell'Autorità e proponendo appello incidentale avverso i capi della sentenza che hanno respinto nel merito il secondo ed il terzo motivo del ricorso di primo grado. La FIEG – Federazione Italiana Editori Giornali è intervenuta nel giudizio a sostegno della posizione dell'Autorità.

Il Consiglio di Stato, esaminata la statuizione impugnata in relazione ai motivi alla base dell'istanza cautelare proposta in primo grado da Meta, ha rilevato che:

- i pregiudizi prospettati da Meta non sono concreti ed attuali, paventandosi solo un futuro "rischio sanzionatorio", né tantomeno gravi ed irreparabili risolvendosi al massimo in possibili perdite patrimoniali, come tali per definizione ristorabili;
- i pregiudizi che Meta potrebbe patire non possono dirsi conseguenza diretta ed immediata del Regolamento, ma delle eventuali iniziative che, sulla scorta di questo, AGCOM potrebbe assumere nei suoi confronti (iniziative avverso le quali Meta potrà esperire tutte le azioni, anche cautelari, che l'ordinamento prevede);
- il Regolamento allegato alla Delibera prevede, di fatto, un meccanismo per giungere ad un accordo, ma resta ferma la facoltà di adire il giudice competente;
- ove le informazioni detenute da Meta di cui il Regolamento impone la *disclosure* avessero natura di segreti commerciali, sussisterebbero le preclusioni alla loro rivelazione di cui agli articoli 622 e 623 del codice penale.

Alla luce di tali rilievi, tenuto conto della natura prevalentemente economica dell'interesse di Meta e della necessità di bilanciare i contrapposti interessi, il Consiglio di Stato ha ritenuto non sussistente il requisito del *periculum in mora* e, pertanto, ha rigettato l'istanza cautelare proposta da Meta nel giudizio dinanzi al TAR Lazio, disponendo la prosecuzione del procedimento per la trattazione dell'appello incidentale proposto da Meta.

FRANCESCO SANTONASTASO

Cons. Stato, ord., 11.03.2024, n. 894

2024/1(7)DI

ISSN 2239-8570

7. L'ordinanza della Cassazione n. 13073/2023 del 12.5.2023 sul danno non patrimoniale da violazione della normativa privacy

L'ordinanza n. 13073 della I sezione civile della Corte di Cassazione (pres. Genovese, rel. Terrusi) del 12.5.2023, relativa a una domanda di risarcimento ex art. 82 GDPR (**Ord. Cass. 13073/2023**), si colloca temporalmente a cavallo tra due sentenze rese dalla Corte di Giustizia UE (**CGUE**) sul diritto al risarcimento ai sensi della medesima disposizione del GDPR: la sentenza della CGUE del 4.5.2023, nel caso C-300/21, e la sentenza del 14.12.2023, nel caso C-340/21 (su queste due sentenze v., in questa Rubrica, la notizia n. 22 nel numero 4/2023 [2023/4(22)GR]).

Ord. Cass. 13073/2023 è stata resa in relazione ad una domanda di risarcimento ex art. 82 GDPR conseguente ad una illecita pubblicazione on-line da parte del Comune di Pisa di dati personali di una propria dipendente. I dati personali di quest'ultima erano stati diffusi sull'albo pretorio on-line di quell'ente, in una nota allegata alla determina relativa all'impegno del Comune di Pisa di versare il quinto dello stipendio della dipendente in favore della sua creditrice pignoratizia. Come riconosciuto dallo stesso Comune, la nota allegata alla determina e contenente i dati personali della debitrice/dipendente era stata diffusa on line per mero errore materiale dell'operatore incaricato alla pubblicazione della determinazione anonimizzata (il quale avrebbe inavvertitamente "spuntato" il campo "pubblica") ed era rimasta pubblica per un periodo limitato di tempo (poco più di 24 ore) prima di venire rimossa dall'amministrazione stessa.

La domanda risarcitoria della debitrice/dipendente è stata accolta dal Tribunale di Pisa (21.9.2021, n. 1204). La condanna è stata impugnata dal Comune di Pisa, lamentando tra l'altro ***(i)*** che la sentenza impugnata avesse fatto erronea applicazione del GDPR e dell'art. 2050 c.c., avendo il giudice pisano ignorato che la pubblicazione sull'albo pretorio fosse dipesa da un fatto non prevedibile (errore umano) a cui la pubblica amministrazione aveva immediatamente posto rimedio e; ***(ii)*** che la sentenza impugnata fosse nulla per motivazione apparente giacché il risarcimento era stato accordato dal Tribunale di Pisa in assenza di una prova del danno subito dalla debitrice /dipendente e per il solo fatto del fatto della violazione (c.d. danno *in re ipsa*).

L'Ord. Cass. 13073/2023 ha respinto entrambi questi argomenti, rigettando il ricorso proposto dal Comune di Pisa. In primo luogo, la Cassazione ha escluso la rilevanza del fatto dell'errore umano dell'incaricato alla pubblicazione sull'albo pretorio on-line quale evento idoneo ad escludere la responsabilità dell'ente, affermando "l'elementare ragione" per cui il Comune di Pisa, quale titolare del trattamento dei dati, risponde per il fatto anche colposo dei dipendenti. Per sottrarsi alla responsabilità, un titolare del trattamento deve dimostrare (non già la pronta reazione, che, si legge in Ord. Cass. 13073/2023, costituisce un suo "dovere", ma) che l'evento dannoso non gli sia in alcun modo imputabile ex art. 82(3) GDPR) In secondo luogo, l'Ord. Cass. 13073/2023 ha respinto la doglianza del Comune di Pisa relativa alla nullità della sentenza impugnata per motivazione apparente, rilevando che il Tribunale di Pisa avesse invero

ISSN 2239-8570

accertato l'esistenza di un danno determinato dalla violazione del GDPR commessa dal Comune di Pisa. Per quanto quel giudice di merito avesse menzionato il principio del danno *in re ipsa*, lo stesso aveva infatti dimostrato che il comportamento del Comune avesse causato un pregiudizio alla debitrice/dipendente, integrato dall'ostensione in un contesto socio-lavorativo dei suoi dati personali. Nel respingere tale ultima doglianza, la Suprema Corte ha chiarito *i*) che, come già nel quadro normativo e giurisprudenziale precedente al GDPR, l'illecito trattamento dei dati personali non costituisca un danno *in re ipsa* e; *ii*) che il diritto al risarcimento ex art. 82 GDPR non si sottragga alla verifica della gravità della lesione del diritto alla riservatezza del dato e ciò anche al fine di garantire il principio di solidarietà e di tolleranza della lesione minima (art. 2 Cost. it.) sempre ribadito dalla propria giurisprudenza.

Due principi di diritto sono stati dunque formulati dalla Suprema Corte nell'Ord. Cass. 13073/2023, nei seguenti termini:

«- in base alla disciplina generale del Regolamento (UE) 2016/679, cd. GDPR, il titolare del trattamento dei dati personali è sempre tenuto a risarcire il danno cagionato a una persona da un trattamento non conforme al regolamento stesso, e può essere esonerato dalla responsabilità non semplicemente se si è attivato (come suo dovere) per rimuovere il dato illecitamente esposto, ma solo "se dimostra che l'evento dannoso non gli è in alcun modo imputabile";

- l'esclusione del principio del danno in re ipsa presuppone, in questi casi, la prova della serietà della lesione conseguente al trattamento; ciò vuol dire che può non determinare il danno la mera violazione delle prescrizioni formali in tema di trattamento del dato mentre induce sempre al risarcimento quella violazione che concretamente offenda la portata effettiva del diritto alla riservatezza».

DANIELE IMBRUGLIA

Cass., ord., 12.05.2023, n. 13073

2024/1(8)BCo

8. Le Linee guida AGCOM 9/2023 per la protezione dei minori dai rischi del ciberspazio

Il 21.11.2023 è scaduto il termine per adeguarsi alle linee guida in materia di "sistemi di protezione dei minori dai rischi del cyberspazio", adottate dall'Autorità per le garanzie nelle comunicazioni (di seguito **AGCOM** o l'**Autorità**) con la delibera 9/23/CONS del 25.1.2023 pubblicata il 21.2.2023 (le **Linee guida**). Le Linee guide sono state emanate in attuazione dell'articolo 7-*bis* del decreto legge 30 aprile 2020, n. 28 (introdotto dalla legge di conversione 25 giugno 2020, n. 70), a tenore del quale, i contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice delle comunicazioni elettroniche (decreto legislativo

ISSN 2239-8570

1° agosto 2003, n. 259) "devono prevedere, tra i servizi pre-attivati, sistemi di controllo parentale [di seguito **SCP**] ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto".

L'intervento dell'Autorità, in seguito alle sollecitazioni ricevute in particolare dal Consiglio Nazionale degli Utenti (di seguito **CNU**), risponde "al fine di consentire l'effettiva applicazione dell'intervento legislativo sul punto e la piena attuazione dei diritti da questo attribuiti alla tutela dei minori" e si rende necessario "a tutela dei consumatori nell'assicurare che sia loro fornito un sistema di parental control, il più efficace e efficiente possibile dal punto di vista tecnico".

Le Linee guida, in numero di 10, sono corredate - anche nella parte dei *Considerato* della relativa delibera - da spiegazioni relative al loro procedimento di approvazione e alle loro *rationes*. Di seguito le elenchiamo e riassumiamo le principali spiegazioni.

«1. I fornitori di servizi di accesso ad Internet (ISP), qualsiasi sia la tecnologia utilizzata per l'erogazione del servizio, mettono a disposizione dei consumatori sistemi di parental control ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto».

I SCP vengono definiti come sistemi che quantomeno permettono di limitare o bloccare l'accesso a determinate attività da parte di un minore, impedendo l'accesso, tramite qualunque applicazione, a contenuti inappropriati per la sua età, e si chiarisce l'ambito di applicazione della disciplina rilevante, specificandosi che essa non si estende alla clientela di tipo *business* ma è limitata ai soli consumatori.

Per quanto riguarda l'attesa indicazione, da parte dell'Autorità, dei criteri per individuare le categorie dei contenuti da bloccare, l'AGCOM si è riservata di farlo separatamente e non in queste Linee guida, spiegando che ad un simile compito essa è tenuta sulla base di un altro comparto regolamentare, quello della programmazione audiovisiva, motivo per il quale l'Autorità ha dichiarato nelle Linee guida di ritenere opportuno pronunciarsi una sola volta. In particolare, nelle Linee guida, l'AGCOM ha richiamato l'art. 37 del D.Lgs. n. 208/2021 - recante il testo unico per la fornitura di servizi di media audiovisivi (TUSMA) adottato in attuazione della direttiva (UE) 2018/1808, c.d. nuova direttiva SMAV - rubricato "Disposizioni a tutela dei minori nella programmazione audiovisiva", nella parte in cui si attribuisce (già) all'AGCOM il compito di determinare una classificazione dei contenuti "a visione non libera" che possono essere offerti con una funzione di controllo parentale che inibisce l'accesso al contenuto stesso, salva la possibilità di disattivare tale funzione mediante codice segreto.

Pertanto, l'Autorità si è riservata, anche ai fini dell'art. 7-*bis* del decreto legge 30 aprile 2020, n. 28, di fornire, ai sensi del comma 12 dell'art. 37 del D.Lgs. n. 208/2021, criteri per l'individuazione dei programmi e servizi di cui ai commi 1 e 2 dello stesso, precisando al contempo tuttavia, ai fini delle Linee guida, che, nelle more, gli operatori, debbano tener conto di quanto già indicato dal comma 1 dell'art. 37 citato, laddove esso fissa già delle

ISSN 2239-8570

categorie, e aggiungendo che gli operatori possono utilizzare, nel rispetto di quella disposizione, le liste di domini/sottodomini e contenuti determinate secondo proprie specifiche di servizio e/o fornite da soggetti terzi individuati sulla base della serietà e capacità professionale avuto riguardo alla idoneità degli stessi a perseguire gli scopi della legge e alle migliori prassi.

Al riguardo, le Linee guida offrono una interessante panoramica sulla prassi formatasi ad opera dei principali operatori a proposito dei SCP e sulle categorie che sono state da essi già maggiormente individuate e che, secondo l'AGCOM, possono "essere assunte come generale indicazione":

- *Contenuti per adulti* (siti web riservati ad un pubblico maggiorenne, siti che mostrano nudità totale o parziale in un contesto sessuale pornografico, accessori sessuali, attività orientate al sesso. Siti che supportano l'acquisto online di tali beni e servizi).
- *Gioco d'azzardo/scommesse* (Siti che forniscono informazioni o promuovono il gioco d'azzardo o supportano il gioco d'azzardo online e/o scommesse).
- *Armi* (Siti che forniscono informazioni, promuovono o supportano la vendita di armi e articoli correlati).
- *Violenza* (Siti che presentano o promuovono violenza o lesioni personali, comprese le lesioni autoinflitte, il suicidio, o che mostrano scene di violenza gratuita, insistita o efferata).
- *Odio e discriminazione* (Siti che promuovono o supportano l'odio o l'intolleranza verso qualsiasi individuo o gruppo).
- *Promozione di pratiche che possono danneggiare la salute alla luce di consolidate conoscenze mediche* (Ad es. siti che promuovono o supportano l'anoressia e/o la bulimia, l'uso di sostanze stupefacenti illegali, di alcol o di tabacco).
- *Anonymizer* (Siti che forniscono strumenti e modalità per rendere l'attività online irrintracciabile).
- *Sette* (Siti che promuovono o che offrono metodi, mezzi di istruzione o altre risorse per influire su eventi reali attraverso l'uso di incantesimi, maledizioni, poteri magici o essere soprannaturali).

L'Autorità aggiunge infine che gli operatori dovranno comunicare all'Autorità, per l'espletamento della propria vigilanza, le categorie adottate, i fornitori terzi, e i criteri di selezione, e che gli operatori, naturalmente, una volta che l'Autorità avrà definito le categorie, dovranno tener conto di quanto stabilito e adeguare i criteri di scelta delle categorie.

«2. I SCP sono inclusi e attivati nelle offerte dedicate ai minori. Sulle altre offerte i SCP devono essere resi disponibili come attivabili da parte del titolare del contratto. I soggetti che possono eseguire le operazioni di disattivazione, riattivazione e configurazione sono i maggiorenni, titolari del contratto, e coloro che esercitano la potestà genitoriale sul minore».

