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.

16. **I due ricorsi di NOYB del 16.11.2023 contro la Commissione europea (davanti a EDPS) e del 14.12.2023 contro X (davanti alla DPA olandese) per le pratiche di online microtargeting a supporto di una pubblicità commissionata dalla Commissione europea** [2023/4(16)TB]
17. **Adottato il 6.12.2023 il regolamento Consob per la finanza sulle piattaforme DLT** [2023/4(17)IT]
18. **Il provvedimento interpretativo del Garante privacy del 26.10.2023 sul diritto di accesso degli eredi e dei chiamati all'eredità ai nominativi dei beneficiari delle polizze vita accese dal *de cuius*** [2023/4(18)VC]
19. **La sentenza della CGUE del 7.12.2023 nelle cause riunite C-26/22 e C-64/22 (caso SCHUFA sul controllo giurisdizionale sulle decisioni delle DPA e sulla cancellazione di dati personali relativi all'esdebitazione)** [2023/4(19)RMo]
20. **La sentenza della CGUE del 7.12.2023 nella causa C-634/21 (caso SCHUFA sul credit scoring automatizzato)** [2023/4(20)RMo]
21. **La causa pilota per danni avviata da NOYB contro CRIF e AZ Direct davanti al Tribunale civile di Vienna in conseguenza di una accertata violazione del GDPR relativamente al trattamento di dati personali per fini di calcolo del merito di credito** [2023/4(21)ES]
22. **Le sentenze CGUE nei casi C-300/21 e C-340/21 sul danno non patrimoniale causato da violazione del GDPR** [2023/4(22)GR]
23. **La sentenza CGUE nel caso C-683/21 sulla rilevanza dell'elemento soggettivo nella violazione del GDPR ai fini della sanzione amministrativa pecuniaria** [2023/4(23)VR]
24. **La sentenza CGUE nel caso C-307/22 in materia di accesso, copia e trattamento di dati sanitari** [2023/4(24)EMI]
25. **Le sentenze dei Tribunali di Pordenone e Udine sulla medicina di iniziativa contro le sanzioni del Garante privacy** [2023/4(25)EG]
26. **Il provvedimento sanzionatorio di AGCOM contro Google e Twitch per la pubblicizzazione di gioco d'azzardo e l'archiviazione del procedimento a carico di TikTok** [2023/4(26)VP]
27. **Le cause intentate da oltre 40 Stati degli USA contro Meta per pratiche online che creano dipendenza nei giovani** [2023/4(27)IG]
28. **Aggiornamenti di dicembre 2023-gennaio 2024 sul caso *Fortnite* in USA (le azioni di Epic Games vs Google e Apple per condotta anticoncorrenziale)** [2023/4(28)FP]
29. **La remissione alla CGUE da parte del TAR Lazio di questioni interpretative a proposito delle disposizioni della legge italiana sul diritto di autore e del regolamento AGCOM in materia di equo compenso agli editori di giornali online, in conseguenza del ricorso di Meta** [2023/4(29)FS]
30. **Il primo provvedimento in USA nel caso Stable Diffusion sulla richiesta di protezione del copyright contro i sistemi di IA generativa: *fair use* o non *fair use*?** [2023/4(30)DDA]
31. **La causa intentata dal NYT contro Open AI e Microsoft per la IA generativa** [2023/4(31)EB]
32. **La prima sentenza cinese che riconosce a certe condizioni all'utente del software il diritto d'autore sugli ouput ottenuti da un sistema di IA generativa (caso Li Yunkai *v.* Liu Yuanchun)** [2023/4(32)FG]
33. **L'ultima sentenza della Corte Suprema del Regno Unito in materia di brevetti e IA nel caso Thaler DABUS** [2023/4(33)FG]

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

2023/4(1)SO

1. Adottato il Data Act: Regolamento (UE) 2023/2854 del 13.12.2023 sull'accesso equo ai dati e al loro utilizzo

Il 13 dicembre 2023 è stato adottato il *Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo*, noto come "**Data Act**" (di seguito anche "**DA**" o il "**Regolamento**"). La relativa proposta COM(2022) 68 *final*, contenente una bozza di regolamento e la sua relazione esplicativa (di seguito la "**Proposta**", la "**Bozza di Regolamento**" e la "**Relazione**"), era stata pubblicata il 23 febbraio 2022 (v. in questa Rubrica la notizia n. 4 del numero 1/2022 [2022/1(4)SO]: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf).
Successivamente, erano stati pubblicati il parere congiunto EDPB-EDPS sulla Proposta del 4 maggio 2022, riguardante il rispetto della normativa UE in materia di protezione e circolazione dei dati personali (di seguito il "**Parere congiunto EDPB-EDPS**": https://edpb.europa.eu/system/files/2023-03/edpb-edps_jointopinion_2022-02_data_act_proposal_it.pdf), i testi di compromesso e gli emendamenti del Consiglio e del Parlamento (sul primo, parziale, testo di compromesso del Consiglio della UE del 22 luglio 2022 - di seguito il "**First Presidency compromise text**" - v. in questa Rubrica la notizia n. 3 del numero 3/2022 [2022/3(3)RA]: http://www.personaemercato.it/wp-content/uploads/2022/09/Osservatorio.pdf).
Il **Capo I** del Data Act (artt. 1-2) ne definisce l'oggetto e il campo di applicazione e contiene le definizioni utilizzate nel corpo del provvedimento. L'art. 1(1) DA individua i seguenti sei obiettivi, da intendersi alla luce delle definizioni contenute nell'art. 2 DA:

a) la messa a disposizione all'utente di un prodotto connesso o di un servizio correlato dei dati generati dall'uso del prodotto connesso (dati del prodotto) e del servizio correlato (dati del servizio correlato): è l'oggetto della disciplina del Capo II;
b) la messa a disposizione di dati ai destinatari dei dati da parte dei titolari dei dati: è l'oggetto della disciplina del Capo III;
c) la messa a disposizione di dati, da parte dei titolari dei dati, agli enti pubblici, alla Commissione, alla Banca centrale europea e a organismi dell'Unione, a fronte di necessità eccezionali per l'esecuzione di un compito specifico svolto nell'interesse pubblico: è l'oggetto della disciplina del Capo V;
d) la facilitazione del passaggio da un servizio di trattamento dei dati all'altro: è l'oggetto della disciplina del Capo VI;
e) l'introduzione di garanzie contro l'accesso illecito di terzi ai dati non personali: è l'oggetto della disciplina del Capo VII; e
f) lo sviluppo di norme di interoperabilità per i dati a cui accedere, da trasferire e utilizzare: è l'oggetto della disciplina del Capo VIII.

A questi obiettivi, letteralmente così riassunti nell'art. 1(1) DA, va aggiunto quello del contrasto delle clausole abusive nei contratti tra imprese che hanno ad oggetto l'accesso ai dati e l'uso dei dati, che forma l'oggetto della disciplina del Capo IV.
Alla diversità degli obiettivi dei vari Capi del DA corrisponde una diversità tipologica dei dati che formano l'oggetto delle relative discipline. Ciò è chiarito nell'art. 1(2) DA, dove si specifica che:

- il Capo II si applica ai dati relativi alle prestazioni, all'uso e all'ambiente dei prodotti connessi, ad eccezione del contenuto;
- il Capo III si applica a tutti i dati del settore privato soggetti ad obblighi di condivisione per previsione di legge;
- il Capo IV si applica a tutti i dati del settore privato il cui accesso e utilizzo formano oggetto di contratti tra imprese;
- il Capo V si applica a tutti i dati del settore privato, e contiene anche norme specificamente dedicate ai dati non personali;
- il Capo VI si applica a tutti i dati e servizi trattati dai fornitori di servizi di trattamento dei dati;
- il Capo VII si applica a tutti i dati non personali detenuti nell'Unione da fornitori di servizi di trattamento dei dati.