«3. Gli ISP offrono gratuitamente i SCP ai consumatori e non impongono costi correlati all'attivazione, alla disattivazione, alla configurazione o al funzionamento degli stessi. La fornitura dei SCP non può essere vincolata alla sottoscrizione di qualsiasi servizio accessorio a pagamento».

ISSN 2239-8570

«4. Gli ISP pubblicano sui propri siti web guide chiare ed esaustive per l'utilizzo dei SCP ed offrono assistenza gratuita per l'attivazione, la disattivazione e la configurazione dei SCP attraverso call center con operatore umano ove selezionato dal consumatore secondo la vigente regolamentazione».

«5. I SCP prevedono, come funzionalità minima, almeno il blocco dei domini e siti ospitanti contenuti oggetto di filtro».

«6. Gli operatori possono completare le funzionalità dei SCP mediante l'implementazione della configurabilità degli stessi per fasce orarie e di memorizzazione dei siti visitati».

«7. I SCP realizzano le funzionalità necessarie per le finalità dei servizi in argomento, in conformità con il Regolamento UE n. 2015/2120 in materia di Open Internet».

«8. Le operazioni di attivazione, disattivazione e configurazione dei SCP devono essere realizzabili in modo semplice e intuitivo».

«9. I contenuti oggetto di filtro dei SCP sono configurabili dal titolare del contratto, con la possibilità di personalizzare almeno le categorie di contenuti oggetto di filtro. Gli operatori possono completare le funzionalità dei SCP mediante l'implementazione della configurabilità delle categorie di contenuti oggetto di filtro».

«10. Gli operatori di telefonia, di reti televisive e di comunicazioni elettroniche assicurano adeguate forme di pubblicità dei SCP preattivati, in modo da assicurare che i consumatori possano compiere scelte informate. In particolare, i SCP dovranno essere pubblicizzati sui siti web degli ISP, nelle carte dei servizi e con campagne di comunicazione mirate».

L'AGCOM, dopo aver precisato il concetto di pre-attivazione, ha affermato che il servizio di controllo parentale deve essere non soltanto gratuito, nella sua funzionalità base di filtro dei domini, ma anche obbligatoriamente incluso (pre-attivato) unicamente in relazione alle offerte dedicate ai minori. L'obbligo di pre-attivazione invece non esiste per le funzionalità più avanzate (servizi aggiuntivi rispetto al blocco dei siti) e per le altre offerte, non dedicate ai minori, le quali possono essere previste come facoltative, garantendo la massima trasparenza sui costi nel caso in cui siano a pagamento. Resta tuttavia fermo che anche per le offerte non dedicate ai minori, i servizi di controllo parentale, ove richiesti dal consumatore, devono essere gratuiti nelle loro funzionalità di base.

Circa le forme di autenticazione (SPID; codice PIN fornito all'atto dell'attivazione dell'utenza, comunicato in forma riservata, ad esempio tramite SMS; autenticazione nell'area riservata del sito web dell'operatore; OTP inviato via SMS o e-mail), l'Autorità chiarisce l'alternatività tra queste.

Quanto alle interfacce messe a disposizione del consumatore per attivare, disattivare e configurare il *parental control*, le Linee guida rimettono agli operatori la scelta dei requisiti delle modalità di implementazione delle interfacce dei SCP e dei canali di attivazione, disattivazione e configurazione dei SCP, a condizione che questi siano realizzabili in modo

ISSN 2239-8570

semplice ed intuitivo e che avvengano con le tempistiche consentite dalla capacità tecnologica disponibile.

In seguito all'analisi delle offerte di *parental control* da parte degli operatori, la quale ha evidenziato che gli stessi sono sovente forniti a titolo oneroso abbinati con altri servizi di protezione e sicurezza (c.d. "*bundling*"), l'Autorità ha disposto che il sistema base di *parental control* debba essere garantito gratuitamente e separatamente in maniera non abbinata ad altri servizi.

In relazione ai canali attraverso i quali gli operatori sono tenuti ad adempiere gli obblighi informativi circa la presenza dei SCP, l'Autorità ha indicato i seguenti: pubblicazione di contenuti su *home-page*; invio di e-mail; *self-care* nell'area cliente; documento di fatturazione per i clienti fissi; notifica via SMS per i clienti mobili nel caso di attivazione del servizio; documentazione contrattuale; call center; carta dei servizi. L'AGCOM ha invece ritenuto di non includere tra tali canali quello della chiamata diretta da parte dell'operatore, in ragione degli eccessivi e non proporzionati costi e della loro dubbia utilità alla luce del fenomeno del *teleselling illegale*, per il quale i consumatori potrebbero non rispondere alla chiamata.

Viene, inoltre, dichiarata non obbligatoria la comunicazione mediante sms ed eliminato l'obbligo per le *Pay TV* di dare notizia dell'esistenza dei SCP su fattura o *set-top box*, inserendo un obbligo per tutte le emittenti nazionali di dare evidenza di tali servizi.

Infine, per quanto riguarda l'assistenza ai consumatori, si trova spiegato che le Linee guida volutamente non hanno introdotto alcuna disposizione specifica, in quanto l'Autorità ha dichiarato di ritenere sufficiente il ricorso agli attuali canali di assistenza come previsti dalla delibera dell'AGCOM n. 79/09/CSP.

BRUNO CONCAS

Delibera AGCOM 9/2023
Allegato A alla Delibera AGCOM 9/2023
AGCOM Webinar 5.4.2024

2024/1(9)SGh

9. L'avvio da parte dell'AGCOM di una consultazione pubblica sulle modalità tecniche e di processo per l'obbligatoria verifica della maggiore età da parte dei gestori di siti web e dei fornitori delle piattaforme di condivisione video in attuazione della nuova normativa in materia di verifica della maggiore età per l'accesso ai siti pornografici

Successivamente alle Linee guida AGCOM 9/2023 per la protezione dei minori dai rischi del ciberspazio (su cui v. la notizia precedente in questo numero di questa Rubrica [2024/1(8)BCo]), è stato emanato il decreto-legge n. 123/2023 del 15.9.2023, poi convertito, con modificazioni, dalla legge n.

ISSN 2239-8570

159/2023 del 13.11.2023, recante "Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la *sicurezza dei minori in ambito digitale*".

L'art. 13-*bis* di questo decreto-legge (il **DL 123/2023**), inserito nel Capo IV intitolato *Disposizioni sulla sicurezza dei minori in ambito digitale*, è rubricato *Disposizione per la verifica della maggiore età per l'accesso a siti pornografici*.

Il comma 1 di questo articolo statuisce un 'divieto di accesso' dei minori a 'contenuti pornografici': "*È vietato l'accesso dei minori a contenuti a carattere pornografico, in quanto mina il rispetto della loro dignità e ne compromette il benessere fisico e mentale, costituendo un problema di salute pubblica*".

Il comma 2 del medesimo articolo prevede un obbligo a carico dei "*gestori di siti web e dei fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico*" di verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto.

Il comma 3 dello stesso articolo prevede che l'Autorità per le garanzie nelle comunicazioni (**AGCOM** o l'**Autorità**) emani un provvedimento che disciplini "*le modalità tecniche e di processo*" che i soggetti obbligati ai sensi del comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti. La medesima disposizione impone all'AGCOM di emanare un simile provvedimento "*sentita l'Autorità garante per la protezione dei dati personali*" (**Garante privacy**) ed "*assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo*".

Si prevede dunque che entro 6 mesi dall'emanazione del provvedimento dell'AGCOM di cui al comma 3, i soggetti obbligati ai sensi del comma 2 debbano adeguarsi al medesimo provvedimento (art. 13-*bis*, co. 4 DL 123/2023).

Infine, l'art. 13-*bis*, co. 5 DL 123/2023 prevede che l'AGCOM vigili sulla corretta applicazione del medesimo articolo e, in caso di inadempimento, contesti ai soggetti di cui al comma 2, anche d'ufficio, la violazione, applicando le disposizioni di cui all'articolo 1, co. 31, della l. 249/1997 (legge istitutiva dell'AGCOM), e che li diffida ad adeguarsi entro venti giorni.

L'ultima proposizione del co. 5 dell'articolo in commento prevede che in caso di inottemperanza alla diffida, l'AGCOM adotti "*ogni provvedimento utile per il blocco del sito o della piattaforma fino al ripristino, da parte dei soggetti di cui al comma 2, di condizioni di fornitura conformi ai contenuti della diffida dell'Autorità*".

In conseguenza di quanto sopra, dunque, l'AGCOM ha deliberato di aprire una consultazione pubblica propedeutica all'adozione del richiesto provvedimento ex art. 13-*bis* co. 3 DL 123/2023, in particolare adottando in sequenza due delibere (la prima strumentale alla seconda) e procurandosi un parere del Garante privacy.

Più precisamente: con delibera del 10.1.2024, n. 9/24/CONS (la **Prima delibera AGCOM**) l'Autorità ha avviato l'istruttoria; con provvedimento n.

ISSN 2239-8570

88 dell'8.2.2024, il Garante privacy ha espresso parere favorevole all'avvio della consultazione pubblica prevista dall'Autorità con la Prima delibera AGCOM (il **Parere del Garante privacy**); e con delibera del 4.3.2024, n. 61/24/CONS (la **Seconda delibera AGCOM**), nell'ambito del procedimento istruttorio avviato con la Prima delibera AGCOM, è stata infine avviata la consultazione pubblica per l'approvazione del provvedimento AGCOM di cui al comma 3 dell'art. 13-bis DL 123/2023.

Il documento di consultazione pubblica risulta allegato alla Seconda delibera AGCOM come allegato B (il **Documento di consultazione pubblica**).

Sembra interessante osservare come, dalla lettura della Seconda delibera, si evinca la consapevolezza da parte dell'Autorità che l'ambito applicativo rispetto al quale essa è stata richiesta di operare (divieto di accesso dei minori a contenuti pornografici), si inserisce in un contesto normativo significativamente più ampio.

Ed invero, nella Seconda delibera AGCOM si citano una pluralità di fonti che propongono più generalmente il tema del controllo dell'età degli utenti di contenuti online per finalità di protezione dei minori, mettendosi in luce che "la normativa vigente richiama più volte l'esigenza di implementare meccanismi di *age verification* stabilendo che i minori hanno diritto ad un livello più elevato di protezione dai contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale, anche introducendo misure più rigorose nei confronti di ogni servizio della società dell'informazione".

Nella Seconda delibera si richiamano al riguardo sia il regolamento (UE) 2022/2065 cd. Digital Service Act (**DSA**), che il regolamento (UE) 2016/679 (**GDPR**), che il D.Lgs. n. 208/2021 recante il testo unico per la fornitura di servizi di media audiovisivi (**TUSMA**) adottato in attuazione della direttiva (UE) 2018/1808 (**nuova direttiva SMAV**).

In particolare, si citano:

quanto al DSA, l'art. 28 DSA che richiede che tutti i fornitori di piattaforme on-line accessibili ai minori adottino misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori, *anzitutto mediante l'attivazione dei meccanismi di verifica dell'età*; l'art. l' 35(1)(j) DSA, ai sensi del quale i fornitori di piattaforme online di dimensioni molto grandi (**VLOPs**) e i motori di ricerca online di dimensioni molto grandi (**VLOSEs**) adottano misure di attenuazione dei rischi sistemici, tra cui "misure mirate per tutelare i diritti dei minori, *compresi strumenti di verifica dell'età e di controllo parentale*, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi";

quanto al GDPR, l'art. 8 GDPR che reca le condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;

quanto al TUSMA: l'art. 41 co. 7 TUSMA laddove si prevede che "la libera circolazione di programmi, video generati dagli utenti e comunicazioni commerciali audiovisive veicolati da una piattaforma per la condivisione di video il cui fornitore è stabilito in un altro Stato membro e diretti al pubblico italiano può essere limitata, *con provvedimento dell'Autorità*, secondo la procedura di cui all'articolo 5, commi 2, 3 e 4 del

ISSN 2239-8570

decreto legislativo n. 70 del 2003, *per i seguenti fini: a) la tutela dei minori da contenuti che possono nuocere al loro sviluppo fisico, psichico o morale a norma dell'articolo 38, comma"*; l'art. 42 commi 1, 6 e 7 del TUSMA a tenore dei quali "[comma 1] Fatti salvi gli articoli da 14 a 17 del decreto legislativo 9 aprile 2003, n. 70, *i fornitori di piattaforme per la condivisione di video soggetti alla giurisdizione italiana devono adottare misure adeguate a tutelare*: a) *i minori da programmi, video generati dagli utenti e comunicazioni commerciali audiovisive che possano nuocere al loro sviluppo fisico, mentale o morale* a norma dell'articolo 38, comma 3; [comma 6] Ai fini della tutela dei minori di cui al comma 1, lettera a), *i contenuti maggiormente nocivi sono soggetti alle più rigorose misure di controllo dell'accesso*; [comma 7] I fornitori di piattaforma per la condivisione di video sono in ogni caso tenuti a: [omissis] f) *predisporre sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori*; [omissis] h) dotarsi di sistemi di controllo parentale sotto la vigilanza dell'utente finale per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori".

Per questi motivi, tra i Considerando della Seconda delibera AGCOM, l'Autorità ha dichiarato espressamente che ritiene opportuno valutare, nell'ambito della consultazione pubblica di cui ha disposto l'avvio, "se il sistema di verifica dell'età delineato nel documento posto in consultazione mediante l'indicazione di requisiti generali e di indicatori di performance sia efficace, idoneo e funzionale a trovare applicazione, ai sensi del contesto normativo da ultimo richiamato, *anche con riferimento ad ulteriori tipologie di contenuti che potrebbero nuocere allo sviluppo fisico, mentale o morale dei minori*", con ciò facendo chiaro di ritenere che la consultazione pubblica da essa disposta con la Seconda delibera potrà essere utile anche nell'ambito dello studio delle tecniche di controllo dell'età per finalità ulteriori e non limitate all'applicazione del divieto di accesso ai contenuti pornografici da parte dei minori.

SIMONA GHIONZOLI

Prima delibera AGCOM
Parere del Garante privacy
Seconda delibera AGCOM
Documento di consultazione pubblica (Allegato B alla Seconda delibera AGCOM)

2024/1(10)EG

10. Il documento di indirizzo del Garante privacy italiano del 21.12.2023 sulla conservazione dei metadati della posta

ISSN 2239-8570

elettronica dei dipendenti e la successiva apertura di una consultazione pubblica con provvedimento del 22.2.2024

Richiamando l'attenzione su alcuni aspetti relativi alla disciplina di protezione dei dati e alle norme a tutela del lavoratore, l'Autorità garante per la protezione dei dati personali (**Garante privacy**), con il provvedimento n.642 del 21.12.2023, ha adottato un documento di indirizzo denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", che impone ai datori di lavoro pubblici e privati una serie di indicazioni per la gestione e conservazione dei metadati delle e-mail dei dipendenti.

Il documento in parola nasce a seguito di alcuni accertamenti condotti dal Garante privacy con riguardo ai trattamenti dei dati personali effettuati nel contesto lavorativo. In queste occasioni, il Garante privacy ha avuto modo di accertare il rischio che i programmi informatici per la gestione della posta elettronica possano raccogliere e conservare, per impostazione predefinita, in modo preventivo e generalizzato, i metadati relativi all'utilizzo degli account di posta elettronica in uso ai dipendenti (ad esempio, giorno, ora, mittente, destinatario, oggetto e dimensione dell'e-mail), "custodendo" gli stessi per un esteso e, spesso, eccessivo, arco temporale. In alcuni casi, è stata addirittura appurata l'impossibilità per i datori di lavoro di modificare le impostazioni di base del programma informatico al fine di disabilitare la raccolta sistematica dei dati, nonché di ridurre il periodo di conservazione degli stessi. Questa circostanza comporta (o potrebbe comportare) – secondo il Garante privacy – un indiretto controllo a distanza dell'attività del lavoratore da parte del datore di lavoro che richiede, inevitabilmente, il rispetto delle garanzie procedurali previste dall'art. 4, comma 1 della Legge 300/1970 (**Statuto dei Lavoratori**). Infatti, solo gli strumenti preordinati alla "registrazione degli accessi e delle presenze" e allo "svolgimento della prestazione" non soggiacciono ai limiti del primo comma dell'art. 4 dello Statuto dei Lavoratori. Tra essi – secondo l'interpretazione del Garante privacy – non rientrerebbero i programmi e servizi informatici di gestione della posta elettronica oggetto del provvedimento. Ebbene, partendo da tale assunto il Garante privacy ha imposto ai datori di lavoro:

i. di verificare accuratamente se i programmi e i servizi informatici di posta elettronica in uso ai dipendenti – soprattutto quelli forniti in modalità cloud o *as-a-service* – consentano al cliente (datore di lavoro) di modificare le impostazioni di base, impedendo la raccolta dei metadati o limitando il periodo di conservazione fino ad un limite massimo di 7 giorni, estensibile, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento, di ulteriori 48 ore;

ii. di procedere alla firma di un accordo con le organizzazioni sindacali o di ottenere il rilascio di un'autorizzazione dell'Ispettorato del Lavoro (ai sensi dell'art. 4 Statuto dei Lavoratori) qualora vi sia la necessità di perseguire esigenze organizzative o produttive che impongano di conservare i metadati per un lasso di tempo più esteso.

In forza dell'appena richiamato quadro giuridico, il Garante privacy sottolinea che l'utilizzo (*rectius* il trattamento) dei metadati, raccolti in

ISSN 2239-8570

assenza delle summenzionate garanzie, sarebbe illecito sotto molteplici profili.

In primo luogo, sarebbe ravvisabile un contrasto con la normativa in materia di protezione dei dati personali e con la summenzionata disciplina giuslavoristica. Nello specifico, vi sarebbe violazione degli artt. degli artt. 5(1)(a), 6 e 88(1) del regolamento (UE) 2016/679 (**GDPR**) nonché dell'art. 114 del D.Lgs. 193/2003 (**Codice privacy**) in relazione all'art. 4, co. 1, dello Statuto dei Lavoratori.

Inoltre sarebbe configurabile, secondo il Garante, anche la violazione art. 8 dello Statuto di Lavoratori e dell'art. 10 del D.Lgs. 10 settembre 2003, n. 276, richiamati espressamente dall'art. 113 del Codice privacy, in quanto "dagli elementi ricavabili dai dati esteriori della corrispondenza, come l'oggetto, il mittente e il destinatario e altre informazioni che accompagnano i dati in transito, definendone profili temporali (come la data e l'ora di invio/ricezione), nonché dagli aspetti quali-quantitativi anche in ordine ai destinatari e alla frequenza di contatto (in quanto anche questi dati sono, a propria volta, suscettibili di aggregazione, elaborazione e di controllo), è possibile acquisire informazioni riferite alla sfera personale o alle opinioni dell'interessato". In sostanza: "la generalizzata raccolta e la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, per un periodo di tempo esteso, in assenza di idonei presupposti giuridici, può, dunque comportare la possibilità per il datore di lavoro di acquisire, informazioni non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore".

Non solo. Secondo il Garante privacy verrebbero trasgrediti anche i principi di limitazione della conservazione - art. 5(1)(e) GDPR - di protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché quello di responsabilizzazione.

Per quanto riguarda le iniziative da adottare per la compliance normativa, il Garante privacy, dopo aver ribadito l'obbligo di "verificare con la dovuta diligenza che i programmi e servizi informatici di gestione della posta elettronica in uso ai dipendenti - specialmente nel caso in cui si tratti di prodotti di mercato forniti in modalità cloud o *as-a-service* - consentano al cliente (datore di lavoro) di modificare le impostazioni di base, impedendo la raccolta dei predetti metadati o limitando il periodo di conservazione degli stessi ad un limite massimo di sette giorni, estensibile di ulteriori 48 ore", specifica che i datori di lavoro "dovranno alternativamente, nel caso in cui i trattamenti di dati personali in questione si dovessero comunque rendere necessari per il perseguimento di esigenze organizzative o produttive, espletare le richiamate procedure di garanzia previste dalla disciplina di settore (art. 4 dello Statuto dei Lavoratori) o cessare l'utilizzo di tali programmi e servizi informatici".

In ogni caso, nelle more dell'eventuale espletamento delle procedure di garanzia, i predetti metadati non possono essere utilizzati.

Da ultimo, il Garante segnala la necessità di fornire ai lavoratori una informativa del trattamento dei dati personali prima di dare inizio allo stesso, quale essenziale e specifica precondizione per il lecito utilizzo dei dati raccolti attraverso strumenti tecnologici da parte del datore di lavoro.

ISSN 2239-8570

L'avvio di una consultazione pubblica

Gli stringenti limiti temporali di conservazione dei metadati imposti dal Garante con il provvedimento n.642 del 21.12.2023 hanno sollevato numerose perplessità. A conferma dello stato di "confusione" generato, il Garante privacy ha deciso di sospenderne l'efficacia e di accogliere le preoccupazioni in merito all'impatto e alle limitazioni che le società e i fornitori avrebbero dovuto gestire.

Con provvedimento n. 127 del 22.2.2024, il Garante privacy ha deliberato l'avvio di una procedura di consultazione pubblica di 30 giorni al fine di individuare un termine congruo per la conservazione dei metadati, presumibilmente superiore e più elastico rispetto a quello ipotizzato nel documento di indirizzo (7 giorni). Come emerge da questo provvedimento, obiettivo della consultazione è quello di acquisire osservazioni e proposte da parte di datori di lavoro pubblici e privati, di esperti della disciplina di protezione dei dati e da parte di tutti i soggetti interessati. Il Garante privacy ha quindi aperto la possibilità di rivedere e modificare la propria posizione, posponendo l'efficacia del documento di indirizzo al termine della consultazione pubblica pur sottolineando che "i contributi inviati dai partecipanti alla consultazione non precostituiscono alcun titolo, condizione o vincolo rispetto ad eventuali successive determinazioni del Garante".

ELISA GROSSI

Provvedimento del 21.12.2023
Provvedimento del 22.2.2024

2024/1(11)SO

11. La notifica ad OpenAI da parte del Garante privacy italiano di un atto di contestazione di violazione del GDPR per il servizio ChatGPT

Con comunicato del 29.1.2024, l'Autorità garante per la protezione dei dati personali (il **Garante privacy italiano** o il **Garante** o l'**Autorità**) ha dichiarato di aver notificato a OpenAI L.L.C. (**OpenAI**) un atto di contestazione di violazione della normativa in materia di protezione dei dati personali relativamente al servizio ChatGPT (il **Comunicato del 29.1.204** o il **Comunicato**). Nel Comunicato, il Garante specificava che la misura segue il provvedimento adottato dalla medesima Autorità il 30.3.2023, e che l'istruttoria svolta ha fatto emergere elementi che possono configurare una o più violazioni delle disposizioni del Regolamento (UE) 2016/679 (il **GDPR**). Nel Comunicato, si aggiungeva che OpenAI dispone di un termine di 30 giorni per proporre le sue difese, e che, nella definizione del procedimento, il Garante terrà conto dei lavori in corso nell'ambito della speciale *task force* costituita in seno al Comitato europeo per la protezione dei dati personali (**EDPB**).

Il contenuto dell'atto di contestazione notificato ad OpenAI non è stato pubblicato. Per quanto riguarda il precedente provvedimento del Garante del

ISSN 2239-8570

30.3.2023 e l'istruttoria, menzionati nel Comunicato, deve ricordarsi che lo scorso anno il Garante ha adottato due provvedimenti, a distanza di 10 giorni circa l'uno dall'altro, e che, in esito al primo, OpenAI ha sospeso il servizio ChatGPT in Italia mentre in seguito al secondo OpenAI ha riattivato il medesimo servizio.

Più in particolare:

- con provvedimento cautelare del 30.3.2023, il Garante, sulla base della contestazione di una violazione degli artt. 5, 6, 8, 13 e 25 GDPR, disponeva in via d'urgenza ai sensi dell'art. 58(2)(f) GDPR nei confronti di OpenAI, in relazione al suo servizio ChatGPT e in qualità di titolare del trattamento dei dati personali effettuato attraverso la relativa applicazione, la misura della limitazione provvisoria del trattamento dei dati personali degli interessati stabiliti nel territorio italiano (provvedimento del 30.3.2023 doc. web 9870832: il **Primo provvedimento**);
- il 31.3.2023 OpenAI annunciava la sospensione del servizio ChatGPT in Italia, che veniva disabilitato a far data dal 1.4.2023;
- con un secondo provvedimento, adottato in data 11.4.2023, il Garante disponeva la sospensione del Primo provvedimento a far data da - e quindi, condizionatamente a - l'adempimento di alcune prescrizioni da parte di OpenAI (provvedimento dell'11.4.2023 doc. web 9874702: il **Secondo provvedimento**) e, precisamente:

1) pubblicare sul sito internet di OpenAI un'informativa, *ex* art. 12 GDPR, per spiegare agli interessati anche diversi dagli utenti del servizio ChatGPT, i cui dati sono stati raccolti e trattati ai fini dell'addestramento degli algoritmi, le modalità del trattamento, la logica alla base del trattamento necessario al funzionamento del servizio, i diritti loro spettanti in qualità di interessati e ogni altra informazione prevista dal GDPR;

2) mettere a disposizione, sul sito Internet di OpenAI, almeno agli interessati, anche diversi dagli utenti del servizio ChatGPT, che si collegano dall'Italia, uno strumento attraverso il quale possano esercitare il diritto di opposizione rispetto ai trattamenti dei propri dati personali, ottenuti da terzi, svolti dalla società ai fini dell'addestramento degli algoritmi e dell'erogazione del servizio;

3) mettere a disposizione, sul proprio sito Internet, almeno agli interessati, anche diversi dagli utenti del servizio ChatGPT, che si collegano dall'Italia, uno strumento attraverso il quale chiedere e ottenere la correzione di eventuali dati personali trattati in maniera inesatta nella generazione dei contenuti o, qualora ciò risulti impossibile allo stato della tecnica, la cancellazione dei propri dati personali;

4) inserire un *link* all'informativa rivolta agli utenti dei propri servizi nel flusso di registrazione in una posizione che ne consenta la lettura prima di procedere alla registrazione, attraverso modalità tali da consentire a tutti gli utenti che si collegano dall'Italia, ivi inclusi quelli già registrati, al primo accesso successivo all'eventuale riattivazione del servizio, di prendere visione di tale informativa;

ISSN 2239-8570

5) modificare la base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento degli algoritmi, eliminando ogni riferimento al contratto e assumendo come base giuridica del trattamento il consenso o il legittimo interesse in relazione alle valutazioni di competenza della società in una logica di *accountability*;

6) mettere a disposizione, sul proprio sito Internet, almeno agli utenti del servizio, che si collegano dall'Italia, uno strumento facilmente accessibile attraverso il quale esercitare il diritto di opposizione al trattamento dei propri dati acquisiti in sede di utilizzo del servizio per l'addestramento degli algoritmi qualora la base giuridica prescelta ai sensi del punto 5) sia il legittimo interesse;

7) in sede di eventuale riattivazione del servizio dall'Italia, inserire la richiesta, a tutti gli utenti che si collegano dall'Italia, ivi inclusi quelli già registrati, di superare, in sede di primo accesso, un *age gate* che escluda, sulla base dell'età dichiarata, gli utenti minorenni;

- con comunicato del 13.4.2023 l'EDPB annunciava di aver costituito una task force su ChatGPT in conseguenza del Primo provvedimento;
- con comunicato del 28.4.2024 OpenAI annunciava di aver riaperto il servizio ChatGPT in Italia ritenendo di aver assolto alle prescrizioni del Garante, contenute nel Secondo provvedimento;
- con comunicato del 28.4.2024 il Garante esprimeva soddisfazione per "i passi in avanti" compiuti da OpenAI, pur dichiarando che avrebbe proseguito nella sua istruttoria e nel lavoro con l'apposita task force costituita in seno all'EDPB con le altre autorità di controllo europee;
- infine, con il Comunicato del 29.1.2024, il Garante dichiarava di aver notificato a OpenAI una contestazione di violazione delle disposizioni del GDPR.