Questa elencazione non contempla il Capo VIII che contiene la disciplina dell'interoperabilità.
L'art. 1(3) DA individua i soggetti destinatari e l'ambito territoriale di applicazione delle norme del Data Act, stabilendo *inter alia* il principio di irrilevanza del luogo di stabilimento. In particolare, è previsto che, con riguardo ai fabbricanti di prodotti connessi immessi sul mercato dell'Unione e ai fornitori dei servizi correlati, il DA si applica indipendentemente dal loro luogo di stabilimento. Il principio di irrilevanza del luogo di stabilimento trova applicazione anche in relazione ai titolari dei dati, che mettono dati a disposizione dei destinatari dei dati nell'Unione, e ai fornitori di servizi di

trattamento dei dati che offrono tali servizi a clienti nell'Unione.
Ad eccezione della definizione di «dati» e di poche altre, la maggior parte delle definizioni dell'art. 2 DA sono state modificate rispetto al testo della Bozza di Regolamento, e numerose nuove definizioni sono state introdotte.
La definizione di «**dati**» è la stessa contenuta nel Data Governance Act [Regolamento (UE) 2022/868 del 30.5.2022, su cui v. in questa Rubrica la notizia n. 1 del numero 2/2022 [2022/2(1)RA] http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf], ossia: "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva".
La nuova definizione di «**prodotto connesso**» è la seguente "un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente".
Il «**servizio correlato**» è definito come "un servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto al momento dell'acquisto, della locazione o del noleggio in modo tale che la sua assenza impedirebbe al prodotto connesso di svolgere una o più delle sue funzioni o che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto connesso".
L'art. 1(4) DA precisa che nei casi in cui il DA fa riferimento a prodotti connessi o a servizi correlati, tali riferimenti comprendono anche gli **assistenti virtuali** (definiti come "software che può elaborare richieste, compiti o domande, compresi quelli basati su input sonori o scritti, gesti o movimenti, e che, sulla base di tali richieste, compiti o domande, fornisce accesso ad altri servizi o controlla le funzioni dei prodotti connessi") nella misura in cui interagiscono con un prodotto connesso o un servizio correlato.
I «**dati del prodotto**» sono definiti come i "dati generati dall'uso di un prodotto connesso e progettati dal fabbricante in modo tale che un utente, un titolare dei dati o un terzo, compreso se del caso il fabbricante, possano reperirli tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo"
I «**dati di un servizio correlato**» sono definiti come i "dati che rappresentano la digitalizzazione delle azioni o degli eventi degli utenti relativi al prodotto connesso, registrati intenzionalmente dall'utente o generati come sottoprodotto dell'azione dell'utente durante la fornitura di un servizio correlato da parte del fornitore".
L'«**utente**» è definito come "una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato".
Il «**titolare dei dati**» («*data holder*» nella versione in lingua inglese del DA) è definito come "una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato".
Il «**destinatario dei dati**» è definito come "una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione".
Il «**servizio di trattamento dei dati**» è definito come "un servizio digitale fornito a un cliente e che consente l'accesso di rete universale e su richiesta a un pool condiviso di risorse informatiche configurabili, scalabili ed elastiche di natura centralizzata, distribuita o altamente distribuita e che può essere rapidamente erogato e rilasciato con un minimo sforzo di gestione o interazione con il fornitore di servizi".
Lo ***smart contract*** è così definito: "«**contratto intelligente**»: un programma informatico utilizzato per l'esecuzione automatica di un accordo o di parte di esso utilizzando una sequenza di registrazioni elettroniche di dati e garantendone l'integrità e l'accuratezza del loro ordine cronologico".
Nuove sono – tra le altre - le definizioni di metadati e di dati prontamente disponibili:

- "«**metadati**»: una descrizione strutturata del contenuto o dell'uso dei dati che agevola la ricerca o l'utilizzo di tali dati";
- "«**dati prontamente disponibili**»: dati del prodotto e dati di un servizio correlato che un titolare dei dati ottiene o può ottenere

legittimamente dal prodotto connesso o dal servizio correlato senza che ciò implichi uno sforzo sproporzionato che vada al di là di una semplice operazione". Quest'ultima definizione è particolarmente importante perché (anche questa è una innovazione rispetto alla Bozza di Regolamento) le limitazioni e gli obblighi del titolare dei dati ex artt. 4 e 5 DA riguardano soltanto i dati prontamente disponibili.