Si attende dunque di sapere lo sviluppo del procedimento pendente dinanzi al Garante e di conoscere nel dettaglio le violazioni che formano oggetto della contestazione di cui al Comunicato del 29.1.2024.

Sulla costituzione della task force in seno all'EDPB per il caso ChatGPT e sui due provvedimenti del Garante italiano del 30.3.2023 e del 11.4.2023 v. più nel dettaglio in questa Rubrica notizie n. 3 e 5 del numero 1/2023 [2023/1(3)SO] [2023/1(5)SO]

SALVATORE ORLANDO

Comunicato stampa del 29.1.2024

2024/1(12)SO

12. Il Garante privacy Italiano apre una procedura istruttoria a carico di OpenAI per il servizio Sora

ISSN 2239-8570

Con un comunicato stampa in data 8.3.2024, l'Autorità garante per la protezione dei dati personali (il **Garante**) ha annunciato di aver aperto un'istruttoria nei confronti di OpenAI L.L.C. (**OpenAI** o la **Società**), in relazione al modello di intelligenza artificiale, denominato "Sora", in grado, da quanto dichiarato da OpenAI , di "creare video dal testo", ovvero "scene realistiche e fantasiose, partendo da istruzioni testuali".

Nel predetto comunicato, il Garante ha dichiarato di aver ritenuto necessario chiedere ad OpenAI di fornire una serie di chiarimenti in considerazione delle "possibili implicazioni che il servizio 'Sora' potrebbe avere sul trattamento dei dati personali degli utenti che si trovano nell'Unione europea e in particolare in Italia".

In particolare, secondo quanto si apprende dal medesimo comunicato, è stato chiesto ad OpenAI di comunicare al Garante entro 20 giorni se il nuovo modello di intelligenza artificiale sia stato applicato ad un servizio già disponibile al pubblico e se un simile servizio venga o verrà offerto ad utenti che si trovano nell'Unione europea, e in particolare in Italia.

Si apprende anche che il Garante ha chiesto alla Società di chiarire una serie di elementi, tra i quali: "le modalità di addestramento dell'algoritmo; i dati raccolti ed elaborati per addestrarlo, specialmente se si tratti di dati personali; se tra questi vi siano anche particolari categorie di dati (convinzioni religiose, filosofiche, opinioni politiche, dati genetici, salute, vita sessuale); quali siano le fonti utilizzate".

Infine, per il caso in cui un servizio rispondente al modello 'Sora' venga o verrà offerto a utenti che si trovano nell'Unione europea, il Garante ha chiesto ad OpenAI di "indicare se le modalità previste per informare utenti e non utenti e le basi giuridiche del trattamento dei dati forniti di quanti accedono al servizio siano conformi al Regolamento (UE) 2016/679".

SALVATORE ORLANDO

Comunicato stampa 08.03.2024

2024/1(13)VR

13. Il provvedimento del Garante privacy italiano contro il Comune di Trento in materia di videosorveglianza e sicurezza urbana

L'11.1.2024 il Garante per la protezione dei dati personali (**Garante privacy**) ha sanzionato il Comune di Trento (di seguito anche il **Comune**) per aver condotto, nell'ambito del programma "*Trento Smart city*", tre progetti di sperimentazione di sistemi di intelligenza artificiale, ponendo in essere massive e invasive acquisizioni di dati personali utilizzando telecamere, microfoni e reti sociali. I suddetti progetti, finanziati con fondi europei, erano volti a sviluppare soluzioni tecnologiche tese a migliorare la sicurezza urbana, secondo il paradigma della c.d. *smart urban security* e dunque si caratterizzavano per finalità di ricerca scientifica. Negli accordi

ISSN 2239-8570

stipulati per la fruizione dei fondi comunitari (c.d. "*grant agreements*") il Comune veniva identificato come soggetto leader e coordinatore ai fini della conduzione delle sperimentazioni nel proprio territorio in tre progetti di ricerca.

Più in dettaglio, il progetto "Marvel" ("*Multimodal Extreme Scale Data Analytics for Smart Cities Environments*") prevedeva l'acquisizione di filmati da quattordici telecamere di videosorveglianza già installate nel territorio comunale e di segnali audio da due microfoni appositamente collocati sulla pubblica via. I dati così raccolti venivano asseritamente anonimizzati, caricati periodicamente nel *data corpus* del progetto e analizzati dagli algoritmi.

Il progetto "Protector" ("*PROTECTing places of wORship*") era invece prettamente volto al contrasto dei crimini d'odio e delle minacce terroristiche, oltre alla valutazione delle misure di sicurezza e delle iniziative adottate dalle forze dell'ordine. La piattaforma in questione procedeva alla raccolta e all'analisi di filmati di videosorveglianza, privi di segnale audio, e di messaggi e commenti pubblicati sui social network. In seguito, l'analisi automatica di tali dati veniva effettuata mediante diversi software di IA. Più precisamente: l'esame dei dati visuali si basava su un componente di rilevamento automatico di oggetti, uno di tracciamento dei movimenti di questi e uno di rilevamento e categorizzazione delle anomalie in ambito urbano (situazioni di criminalità o devianza); l'esame dei messaggi d'odio religioso online si avvaleva di *dataset* generici e di dati appositamente raccolti, quali i commenti pubblicati su Twitter (ora, "X") e YouTube, al fine di cogliere indicatori di emozioni negative associate a temi religiosi o a rilevare la diffusione di *fake news* in tale ambito.

Ad essi si accompagnava anche il progetto "Precrisis", che tuttavia, al tempo dello svolgimento dell'istruttoria da parte del Garante privacy, risultava in fase di attivazione e per il quale non era stata ancora sviluppata alcuna componente software basata su AI.

Per i trattamenti condotti nell'ambito dei progetti illustrati, il Comune individuava come base giuridica l'art. 2-*ter* del D.Lgs. 196/2003 (di seguito, "**Codice privacy**"), in combinato disposto con l'art. 2 della l. regionale 2/2018 e gli artt. 3 e 7 dello Statuto comunale, che annoverano tra le funzioni amministrative di interesse locale lo sviluppo culturale, sociale ed economico della popolazione, al quale è riconducibile lo sviluppo del programma "*Trento Smart city*".

All'esito di un'approfondita istruttoria, il Garante privacy rilevava molteplici violazioni della disciplina in materia di protezione dei dati personali.

Innanzitutto, l'acquisizione di immagini dai filmati di videosorveglianza allo specifico fine di addestrare gli algoritmi dei progetti "Marvel" e "Protector" implicava il trattamento di dati personali relativi anche a reati e a categorie particolari, rispetto ai quali difettava un'idonea base giuridica. Parimenti deve dirsi per i messaggi e commenti acquisiti nelle reti sociali, idonei a rivelare le convinzioni religiose degli autori e di terzi. Più precisamente, i citati artt. 2 della l. regionale 2/2018 e 3 e 7 dello Statuto comunale attribuiscono al Comune una competenza del tutto generica e

ISSN 2239-8570

meramente programmatica e, come tali, non possono ritenersi idonei a soddisfare i requisiti fissati dagli artt. 5, par. 1, lett. *a*), 6, par. 1, lett. *e*), e parr. 2 e 3, e 9, par. 2, lett. *g*), del Regolamento (UE) 679/2016 (di seguito **GDPR** o il **Regolamento**), nonché dagli artt. 2-*ter*, 2-*sexies* e 2-*octies* del Codice privacy. Al riguardo, merita evidenziare che la Corte di Giustizia ha da tempo precisato che, ai sensi dell'art. 52 della Carta dei diritti fondamentali dell'Unione europea (**CDFUE**), le limitazioni ai diritti e alle libertà fondamentali – tra cui certamente rientrano il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, garantiti rispettivamente agli artt. 7 e 8 CDFUE – devono essere previste dalla legge con disposizioni chiare e precise, anche al fine di garantire il rispetto del principio di proporzionalità di cui all'art. 5 del Trattato sull'Unione europea (**TUE**). Analoghe considerazioni reca altresì la giurisprudenza della Corte europea dei diritti dell'uomo (**CEDU**).

Pertanto, il Garante privacy concludeva che il Comune, nell'ambito dei progetti "Marvel" e "Protector", aveva trattato dati personali, anche relativi a reati e appartenenti a categorie particolari in maniera non conforme ai principio di liceità, correttezza e trasparenza e in assenza di un'idonea base giuridica, in violazione degli artt. 5, par. 1, lett. *a*), 6, 9 e 10 GDPR, nonché artt. 2-*ter*, 2-*sexies* e 2-*octies* del Codice privacy.

Di poi, gravemente insufficienti dovevano ritenersi, secondo il Garante privacy, le tecniche di anonimizzazione impiegate dal Comune. Il punto è di particolare rilevanza, dacché, su tale presupposto, i dati acquisiti venivano successivamente condivisi con soggetti terzi coinvolti a vario titolo nei progetti.

In particolare, nell'ambito del progetto "Marvel", il Garante privacy rilevava, con riferimento ai dati audio, che la mera sostituzione della voce del soggetto parlante non assicurava affatto l'anonimizzazione. Infatti, dal contenuto delle conversazioni era possibile ricavare informazioni potenzialmente atte a identificare tanto il soggetto parlante quanto i suoi interlocutori o i soggetti terzi eventualmente menzionati. Inoltre, l'ampio ventaglio di argomenti astrattamente affrontabili non consentiva di escludere con sicurezza trattamenti di dati personali relativi a reati o a categorie particolari o comunque riguardanti soggetti vulnerabili (minori, lavoratori, soggetti fragili, ecc.).

Per quanto attiene ai file video utilizzati nell'ambito dei progetti "Marvel" e "Protector", assolutamente insufficiente era, ad avviso del Garante privacy, il semplice offuscamento dei volti delle persone e delle targhe dei veicoli ripresi. Infatti, gli interessati erano comunque potenzialmente identificabili, tramite: altre caratteristiche fisiche o elementi di contesto (*e.g.* corporatura, abbigliamento, caratteristiche fisiche particolari, ecc.); informazioni detenute da terzi (*e.g.* notizie di cronaca, testimonianze di persone presenti sulla scena filmata, ecc.); informazioni desumibili dalla localizzazione della telecamera; informazioni relative al percorso effettuato da una determinata persona, individuata nelle immagini video mediante le predette caratteristiche fisiche e gli elementi di contesto. Al riguardo, il Garante privacy precisava che per "identificazione", "non si intende solo la possibilità di recuperare il nome e/o l'indirizzo di una

ISSN 2239-8570

persona, ma anche la potenziale identificabilità mediante individuazione, correlabilità e deduzione" (Gruppo di Lavoro Art. 29, "Parere 05/2014 sulle tecniche di anonimizzazione", WP216; cfr. anche provvedimenti del Garante privacy 18.7.2023, n. 311; 2.3.2023, n. 65; 25.2.2021, n. 68; 2.7.2020, n. 118 e 119).

Infine, con riferimento ai messaggi e commenti pubblicati sulle reti sociali acquisiti nell'ambito del progetto "Protector", il Garante privacy rilevava che i dati relativi agli utenti di "Twitter" (ora "X") erano stati soltanto pseudonimizzati mediante sostituituzione del nome utente reale con un ID generato casualmente e automaticamente. Com'è noto, i dati pseudonimizzati sono a tutti gli effetti dati personali, giacché mediante l'impiego di informazioni aggiuntive è possibile risalire all'identità degli interessati.

Criticità emergevano anche sotto il profilo della trasparenza.

Laddove si impieghino sistemi di videosorveglianza, il titolare del trattamento, oltre a rendere l'informativa di primo livello mediante l'apposita segnaletica, deve fornire agli interessati anche "informazioni di secondo livello", le quali devono contenere tutti gli elementi obbligatori a norma dell'art. 13 GDPR ed essere facilmente accessibili per l'interessato. Ebbene, nel caso di specie l'informativa di primo livello, pur menzionando i progetti "Marvel" e "Protector", non faceva specificamente riferimento alla finalità di trattamento connessa alla ricerca scientifica, lasciando erroneamente intendere agli interessati che anche i trattamenti posti in essere nell'ambito dei due progetti fossero riconducibili alle finalità di sicurezza urbana. A proposito della finalità del trattamento per motivi di ricerca scientifica, il Garante privacy faceva notare le ulteriori incongruenze del Comune, che, da un lato, aveva dichiarato di ritenere pertinenti le disposizioni di cui alle regole deontologiche per finalità di ricerca e statistiche di cui all'Allegato A.5 al Codice privacy ("*trattandosi di progetti di ricerca, sono inoltre state ritenute pertinenti le disposizioni dell'Allegato A.5 del [Codice] contenente le Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, in conformità all'art. 89 del [Regolamento]*"), ma dall'altro lato, e al contempo, aveva precisato di non ritenere questa la base giuridica del trattamento ed inoltre manifestava di difettare dei requisiti soggettivi previsti da quelle stesse regole deontologiche. In particolare, sotto quest'ultimo aspetto, il Garante privacy osservava quanto segue: "il Comune non ha comprovato che tra le proprie competenze istituzionali figuri anche l'attività di ricerca scientifica, non potendo, pertanto, lo stesso essere considerato un 'istituto o ente di ricerca' ai fini dell'art. 1, par. 1, lett. d), delle predette Regole deontologiche; né il Comune ha comprovato di aver agito, nell'ambito dei due progetti, attraverso il proprio Ufficio di statistica, istituito ai sensi del d.lgs. 322/1989. La finalità di ricerca scientifica non è annoverata tra le competenze istituzionali del Comune e, pertanto, i trattamenti di dati personali in questione non possono ritenersi autorizzati ai sensi del quadro giuridico europeo e nazionale che definisce, tra le altre, i presupposti soggettivi e oggettivi per effettuarli (v. artt. 6 e 89 del Regolamento; art. 106

ISSN 2239-8570

del Codice; Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica)".

Non solo. Tornando alla questione dell'informativa, il Garante notava che, sebbene l'informativa contenesse un riferimento all'audio, non veniva indicato chiaramente che il contenuto delle conversazioni dei destinatari dell'informativa sarebbe stato acquisito e trattato ai fini del progetto Marvel. Inoltre, quanto alla menzione dei diritti degli interessati, l'informativa di primo livello si limitava a menzionare il solo diritto di accesso ai dati, accompagnandovi un generico riferimento agli "altri diritti riconosciuti dalla legge", senza un espresso rinvio agli artt. 15-22 GDPR, in violazione dell'art. 13, par. 2, lett. *b*) GDPR. Dal canto suo, l'informativa di secondo livello ometteva di menzionare i microfoni impiegati nell'ambito del progetto "Marvel" per la raccolta dell'audio.

Le informative mancavano poi di illustrare i trattamenti di dati personali degli utenti che avevano pubblicato messaggi sulla piattaforma "Twitter" (ora, "X") o commenti sulla piattaforma "YouTube" nell'ambito del progetto "Protector". Infine, la sezione "diritti dell'interessato" non conteneva alcun riferimento al diritto di proporre reclamo a un'autorità di controllo, in violazione dell'art. 13, par. 2, lett. *d*) GDPR.

Alla luce di questi rilievi, il Garante accertava la violazione degli artt. 13, par. 1, lett. *c*) ed *e*), par. 2, lett. *a*), *b*) e *d*), e 14 GDPR. In aggiunta, alla luce della gravità, del carattere trasversale e delle conseguenze delle violazioni commesse dal Comune in punto di trasparenza del trattamento, veniva altresì accertata la violazione dei principio di liceità, correttezza e trasparenza di cui all'art. 5, par. 1, lett. *a*) GDPR.

Ulteriori censure venivano avanzate dal Garante privacy con riferimento al perimetro di comunicazione dei dati estratti nell'ambito dei progetti menzionati. Più precisamente: in seno al progetto "Marvel", i contenuti audio e video venivano condivisi con i partner del progetto; in seno al progetto "Protector" i contenuti video, assieme ai nomi utente pseudonimizzati degli autori dei messaggi/commenti pubblicati sulle piattaforme "Twitter" (ora, "X") e "YouTube", venivano condivisi, oltre che con i partner, anche con la Commissione europea e i revisori del progetto. Non solo. Nell'ambito del progetto "Protector", la comunicazione raggiungeva altresì la Polizia di Anversa e il Ministero dell'Interno della Bulgaria. Orbene, alla luce di quanto accertato in merito all'inadeguatezza delle tecniche di anonimizzazione impiegate, alla natura di dati personali delle informazioni pseudonimizzate e all'assenza di un quadro giuridico di riferimento idoneo a fondare la conduzione dei progetti di ricerca (v. par. 3.4), la comunicazione dei dati personali in questione veniva dichiarata non conforme al principio di liceità, correttezza e trasparenza e violativa degli artt. 5, par. 1, lett. *a*), 6, 9 e 10 GDPR, nonché degli artt. 2-*ter*, 2-*sexies* e 2-*octies* del Codice privacy. A corroborazione, veniva rimarcato che la condivisione dei messaggi/commenti presenti sulle reti sociali comportava che la trasmissione anche dati personali relativi a reati e a categorie particolari di dati, quali le convinzioni religiose.

Infine, l'impiego di nuove tecnologie e la sorveglianza sistematica di zone accessibili al pubblico e i conseguenti rischi che i due progetti

ISSN 2239-8570

implicavano, avrebbero imposto al Comune, in qualità di titolare del trattamento, di effettuare una valutazione d'impatto sulla protezione dei dati. All'esito dell'istruttoria, tuttavia, non poteva dirsi comprovata l'avvenuta redazione da parte del Comune della valutazione in questione prima di porre in essere i trattamenti di dati personali nell'ambito dei progetti "Marvel" e "Protector", con violazione anche degli artt. 35 e 36, par. 1, GDPR.

Alla luce di tutto quanto in precedenza illustrato, il Garante dichiarava l'illiceità del trattamento di dati personali effettuato dal Comune, per aver posto in essere trattamenti di dati personali: in maniera non conforme al principio di liceità, correttezza e trasparenza, in violazione dell'art. 5, par. 1, lett. *a*) GDPR; in assenza di base giuridica, in violazione degli artt. 6, 9 e 10 GDPR, nonché degli 2-*ter*, 2-*sexies* e 2-*octies* del Codice privacy; omettendo di fornire agli interessati taluni elementi informativi richiesti dalla disciplina in materia di protezione dei dati, in violazione degli 13, par. 1, lett. *c*) ed *e*), e par. 2, lett. *a*), *b*) e *d*), e 14 GDPR; comunicando a terzi dati personali, anche relativi a reati e a categorie particolari (convinzioni religiose), in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. *a*), 6, 9 e 10 GDPR, nonché 2-*ter*, 2-*sexies* e 2-*octies* del Codice privacy; omettendo di redigere una valutazione d'impatto sulla protezione dei dati conforme ai requisiti previsti dalla normativa in materia di protezione dei dati, in violazione dell'art. 35 GDPR.

Di conseguenza, il Garante ingiungeva al comune il pagamento di una sanzione pecuniaria *ex* art. 83, par. 1 GDPR fissata nella misura di 50.000€ e, quali misure correttive ai sensi dell'art. 58, par. 2, lett. *d*), *f*) e *g*) GDPR, il divieto di trattare i dati personali già raccolti nell'ambito dei progetti "Marvel" e "Protector" e la cancellazione degli stessi.

VALENTINO RAVAGNANI

Provvedimento 11.01.2024

2024/1(14)LC

14. Il provvedimento dell'AGCM del 5.3.2024 contro TikTok per pratiche commerciali scorrette per il caso della 'cicatrice francese'

Il provvedimento del 14.3.2024 in epigrafe si pone in esito all'attività istruttoria dell'Autorità Garante della Concorrenza e del Mercato (di seguito, **AGCM** o **Autorità**) avviata un anno prima, il 21.3.2023, nei confronti della piattaforma TikTok (sul punto, v. in questa Rubrica, notizia n. 13 del numero 1/2023 [2023/1(13)GD]). Segnatamente, l'AGCM ha irrogato, con provvedimento adottato all'adunanza del 5.3.2024, una sanzione amministrativa pecuniaria nella misura del massimo edittale, pari a dieci milioni di euro, in solido alle tre società del gruppo Bytedance Ltd., ovvero l'irlandese TikTok Technology Limited, la britannica TikTok Information Technologies UK Limited e l'italiana TikTok Italy S.r.l.

ISSN 2239-8570

L'attività istruttoria ha consentito, infatti, di accertare, tra le altre, la responsabilità di TikTok nella diffusione di contenuti suscettibili di ledere l'integrità psico-fisica degli utenti, specialmente se minori e vulnerabili. Nella fattispecie si è trattato della diffusione di video sulla cd. *challenge* denominata "cicatrice francese", consistente nell'infliggersi lesioni al volto e farne oggetto di vanto sulla piattaforma, inducendo così altri utenti, per lo più coetanei, a sfidarsi attraverso atti di emulazione sempre più violenti nei confronti di se stessi e del proprio corpo. Dalle evidenze acquisite, è emerso come simili pratiche siano state diffuse e amplificate grazie ad un vero e proprio processo automatizzato di raccomandazione di contenuti rivolto a specifici utenti, minori e vulnerabili, basato sulla profilazione algoritmica dei dati di questi ultimi. Sebbene TikTok abbia rappresentato tale processo di personalizzazione come un fattore positivo che contribuisce alla scoperta del mondo (testualmente, "che ispira la creatività e porta gioia"), per l'Autorità la questione si pone in termini ben più complessi quando, al contrario, l'esperienza assume contorni negativi e dannosi per la salute psico-fisica di soggetti vulnerabili, al punto tale da suscitare allarme tra gli specialisti in campo medico e, in particolare, neuropsichiatrico, le cui osservazioni sono state acquisite in fase istruttoria. In esse è ben evidenziato, infatti, come comportamenti autolesionistici, quali quelli in argomento, sono comunque in grado di rappresentare un pericolo per soggetti vulnerabili, posto che il comportamento autolesionistico anche lieve costituisce il primo fattore di rischio di condotte ulteriori, di tipo suicidario. Le stesse considerazioni sono emerse in un rapporto del 2023 del *U.S. Surgeon General*, il principale portavoce del governo federale in materia di salute (su cui v. in questa Rubrica la notizia n. 10 del numero 2/2023 [2023/2(10)IG]. Difatti, tali comportamenti vanno letti alla luce dei più recenti studi neurologici, secondo i quali la dipendenza dai dispositivi elettronici è analoga a quella che deriva dalle sostanze stupefacenti, con l'interessamento delle stesse aree del cervello che si attivano in caso di astinenza. Da ciò l'esigenza di effettuare un controllo ancor più stringente su questo tipo di contenuti, alla luce dei meccanismi cognitivi di minori e adolescenti, che hanno una capacità limitata di valutare le conseguenze delle proprie azioni. Nel caso in esame, i video relativi alla cicatrice francese sono stati sottoposti da TikTok, in un primo momento, al vaglio del processo di *revisione automatizzata* e, solo a seguito della rilevanza mediatica assunta dal fenomeno, sono stati sottoposti altresì al vaglio della – successiva e solo eventuale – *revisione manuale.* Tuttavia, anche ad esito di tale analisi, è stato ritenuto da TikTok che i contenuti non dovessero essere eliminati dalla piattaforma, in quanto riprodurrebbero un comportamento indotto dal mero desiderio di "apparire interessanti". Sicché, la piattaforma si è limitata a porre in essere una serie di misure a titolo precauzionale, come l'inserimento di un "*warning label*" nella parte inferiore dello schermo con l'avviso "la partecipazione a questa attività potrebbe causare pericoli a te o ad altri", ma nulla che impedisse la massimizzazione della presenza sulla piattaforma, generata dall'estesa diffusione dei contenuti, che rappresenta il principale canale di introito in termini di profitti. Il maggior tempo speso dal singolo utente sulla piattaforma implica, infatti, un aumento

ISSN 2239-8570

dei ricavi di TikTok, in quanto gli utili derivanti dalla raccolta pubblicitaria dipendono in modo cruciale dalle visualizzazioni degli utenti e dalle loro interazioni. L'interesse economico consiste proprio nella monetizzazione di questo effetto di *addiction* e, a tal proposito, l'Autorità richiama significativamente la recente Risoluzione del Parlamento europeo del 12 dicembre 2023 sulla progettazione di servizi online che crea dipendenza e sulla tutela dei consumatori nel mercato unico dell'UE, ove vengono presi in considerazione molti servizi digitali che progettano i propri sistemi per sfruttare la vulnerabilità degli utenti al fine di catturare la loro attenzione e aumentare la quantità di tempo che trascorrono sulle piattaforme. Per l'Autorità, dunque, quanto descritto integra una pratica commerciale scorretta che è causa di un indebito condizionamento dei consumatori, in particolare minori e vulnerabili, in relazione al tempo e modo di fruizione del servizio offerto da TikTok, limitandone la capacità di prendere una decisione consapevole e alterando la decisione di consumo in violazione dell'articolo 25, comma 1, lettera c) del Codice del Consumo. Inoltre, l'omessa adozione di misure e procedure adeguate, pur nella disponibilità di TikTok, volte a prevenire e rimuovere la diffusione di contenuti potenzialmente pericolosi, in linea con quanto solo astrattamente enunciato nelle proprie Linee Guida, viola l'articolo 20 commi 2 e 3, del Codice del consumo. Infine, le descritte condotte integrano, altresì, una violazione dell'articolo 21, comma 4, del Codice del consumo, che prevede una tutela rafforzata per condotte in grado di ledere la salute psico-fisica di alcune categorie di utenti e, in particolare, di minacciare anche indirettamente la sicurezza di bambini e adolescenti.

LUCIO CASALINI

Provvedimento 14.03.2024

2024/1(15)GD

15. Avviata indagine dell'AGCM contro Booking.com per presunto abuso di posizione dominante

Il 12.3.2024, l'Autorità Garante della Concorrenza e del Mercato (**AGCM** o l'**Autorità**) ha avviato un'istruttoria nei confronti di Booking.com per accertare un possibile abuso di posizione dominante nel mercato dei servizi online di intermediazione e prenotazione alberghiera offerti dalle Online Travel Agencies (**OTA**) alle strutture ricettive alberghiere e paralberghiere (le **Strutture**). Il procedimento è stato avviato su segnalazione di Federalberghi e di Associazione Italiana Confindustria Alberghi.

Secondo l'Autorità, Booking.com – che ricopre una posizione "largamente dominante" nel mercato, sia nazionale che europeo, dei servizi online di intermediazione e prenotazione alberghiera offerti dalle OTA – potrebbe aver posto in essere pratiche limitative dell'autonomia delle

ISSN 2239-8570

Strutture nella definizione dei prezzi online ai clienti finali, con effetti assimilabili a quelli derivanti dall'applicazione di clausole di parità, idonee a rendere irrinunciabile per le Strutture il ricorso alla piattaforma Booking.com, e, in ultima analisi, ad escludere dal mercato, o comunque a marginalizzare, le altre OTA.

In particolare, l'AGCM si è focalizzata su due aspetti:

1) il c.d. Programma Partner Preferiti (**PPP**), nonché la sua declinazione "plus" (**PPP Plus**) e

2) l'applicazione del c.d. Sconto Sponsorizzato, o Booking Sponsored Benefit.

Il PPP è un servizio facoltativo offerto da Booking.com alle Strutture per migliorare la visibilità (ranking) sulla piattaforma e aumentare le possibilità di guadagno, in cambio di un aumento della commissione base sulle prenotazioni (dal 15% al 18%). I requisiti per accedere al PPP consistono nel possesso di: *(i)* un determinato punteggio derivante dalla combinazione delle prenotazioni annuali generate dalla struttura in questione e la domanda dei viaggiatori per la medesima struttura; *(ii)* un punteggio di recensione degli utenti di almeno 7/10; e *(iii)* prezzi "competitivi" sulla piattaforma Booking.com rispetto ai "prezzi esterni" (ossia prezzi praticati su altre OTA o sul proprio sito).

Secondo l'Autorità, solamente il terzo criterio relativo ai "prezzi esterni" avrebbe un peso significativo per determinare l'accesso e la permanenza nel PPP. In linea di principio, le Strutture possono scegliere volontariamente di uscire dal PPP in qualunque momento, con effetto immediato e a propria discrezione. Tuttavia, qualora una struttura volesse successivamente rientrarvi, Booking.com si riserva fino a sei mesi di tempo per valutare il rispetto i requisiti di accesso. Ne consegue che la struttura non è pienamente libera di uscire e rientrare nel PPP, scegliendo l'arco temporale di adesione in modo strategico, ad esempio, a seconda dell'afflusso medio di turisti in una determinata stagione.

Inoltre, per le migliori Strutture facenti parte del PPP è prevista la possibilità di accedere al PPP Plus

che garantisce benefici ulteriori in termini di visibilità ma prevede il pagamento di una commissione maggiorata. Questo meccanismo potrebbe indurre le Strutture, soprattutto quelle site in destinazioni con alto afflusso di turisti dove le commissioni sono di norma già al 18% (ad es. Roma e Firenze), ad aderire al PPP Plus aumentando la percentuale di commissioni pagate a Booking.com fino al 23% per apparire prima dei competitor.

Lo Sconto Sponsorizzato consiste, invece, in una riduzione del prezzo finanziato interamente da Booking.com, che rinuncia a una parte della commissione per ridurre il prezzo al pubblico offerto sulla piattaforma. In particolare, quando, all'esito di un monitoraggio capillare e sofisticato, Booking.com riscontra che una struttura offre prezzi migliori su altri siti online, si riserva la possibilità di applicare, senza il consenso delle strutture interessate, il Booking Sponsored Benefit per allineare l'offerta presente sulla propria piattaforma (Booking.com) alla migliore offerta tra quelle disponibili online.

ISSN 2239-8570

In sintesi, l'Autorità ha ritenuto che la strategia posta in essere da Booking.com potrebbe sostanziarsi, da un lato, in un vincolo *ex-ante* per le Strutture – attraverso l'adesione al PPP – a offrire su Booking.com prezzi non superiori a quelli offerti "esternamente" per ottenere migliore visibilità sulla piattaforma; e dall'altro, in un intervento *ex-post*, con l'applicazione unilaterale dello Sconto Sponsorizzato qualora Booking.com rilevi una "scarsa competitività" di una struttura sulla sua piattaforma.

Secondo l'Autorità, in questo modo Booking.com sarebbe in grado di limitare l'autonomia delle Strutture nella definizione dei prezzi ai clienti finali, riproducendo – anche attraverso l'applicazione di alte commissioni che le Strutture sono costrette a pagare per poi ribaltarne il peso sui consumatori - effetti assimilabili a quelli derivanti dall'applicazione di clausole di parità. Com'è noto, tramite le clausole di parità (anche *Most Favored Nation clauses*) – espressamente vietate in Italia a partire dalla Legge Annuale per il Mercato e la Concorrenza n. 124/2017 – le Strutture si impegnano verso le piattaforme di prenotazione a cui sono affiliate a non offrire, sui propri canali diretti o su altre piattaforme, prezzi o altre condizioni per il pernottamento più vantaggiose o favorevoli per il consumatore rispetto a quanto offerto sulle piattaforme affiliate.

La strategia abusiva posta in essere da Booking.com, secondo l'Autorità, sarebbe idonea a escludere, o comunque a marginalizzare, dal mercato le altre OTA, in quanto Booking.com in questo modo sfrutta abusivamente il proprio potere di mercato nei confronti delle Strutture, per le quali rappresenterebbe un canale di intermediazione irrinunciabile. Tale strategia sarebbe, inoltre, in grado di disincentivare ulteriormente, se non dissuadere del tutto, nuove OTA dall'accedere al mercato, non essendo queste ultime in grado di contrastare l'operatore in posizione dominante con gli ordinari strumenti di mercato (ad esempio, offrendo alle Strutture commissioni più basse in cambio di prezzi delle camere più convenienti sui propri siti).

In conclusione, secondo l'Autorità, le condotte di Booking.com appaiono idonee a produrre un aumento generalizzato dei prezzi su tutti i canali di vendita online nel medio-lungo termine. Le Strutture saranno infatti incentivate, secondo l'Autorità, ad aumentare il prezzo per far fronte alle maggiori commissioni richieste da Booking.com e, nel contempo, lo Sconto Sponsorizzato non garantirebbe un effettivo beneficio ai consumatori, che comunque pagherebbero in ultima istanza un prezzo maggiore e godrebbero di minore scelta nei servizi di intermediazione e prenotazione online.

L'avvio dell'istruttoria in questione dimostra come l'Autorità sia attenta, tra le altre cose, nel valutare condotte ritenute potenzialmente idonee a produrre effetti assimilabili a quelli derivanti da clausole di parità. Non rimane che attendere l'esito dell'istruttoria per scoprire se l'Autorità confermerà o meno le ipotesi avanzate.

GIORGIA DIOTALLEVI

Provvedimento 31126 del 12.03.2024

ISSN 2239-8570

72024/1(16)RM

16. Il Garante privacy francese irroga una sanzione da 32 milioni di euro ad Amazon per monitoraggio invasivo delle prestazioni lavorative

La Commission Nationale de l'Informatique et des Libertés, l'autorità francese di controllo per la protezione dei dati personali (di seguito **CNIL**), ha irrogato ad Amazon France Logistique (di seguito anche la **Società**) una sanzione pecuniaria pari a euro 32 milioni ai sensi del regolamento (EU) 2016/679 (**GDPR**) per violazione della privacy dei dipendenti. In particolare, secondo l'autorità d'oltralpe, il datore di lavoro avrebbe posto in essere un eccesso di monitoraggio sulle attività lavorative rese dai dipendenti, con ciò incorrendo in molteplici violazioni del GDPR.

La multa è di importo particolarmente significativo e ammonta al 3% del fatturato che la società destinataria del provvedimento – che si occupa di gestire i magazzini di Amazon ubicati in territorio francese – ha fatto registrare nel 2021.

Il provvedimento sanzionatorio è stato irrogato su impulso di una serie di reclami presentati dai lavoratori e all'esito degli accessi ispettivi che ne sono seguiti.

La CNIL ha ritenuto che Amazon France Logistique abbia violato diversi principi del GDPR sotto diversi profili.

In primo luogo, la CNIL ha analizzato il **monitoraggio dell'attività dei dipendenti svolto dalla Società tramite lo scanner utilizzato dai lavoratori nell'ambito della gestione delle scorte di magazzino e degli ordini**. Secondo l'autorità francese, la Società utilizza indicatori sull'attività e sulle prestazioni dei dipendenti, raccolti tramite scanner, per gestire in tempo reale le scorte e gli ordini nei suoi magazzini. Ebbene, in tale contesto, il datore di lavoro è incorso nella **violazione del principio di minimizzazione dei dati** (art. 5.1.c del GDPR). La CNIL ha ricostruito il processo di gestione delle scorte e degli ordini evidenziando che lo stesso si articola in diversi compiti (ricezione degli articoli, immagazzinamento delle scorte, preparazione e spedizione degli ordini) e comprende anche la formazione di ciascun dipendente nello svolgimento di questi compiti, se necessario (*coaching*), o nella riassegnazione ad altri compiti, se necessario. La violazione del principio di minimizzazione risiederebbe nel fatto che, secondo la CNIL, l'obiettivo di fornire assistenza a un dipendente o riassegnarlo in tempo reale ad altri compiti non richiede né legittima l'accesso ai minimi dettagli relativi agli indicatori di qualità e produttività del dipendente, raccolti con gli scanner nell'ultimo mese. La CNIL sottolinea, altresì, che i supervisori possono già utilizzare i dati in tempo reale per individuare eventuali difficoltà di un dipendente che potrebbero richiedere un intervento di *coaching*, o per identificare i dipendenti da riassegnare a un compito in caso di picco di attività. Pertanto, l'autorità francese ritiene che, oltre ai dati in tempo reale, sarebbe sufficiente una selezione di dati aggregati, ad esempio su base settimanale.

ISSN 2239-8570

La Commissione ha, poi, individuato **tre indicatori illeciti elaborati dall'azienda, in violazione del principio di garanzia di un trattamento lecito** (art. 6 GDPR). Si tratta, segnatamente, dei seguenti indicatori ritenuti illegali:

1. l'indicatore "*Stow Machine Gun*", che segnala un errore quando un dipendente scansiona un articolo "troppo velocemente" (cioè in meno di 1,25 secondi dopo aver scansionato un articolo precedente);
2. l'indicatore di "tempo di inattività", che segnala i periodi di inattività dello scanner di dieci minuti o più;
3. l'indicatore "tempo di latenza inferiore a dieci minuti", che segnala periodi di inattività dello scanner compresi tra uno e dieci minuti.

La CNIL parte dal presupposto che non sia possibile mettere in discussione la necessità di un monitoraggio preciso delle movimentazioni effettuate e della situazione di ciascun dipendente, al fine di garantire la qualità del servizio e la sicurezza nei propri magazzini, ma rileva, tuttavia, che il trattamento di dati personali determinato dai tre predetti indicatori non può basarsi su un interesse legittimo, in quanto comporta un'eccessiva sorveglianza informatica sul dipendente rispetto all'obiettivo perseguito dall'azienda.

La CNIL osserva che, in primo luogo, l'elaborazione dell'indicatore *Stow Machine Gun* consente di monitorare costantemente qualsiasi modifica apportata da un dipendente al secondo e di associarvi un errore in caso di modifica troppo rapida.

In secondo luogo, l'uso degli indicatori "tempi di inattività" e "tempi di latenza inferiori a dieci minuti" consente di monitorare costantemente ogni volta che lo scanner di un dipendente viene interrotto su un'attività diretta, anche per un tempo molto breve (meno di dieci minuti o appena dieci minuti).

Secondo la CNIL, la Società ha già accesso a numerosi indicatori in tempo reale, sia individuali che aggregati, per raggiungere gli obiettivi di qualità e sicurezza nei propri magazzini e l'elaborazione di tali indicatori implica che il dipendente debba potenzialmente giustificare in qualsiasi momento, l'interruzione del suo scanner, anche se per brevissimi momenti.

Tutto ciò rende il trattamento in esame eccessivamente intrusivo.

La CNIL ha rilevato delle carenze anche nella **pianificazione del lavoro e nella valutazione dei dipendenti**, attività che viene realizzata dalla Società tramite i dati e gli indicatori sulle attività e le prestazioni dei dipendenti raccolti dai predetti scanner. Ebbene, anche in tale ambito è stata riscontrata la **violazione del principio di minimizzazione dei dati** (art. 5(1)(c) GDPR) in quanto la pianificazione del lavoro nei magazzini, la valutazione e la formazione dei dipendenti non richiedono l'accesso ai minimi dettagli dei dati e degli indicatori statistici forniti dallo scanner utilizzato dal dipendente e riportati nell'ultimo mese essendo, a tal fine, sufficienti le statistiche per dipendente, aggregate per esempio nell'arco della settimana. Inoltre, secondo la CNIL, l'obiettivo di monitorare l'effettivo lavoro del dipendente, a fini di valutazione o formazione, non

ISSN 2239-8570

giustificano la registrazione di un tempo di inattività superiore a dieci minuti.

La Commissione ha riscontrato altresì il **mancato rispetto degli obblighi di informazione e trasparenza** (artt. 12 e 13 GDPR). Tale mancanza sarebbe stata commessa fino all'aprile 2020 nei confronti del personale temporaneo che lavorava per l'azienda, per il quale la Società non si era assicurata la corretta ricezione dell'informativa sulla privacy prima che i loro dati personali venissero raccolti con gli scanner.

L'ultimo gruppo di violazioni riscontrate riguarda il **trattamento dei dati personali raccolti tramite sistemi di videosorveglianza.** In questo ambito la Commissione ha rilevato il **mancato rispetto degli obblighi di informazione e trasparenza** (artt. 12 e 13 GDPR) e la **violazione dell'obbligo di sicurezza** (articolo 32 del GDPR).

Secondo la CNIL, infatti, i dipendenti e i visitatori esterni non sono stati adeguatamente informati sui sistemi di videosorveglianza, poiché alcune informazioni richieste dall'articolo 13 del GDPR non sono state fornite né nelle bacheche né su altri supporti o documenti.

Inoltre, l'accesso al software di videosorveglianza non era sufficientemente sicuro, in quanto la password di accesso non era abbastanza forte e l'account di accesso era condiviso tra diversi utenti. Tali difetti di sicurezza rendono più difficile tracciare l'accesso alle immagini video e identificare ogni persona che ha effettuato azioni sul software.

RICCARDO MARAGA

Comunicato stampa 23.01.2024

2024/1(17)CAT

17. I Garanti privacy spagnolo e italiano si esprimono in senso contrario al progetto Worldcoin (la criptovaluta di Sam Altman) per il dispositivo "Orb" di scansione dell'iride

L'Agenzia spagnola per la protezione dei dati (**AEPD**) e l'Autorità italiana garante per la protezione dei dati personali (**Garante privacy**) hanno, separatamente l'una dall'altra, espresso valutazioni negative sul progetto Worldcoin Token (**WLD**) relativamente alla conformità al regolamento (UE) 2016/679 (**GDPR**) delle funzioni e delle attività dispiegate dal dispositivo fisico 'Orb' che produce scansioni dell'iride umana a fini identificativi.

WLD è una criptovaluta fondata nel 2019 da Sam Altman, CEO di OpenAI, insieme a Max Novendstern e Alex Blania. Il lancio e la gestione di questo progetto sono stati affidati alla Worldcoin Foundation, una fondazione delle Isole Cayman, con il supporto di Tools for Humanity, laboratorio di ricerca e tech-company con sede principale a San Francisco, California, e a Berlino (Germania). L'operatività di WLD è gestita attraverso un'applicazione mobile (World App) che funge da nucleo centrale del

ISSN 2239-8570

progetto per ogni singolo utente. Attraverso questa app, infatti, gli utenti possono sia disporre del proprio portafoglio criptovalutario che gestire la propria certificazione di identità. Ciò è possibile in quanto WLD non è limitato alla sua natura di token criptografico conforme agli standard di Ethereum, ma mira a creare una rete di individui identificati in modo univoco, confermando la loro autenticità come esseri umani. Il concetto chiave è rappresentato da WorldID, un'identità ottenuta tramite la scansione dell'iride e del volto presso i vari punti di registrazione sparsi nel mondo per mezzo di un dispositivo fisico chiamato "Orb". A seguito di tale procedura, la persona riceve una prova univoca della sua identità personale fondata su dati biometrici. La procedura è stata ideata per evitare che una stessa persona fisica possa registrarsi più volte nella piattaforma con diverse identità. Worldcoin Foundation e World Assets Ltd., una società a responsabilità limitata delle Isole Vergine Britanniche, responsabile anch'essa del protocollo World ID, dichiarano nei loro canali di comunicazione ufficiali che i dati biometrici raccolti vengono trattati in modo sicuro e successivamente cancellati o crittografati.

A seguito del lancio del prodotto al pubblico, il 6.3.2024 l'AEPD ha ordinato una misura cautelare nei confronti di Tools for Humanity, affinché cessasse la raccolta e il trattamento dei dati personali che sta effettuando in Spagna nell'ambito del progetto Worldcoin poiché la sua prosecuzione comporta, secondo l'AEPD, rischi elevati per i diritti e le libertà delle persone fisiche. Tale azione dell'AEPD ha come base giuridica la procedura dell'art. 66(1) GDPR che stabilisce che, in circostanze eccezionali, quando un'autorità di controllo interessata ritiene urgente intervenire per proteggere i diritti e le libertà delle persone fisiche, può adottare misure provvisorie con effetti giuridici nel suo territorio e con un periodo di validità non superiore ai tre mesi.

L'AEPD ha inoltre affermato di aver già ricevuto diversi reclami che lamentano, tra gli altri aspetti, l'insufficiente informazione, la raccolta di dati di minori e l'impossibilità di revocare il consenso dopo aver aderito al progetto, per cui ritiene che l'adozione di misure urgenti di divieto temporaneo di attività sia necessaria.

Sul sito web gestito dalla predetta fondazione delle Isole Cayman e dalla predetta società a responsabilità limitata delle Isole Vergini Britanniche, si trova un comunicato di commento alla vicenda e l'affermazione per cui "*Worldcoin opera legalmente in tutti i luoghi in cui è stata resa disponibile e sotto la stretta supervisione dell'autorità bavarese per la protezione dei dati (BayLDA), l'ente normativo responsabile della supervisione della conformità al GDPR in tutta l'UE (Lead Supervisory Authority). In conformità con i regolamenti dell'UE relativi all'applicazione del GDPR, i collaboratori di Worldcoin hanno regolarmente risposto alle richieste della BayLDA per mesi, operando legalmente in Spagna e in alcuni altri Paesi europei. Questo impegno continua tuttora*". Inoltre, Tools for Humanity ha dichiarato di rispettare tutte le leggi e i regolamenti che disciplinano la raccolta e la trasmissione dei dati biometrici e che l'AEPD non ha giurisdizione per fermare le operazioni della società nel paese, in quanto il GDPR stabilisce che l'Autorità competente è quella del paese di

ISSN 2239-8570

stabilimento della società, ossia la bavarese "BayLDA". Quest'ultima ha peraltro confermato di aver già avviato un'attività di audit nell'ambito dello sviluppo del prodotto nell'estate del 2023, in vista del lancio della criptovaluta, i cui risultati saranno a breve resi pubblici.

In Italia, il 2 aprile 2024, il Garante privacy, attraverso un comunicato stampa, ha a sua volta dichiarato che se il progetto Worldcoin approdasse in Italia, con ogni probabilità violerebbe il GDPR con tutte le conseguenze di carattere sanzionatorio previste dalla normativa, poiché:

1. il trattamento dei dati biometrici basato sul consenso degli aderenti al progetto, rilasciato sulla base di una informativa insufficiente, non può essere considerato una base giuridica valida secondo i requisiti richiesti dal Regolamento europeo;
2. il consenso non risulta prestato liberamente ma condizionato dalla promessa di ricevere WLD token gratuiti;
3. si rileva l'assenza di filtri per impedire l'accesso agli Orb e alla World App ai minori di 18 anni.

CARMINE ANDREA TROVATO

Comunicato stampa Garante privacy spagnolo
Comunicato stampa Garante privacy italiano

2024/1(18)SM

18. "Protecting Americans": le due leggi americane contenute nel National Security Act 2024 contro le applicazioni controllate da Cina, Russia, Iran e Corea del Nord (la legge contro TikTok) e contro qualunque trasferimento di dati sensibili in questi paesi.

All'interno del più ampio National Security Act 2024, H.R.815 — 118th Congress 2023-2024 (il **National Security Act 2024**), il Congresso degli Stati Uniti d'America ha approvato due importanti leggi intese a proteggere i dati personali dei residenti negli Stati Uniti d'America (**USA**) impedendo che possano essere trasferiti in quattro paesi stranieri qualificati come paesi avversari ("*adversary countries*"): Cina, Russia, Iran e Corea del Nord.

Il ***Protecting Americans From Foreign Adversary Controlled Applications Act.***

La prima legge - firmata dal presidente Biden il 4.4.2024 e contenuta nella Sezione H del National Security Act 2024 - è intitolata *Protecting Americans From Foreign Adversary Controlled Applications Act*. Delle due, è quella che ha attirato fin qui maggiore attenzione, in quanto nei media si è parlato di legge disegnata *ad hoc* contro TikTok. Tale legge (di seguito la **Legge contro le applicazioni controllate da avversari stranieri**, o la **Legge**), pur essendo stata indubbiamente promulgata per costringere la società cinese Byte Dance Ltd. (**ByteDance**) - che controlla la società americana TikTok Inc. (dal nome dell'omonima piattaforma online, da essa

ISSN 2239-8570

gestita: **TikTok**) - a dismettere le sue attività negli USA, ha nondimeno una portata generale.

La Legge definisce "*foreign adversary controlled application*" qualunque sito web, o applicazione desktop o mobile o di tecnologia immersiva o aumentata che sia direttamente o indirettamente operata da ByteDance, TikTok o da qualunque altra persona o ente controllato direttamente o indirettamente da un "*foreign adversary"* ("avversario straniero"). Il "*foreign adversary"* è a sua volta definito come qualunque persona o ente domiciliato, residente, avente la propria sede principale o costituito secondo le leggi di un "*foreign adversary country*" ("paese avversario straniero"). Infine, per "*foreign adversary country*" si intende uno dei paesi menzionati in un'altra legge, precisamente, nella sezione 4872(d)(2) del titolo 10 dello United States Code, ossia:

(A) la Repubblica Popolare della Corea del Nord;
(B) la Repubblica Popolare Cinese;
(C) la Federazione Russa; e
(D) la Repubblica Islamica dell'Iran.

La Legge proibisce qualunque attività di distribuzione, mantenimento, aggiornamento e fornitura di servizi internet di memorizzazione (*internet hosting services*) per qualunque applicazione controllata da avversari stranieri. Il divieto cessa di operare nel caso in cui il Presidente degli USA abbia verificato e dichiarato che una applicazione controllata da avversari stranieri sia stata fatto oggetto di una dismissione qualificata (*qualified divestiture*) tale da escludere una situazione di controllo da parte di avversari stranieri nel senso inteso dalla Legge.

La Legge attribuisce un termine di 270 giorni dalla sua emanazione per adeguarsi al divieto (ossia fino al 19 gennaio 2025). È previsto che il Presidente degli USA possa estendere la scadenza del divieto di altri 90 giorni in costanza di evidenti progressi compiuti nella direzione della dismissione qualificata, così dando a ByteDance, in totale, un anno di tempo per dismettere le attività di TikTok negli USA.

Il legislatore statunitense ha a lungo esaminato la questione, valutando il rischio che i dati personali degli americani, cui ByteDance ha di fatto accesso, possano essere acquisiti dal governo della Repubblica Popolare Cinese.

La decisione, infatti, è conseguenza di un'avvertita minaccia alla sicurezza nazionale poiché si teme che la popolarissima app, usata da 170 milioni di utenti negli USA, potrebbe essere utilizzata dal Partito Comunista cinese per sorvegliarli, attraverso l'accesso ai dati personali della popolazione degli Stati Uniti d'America.

La questione appare complessa perché, se, da un lato, vi è la preoccupazione per la sicurezza nazionale e la protezione dei dati personali, dall'altro vi è il timore di perdere un canale di libera espressione e un'importante fonte di reddito per milioni di persone.

Tuttavia, e in definitiva, alla base della legge approvata da Biden prevale il timore del governo statunitense che i dati personali dei cittadini americani possano essere usati per alimentare fake news, disinformazione e

ISSN 2239-8570

manipolare l'opinione pubblica americana a favore di interessi politici cinesi.

Inoltre, come notato, la Legge non si applica solo a TikTok, ma ha una portata generale, e solleva pertanto questioni più ampie sulla libertà di espressione e sul ruolo che i governi hanno o dovrebbe avere nel regolare il cyberspazio.

Il *Protecting Americans' Data from Foreign Adversaries Act of 2024*

La seconda legge, non meno importante della prima, è contenuta nella Sezione I del National Security Act 2024. Essa è intitolata *Protecting Americans' Data from Foreign Adversaries Act of 2024* (**Legge sulla protezione dei dati degli americani da avversari stranieri**). Questa seconda legge vieta ai "broker di dati" di rendere disponibili in qualunque forma "dati sensibili" di persone che risiedono negli USA ai governi dei suddetti quattro paesi avversari, o a qualunque entità controllata da essi (i.e. qualunque persona o ente domiciliato, residente, avente la propria sede principale o costituito secondo le leggi della Cina, Russia, Iran o Corea del Nord). Ai fini di questa legge, i "dati sensibili" comprendono identificatori emessi dal governo USA (es. numeri del sistema della *Social Security* statunitense), numeri di conti correnti, informazioni biometriche, informazioni genetiche, informazioni puntuali di geolocalizzazione e comunicazioni private (quali testi o emails). Sempre ai sensi di questa legge, per "broker di dati" si intende qualunque entità che vende o comunque fornisce dati di persone che essa non raccoglie direttamente dalle persone. Non si intende per broker di dati colui che agisca su richiesta o seguendo le istruzioni della persona cui si riferiscono i dati sensibili, né gli enti che mettono a disposizione della generalità del pubblico notizie o informazioni. La competenza per l'applicazione della Legge sulla protezione dei dati degli americani è attribuita alla *Federal Trade Commission* del Governo USA.

SERENA MIRABELLO

National Security Act 2024

2024/1(19)VH

19. Il Dipartimento di Giustizia USA contro Apple per pratiche anticoncorrenziali legate agli smartphone

Il 21.3.2024 il Dipartimento di Giustizia degli Stati Uniti d'America (U.S. Department of Justice, Antitrust Division, di seguito il **Dipartimento di Giustizia**), unitamente a 16 procuratori statali e distrettuali, ha promosso un'azione civile contro Apple Inc. (**Apple**) per avere monopolizzato, o tentato di monopolizzare, i mercati connessi all'utilizzo e sviluppo degli smartphone, violando così la Sezione II del Sherman Act, la fondamentale legge federale statunitense in materia di antitrust.

Nel ricorso, depositato presso la Corte Distrettuale degli Stati Uniti per il Distretto del New Jersey (il **Ricorso**), si sostiene che Apple detenga

ISSN 2239-8570

illegalmente un monopolio sugli smartphone attraverso una imposizione selettiva di clausole contrattuali restrittive e negando agli sviluppatori informatici cruciali punti di accesso al mercato. Si afferma, sempre nel Ricorso, che Apple penalizzi le applicazioni, i prodotti e i servizi che potrebbero rendere gli utenti meno dipendenti dall'iPhone e che promuovono l'interoperabilità fra i diversi sistemi operativi, così riducendo i costi per consumatori e sviluppatori. In questo modo, Apple sfrutterebbe la propria posizione monopolistica al fine di ricavare maggiori profitti da consumatori, sviluppatori, creatori di contenuti digitali, artisti, editori, piccole imprese e commercianti, tra gli altri. Tramite l'esercizio di questa azione, il Dipartimento di Giustizia e i procuratori generali statali e distrettuali, nel perseguimento dell'interesse pubblico americano, sperano di ottenere un provvedimento che ripristini la concorrenza in questi mercati vitali.

Una volta definita la posizione di monopolio nei mercati connessi allo smartphone, in cui Apple sfrutta il proprio controllo sull'iPhone per assumere intenzionali, svariati e sostenuti comportamenti illegittimi al fine di ottenere maggiori profitti, nel ricorso si delineano quali sarebbero, pur nella loro costante evoluzione, le modalità specifiche in cui si articolano le condotte censurate:

- Il blocco di super app innovative: Apple avrebbe pregiudicato lo sviluppo di applicazioni con ampie funzionalità, le quali renderebbero più facile per gli utenti il passaggio fra le piattaforme operative concorrenti dei vari smartphone.
- La soppressione di servizi portabili di cloud streaming: Apple avrebbe frenato lo sviluppo di app e servizi di cloud streaming che consentirebbero agli utenti di fruire di videogiochi di alta qualità e di altre applicazioni basate su sistemi cloud che permettono di non ricorrere a costose tecnologie hardware.
- L'esclusione qualitativa di applicazioni di messagistica inter-operative: la Apple avrebbe reso la qualità della messaggistica fra diversi sistemi operativi peggiore, meno innovativa e meno sicura per gli utenti, in modo da indurre i propri clienti a continuare a comprare iPhone.
- Diminuendo le funzionalità degli smartwatch non Apple: Apple avrebbe limitato le funzionalità degli smartwatch di terzi con la conseguenza che gli utenti che acquistino l'Apple Watch debbano sostenere costi notevoli se non continuano a comprare iPhone.
- Limitando i portafogli digitali (wallet) di terzi: Apple avrebbe impedito ad applicazioni di terze parti l'utilizzazione della funzionalità tap-to-pay (ossia la tecnologia che permette di pagare direttamente con il dispositivo iPhone), ostacolando così la creazione di portafogli digitali di terzi inter-operativi.

Nel ricorso si chiarisce come le condotte di Apple inciderebbero ben oltre questi esempi riverberandosi negativamente altresì sui servizi browser web, videocomunicazioni, abbonamenti alle notizie, intrattenimento, servizi automobilistici, pubblicità, servizi di localizzazione e altro ancora. Infine, nel chiedere l'adozione di provvedimenti opportuni, si sottolinea come Apple abbia ogni incentivo a estendere e consolidare queste pratiche per

ISSN 2239-8570

acquisire e mantenere il potere su dispositivi e tecnologie di ultima e prossima generazione.

Nel comunicato stampa pubblicato sul sito web del Dipartimento di Giustizia a proposito del Ricorso, viene specificato che nell'anno fiscale 2023, Apple ha generato ricavi netti per 383 miliardi di dollari e un utile netto di 97 miliardi di dollari, sottolineandosi che l'utile netto di Apple supera quello di qualsiasi altra azienda della Fortune 500 e il prodotto interno lordo di più di 100 paesi.

VICTOR HARTL

Comunicato stampa del Dipartimento di Giustizia
Ricorso

2024/1(20)SB

20. La sentenza del British Columbia Civil Resolution Tribunal del 14.2.2024 nel caso Moffatt vs Air Canada per informazione errata fornita dal chatbot del sito web della compagnia aerea

Recentemente ha avuto una vasta risonanza la decisione del 14.2.2024, resa dal *Civil Resolution Tribunal* della British Columbia (Canada) per un caso di lesione dell'affidamento derivante dalle inesatte informazioni rese da un chatbot (quindi, sostanzialmente, da un'applicazione di un sistema di intelligenza artificiale) di Air Canada.

A dispetto del nome, il *Civil Resolution Tribunal* (di seguito, anche solo **CRT**) non è un giudice, ma un organo amministrativo pubblico cui viene demandata una funzione di mediazione e conciliazione di controversie bagatellari (c.d. *small claims* e altre tipologie di controversie ritenute, comunque, di natura minore). Nel momento in cui le parti non addivengono ad una composizione della controversia, il CRT emette una decisione che, una volta depositata in copia conforme davanti al Giudice competente, viene munita da quest'ultimo di clausola esecutiva e diviene, pertanto, eseguibile (Part 6 - artt. 57 e ss. del *Civil Resolution Tribunal Act*); la decisione del CRT è anche impugnabile (Part 5.1, art. 56 del *Civil Resolution Tribunal Act*).

La vicenda è la seguente. Nel novembre 2022, il Sig. Jake Moffat, dovendo recarsi a Toronto per assistere al funerale di un congiunto, si collegava al sito della Air Canada per conoscere i costi dei biglietti ed eventuali tariffe agevolate per i voli prenotati per esigenze di lutti in famiglia. Il Sig. Moffat interloquiva con un assistente virtuale (un chatbot, appunto) che informava della possibilità di ottenere un rimborso parziale del costo dei biglietti una volta rientrato a casa dal volo di ritorno. Il Sig. Moffat faceva uno screenshot della conversazione avuta con il chatbot e, sulla base delle informazioni ricevute, acquistava i biglietti di andata e ritorno a tariffa piena, confidando nel loro parziale rimborso una volta a casa. Chiesto il parziale rimborso Air Canada lo negava. Pur essendo vero, infatti, che Air

ISSN 2239-8570

Canada applicava tariffe agevolate per i voli acquistati in occasione di lutti famigliari, i biglietti a tariffa ridotta dovevano essere acquistati fin da subito tramite un'apposita sezione del sito della compagnia che, quindi, non procedeva al rimborso a posteriori. Air Canada, sebbene riconoscesse l'errore compiuto dal chatbot, imputava al Sig. Moffat una scarsa diligenza perché avrebbe mancato di esaminare l'apposita pagina del sito in cui venivano indicate le tariffe agevolate e dal quale avrebbe potuto procedere all'acquisto dei biglietti ad un costo ridotto. In più ancora (e qui è probabilmente il motivo di reale interesse della decisione), la compagnia sosteneva che, comunque, non poteva essere responsabile delle informazioni rese dal proprio chatbot poiché essa si sarebbe dovuta considerare come un soggetto giuridico autonomo che, in quanto tale, sarebbe stata responsabile delle proprie azioni/parole non imputabili ad Air Canada: "*Air Canada suggests the chatbot is a separate legal entity that is responsible for its own actions*" (così, punto 27 della decisione).

Come anche il CRT ha avuto modo di sottolineare questa seconda linea difensiva "*is a remarkable submission*".

Le due tesi difensive di Air Canada sono state entrambe rigettate e la compagnia è stata condannata a risarcire il Sig. Moffat. Nella motivazione, il CRT non adotta principi innovativi, ritenendo Air Canada responsabile sulla base dei principi ordinari in materia di lesione dell'affidamento. Secondo il CRT, infatti, il Sig. Moffat, aveva correttamente fatto affidamento sulle informazioni dategli dall'assistente virtuale e non aveva alcun obbligo o onere di andare a cercare e a consultare l'apposita sezione del sito della compagnia sulle tariffe agevolate per i voli acquistati in occasione di lutti famigliari. Il chatbot era stata implementato nel sito di Air Canada per fornire quelle stesse informazioni che il Sig. Moffat avrebbe potuto trovare consultando le pagine del sito e non si vede per quali ragioni il Sig. Moffat avrebbe dovuto ritenere che le informazioni rese dal chatbot dovessero avere un minor livello di accuratezza o comunque di riferibilità alla compagnia aerea rispetto alle pagine del sito.

Quanto, poi, alla questione della soggettività del chatbot il CRT ha avuto modo di sottolineare come questa seconda linea difensiva rappresentasse *"a remarkable submission*" e dove "*remarkable*" più che nella sua accezione di "notevole" potrebbe essere tradotta con "straordinario". Come rilevato dal CRT, infatti, il chatbot non ha alcuna soggettività giuridica essendo nient'altro che una componente (interattiva) del sito di Air Canada. È la compagnia che è tenuta a fornire informazioni chiare ed esatte circa i voli e le relative tariffe e, pertanto, se tali informazioni sono errate è irrilevante che esse provengano da una componente interattiva del sito (il chatbot) o da una componente statica quali sono le pagine del sito stesso.

Come si vede, la decisione non presenta carattere eccezionale; il caso è stato deciso fondamentalmente facendo scorta dei principi relativi alla lesione dell'affidamento ingenerato dalle informazioni fornite dall'assistente virtuale. Probabilmente, quindi, l'eco suscitata dal provvedimento è da attribuire alla circostanza che, nel caso di specie, si stesse discutendo di un'applicazione di un sistema di intelligenza artificiale (quale è un chatbot; cfr. al riguardo, ad es. https://www.ibm.com/it-it/topics/chatbots) e, come

ISSN 2239-8570

più sopra si accennava, alla tesi difensiva di Air Canada che pretendeva di qualificare il (proprio) chatbot come un soggetto separato ed autonomo rispetto alla stessa Air Canada, peraltro, senza nemmeno spiegare perché il chatbot si sarebbe dovuto intendere come un soggetto autonomo e perché, in tal caso, operando il chatbot per conto di Air Canada non vi sarebbe stata responsabilità sulla base dei principi che regolano i rapporti *principal/agent* (più o meno assimilabili al nostro rapporto mandante/mandatario) o il fatto dell'ausiliario (nostra responsabilità ex art. 1228 c.c.).

STEFANO BARTOLI

2024 BCCRT 149

2024/1(21)VP

21. La dichiarazione 'Artificial Intelligence and Society' firmata durante il G7 Italia 2024

In data 11 e 12 aprile 2024 presso Palazzo Corsini in Roma, l'Accademia dei Lincei ha ospitato la riunione del G7 della Scienza (di seguito **S7**) e delle Scienze Sociali e Umanistiche (**SSH7**), a cui hanno partecipato le Accademie delle più grandi potenze mondiali (di seguito **Le Accademie**) con l'obiettivo di elaborare documenti congiunti su grandi temi di interesse globale da sottoporre ai Capi di Stato e di governo del G7.

Tra questi merita sicuramente attenzione il documento su "Intelligenza artificiale e società" (di seguito il **Documento**) con il quale – le Accademie - hanno espresso le proprie preoccupazioni in materia di Intelligenza Artificiale (**IA**), formulando un elenco di raccomandazioni ai decisori pubblici su vari aspetti.

Nello specifico sono stati affrontati i seguenti temi:

Protezione da Attacchi e Normativa sulla Privacy

Data la natura dei potenti sistemi di IA, i quali, se utilizzati in modo improprio – rappresentano un potenziale rischio per il pubblico - è emersa la necessità di assicurare loro un'adeguata protezione da attacchi di tipo informatico o materiale. Vi è poi l'invito – rivolto alle istituzioni – di dotarsi di un quadro normativo per la protezione dei dati che non sia standard bensì commisurato al livello del rischio. Con riferimento agli utenti si segnala l'esigenza di fornire indicazioni chiare sulla protezione dei dati, in particolare con riferimento a modalità e tempistiche di utilizzo e conservazione.

Standard rigorosi e Monitoraggio post-Distribuzione

L'evoluzione tecnologica renderà i sistemi di IA sempre più performanti. Questo fenomeno, tuttavia, determinerà l'aumento dei rischi connessi al loro utilizzo. A tal ragione si raccomanda l'implementazione di standard rigorosi per la verifica dei requisiti, la convalida ed il collaudo del sistema. Unitamente a queste sarà fondamentale il monitoraggio successivo alla distribuzione svolto da organismi indipendenti. Sul punto – da una

ISSN 2239-8570

prospettiva di supervisione – sarà necessario che gli Stati individuino gli enti deputati a svolgere tale funzione.

Rischi connessi all'interazione tra esseri umani e sistemi di IA

La certezza del corretto funzionamento dei sistemi di AI – i cui contenuti costituiscono oggi una percentuale sempre maggiore del nostro "ecosistema informativo" - deve essere garantita al fine di ridurre i rischi legati ad un'informazione non corretta e fuorviante. Per tale ragione sarà necessario pensare a modelli che siano volti, da un lato, a promuovere l'accuratezza e l'autenticità dei contenuti generati dall'IA e, dall'altro, ad aumentare l'alfabetizzazione delle popolazioni per capire come identificare ed interagire con i contenuti generati dall'IA.

Protezione dei diritti di Proprietà Intellettuale

L'AI generativa – grazie alla sua capacità di creare contenuti di vario genere sfruttando modelli di deep learning addestrati, ci pone – tra i vari - difronte al dovere di proteggere i diritti di proprietà intellettuale nelle ipotesi in cui questi sistemi vengano utilizzati per creare contenuti apparentemente nuovi ma generati da opere esistenti. Il quadro giuridico in materia di diritto d'autore – sottolineano le Accademie – deve tener conto del fenomeno IA ed essere implementato sulla base delle nuove esigenze.

IA e Sostenibilità

Le riflessioni contenute nel dossier tengono inoltre conto del fenomeno della sostenibilità e del mondo in cui questo dialoga con l'intelligenza artificiale. Alle opportunità che l'evoluzione tecnologica porta nel combattere le sfide ambientali e sociali della nostra epoca – sottolineano le Accademie – si accompagnano importanti rischi. Questi riguardano, da un lato, i meccanismi per abbattere le barriere all'ingresso nel mercato dei sistemi di IA su larga scala (i quali richiedono risorse costose) e, dall'altro, i problemi ambientali legati all'aumento del consumo energetico. Serve dunque un cambio di paradigma che – sul punto – metta in discussione le basi dello sviluppo capitalistico nel quale domina la visione individualizzante della società.

Contrasto alle armi

Le armi autonome di distruzione stanno cambiando il panorama e sono oggi al centro di un complesso dibattito nel quale si incontrano preoccupazioni di carattere giuridico ed etico in relazioni alle conseguenze che da queste potrebbero scaturire. A tal fine s'invitano i legislatori a garantire una regolamentazione che sia in linea con il diritto internazionale umanitario e che preveda la supervisione umana allo scopo di limitare gli effetti dei conflitti armati.

Allineamento IA con etica umana

Stante la crescente influenza dei sistemi di IA sui processi decisionali – attraverso una collaborazione intersettoriale – occorre integrare agli aspetti tecnici anche quelli socioculturali che tengano conto delle diversità e che affrontino tutti quei rischi che potrebbero avere un impatto negativo su gruppi sociali vulnerabili. Raggiungere questo obbiettivo significherebbe aumentare il livello di fiducia ed incoraggiare l'utilizzo di sistemi di AI.

Gestione equa dei benefici dell'IA

ISSN 2239-8570

L'utilizzo di sistemi di IA produce benefici. Tuttavia, l'impatto che questi hanno sul mercato del lavoro, non è privo di rischi. Occorre dunque che i Governi incentivino sistemi in grado di rispondere ad esigenze non ancora soddisfatte. Tocca dunque evitare che l'impatto delle nuove tecnologie basate sull'apprendimento automatico (machine learning) possa sostituirci nelle nostre mansioni lavorative e muovere verso un modello ove la transizione tecnologica venga gestita in modo equo e sostenibile.

Cooperazione tra pubblico e privato

Le Accademia sottolineano come - al fine di creare un sistema che possa innovare rapidamente all'interno di un quadro normativo "etico" - sia necessaria la collaborazione tra pubblico e privato. Occorre infatti pensare ad un sistema alimentato dallo scambio di competenze.

Cooperazione tra diverse discipline accademiche

Le grandi sfide volte a mitigare i rischi connessi all'implementazione dei sistemi di IA richiedono un approccio cooperativo tra diverse discipline accademiche. Ne è un esempio il Documento e la maturata consapevolezza che - per affrontare le sfide tecnologiche della nostra epoca - occorre un approccio interdisciplinare.

Education

Le Accademie si auspicano che i cittadini vengano tecnicamente preparati alle sfide dell'IA e che diventino consapevoli delle sue implicazioni sociali ed etiche.

Dal G7 della scienza sono dunque emersi contributi che costituiscono una bussola per orientare i decisori pubblici nel contesto delle sfide del nostro secolo. L'auspicio è che questi possano muoversi nella direzione auspicata dagli studiosi valorizzando il potenziale che forniscono i sistemi di intelligenza artificiale ed eliminando i numerosi rischi che alla sua crescita sono associati.

VINCENZO PITTELLI

Artificial Intelligence and Society
Science for the future

ISSN 2239-8570