Importante appare la specificazione fatta dal **Considerando 15 DA** dove si esclude l'applicazione del DA ad importanti categorie di dati, precisamente alle "informazioni dedotte o ricavate [dai dati dei prodotti e dai dati dei servizi correlati], che sono il risultato di ulteriori investimenti nell'attribuzione di valori o informazioni derivanti dai dati, in particolare mediante algoritmi proprietari complessi, compresi quelli appartenenti a un software proprietario". Il Considerando 15 afferma che queste informazioni non dovrebbero essere soggette all'obbligo del titolare dei dati di metterle a disposizione di un utente o di un destinatario dei dati, salvo diverso accordo tra l'utente e il titolare dei dati. Ciò equivale a dire che queste informazioni non dovrebbero essere soggette alla disciplina dei Capi II e III del DA. Il Considerando 15 DA, prosegue specificando che può trattarsi, ad esempio, delle "informazioni ricavate dall'integrazione dei sensori, che consente di dedurre o ricavare i dati da più sensori, raccolti nel prodotto connesso, utilizzando algoritmi proprietari complessi, e che potrebbero essere soggetti a diritti di proprietà intellettuale".

Per quanto riguarda i dati personali, di particolare rilevanza sistematica sono i **Considerando 7 e 34 DA** dove si specifica che il DA non introduce una nuova base giuridica per il trattamento dei dati personali, diversa da quelle dell'art. 6 del Regolamento (UE) 2016/679 (il **GDPR**), nonché il **Considerando 35 DA** dove – a proposito della richiesta dell'utente di mettere i propri dati personali a disposizione di terzi - si specifica che il DA integra in vari modi il diritto di ricevere i dati personali e il diritto alla portabilità degli stessi a norma dell'art. 20 GDPR.

La finalità della disciplina del **Capo II** (artt. 3-7 DA) è consentire ai consumatori e alle imprese di accedere ai dati originati dall'uso dei prodotti connessi e dei servizi correlati. Secondo la specificazione dell'art. 1(2)(a) DA non rientrano nella disciplina del Capo II i "contenuti". Tale previsione deve mettersi in relazione al **Considerando 16**, dal quale si ricava che per "contenuti" si intendono la generalità di contenuti quali audio, video e testi, mentre sono generalmente sottoposti alla disciplina del Capo II, i dati "relativi alle prestazioni, all'uso e all'ambiente dei prodotti connessi e dei servizi correlati". Il Considerando 16 DA specifica inoltre che sono esclusi dalla disciplina del DA i "dati ottenuti, generati o consultati dal prodotto connesso, o ad esso trasmessi, a fini di archiviazione o altre operazioni di trattamento per conto di altre parti diverse dall'utente, come nel caso di server o infrastrutture cloud gestiti dai rispettivi proprietari interamente per conto di terzi, anche per uso da parte di un servizio online". L'art. 3 DA prevede che i prodotti e i servizi correlati debbano essere progettati in un modo che renda i dati e i pertinenti metadati facilmente accessibili "*by default*" e che gli utenti debbano essere informati su quali dati sono accessibili e sulle modalità di accesso. L'art. 4 prevede che i dati e i pertinenti metadati debbano essere messi dal titolare dei dati a disposizione dell'utente senza costi e, ove non direttamente accessibili, dietro semplice richiesta dell'utente. È tuttavia previsto che gli utenti e i titolari dei dati possano limitare o vietare contrattualmente l'accesso ai dati, il loro uso o la loro ulteriore condivisione nel caso in cui tale trattamento possa compromettere i requisiti di sicurezza del prodotto connesso, come previsto dal diritto dell'Unione o nazionale, e comportare gravi effetti negativi per la salute, la sicurezza o la protezione delle persone fisiche. Sono previste alcune disposizioni che condizionano il diritto di accesso in relazione a segreti commerciali, come definiti dalla Direttiva (UE) 2016/943, e altre che vietano all'utente di utilizzare i dati ottenuti dal titolare dei dati per sviluppare prodotti che competono con il prodotto da cui generano i dati. Laddove si tratti di dati personali e l'utente non sia la persona interessata, il titolare dei dati può rendere tali dati personali accessibili all'utente soltanto nel rispetto delle condizioni previste dall'art. 6(1) GDPR, e, ove applicabile, dall'art. 9 GDPR. L'art. 4(13) DA prevede che il titolare dei dati può utilizzare i «dati non personali prontamente disponibili» soltanto sulla base di un accordo con l'utente. Questa disposizione *a contrario* significa che il titolare dei dati è libero di utilizzare come vuole i dati non personali *non* prontamente disponibili. L'art. 4(13) fa inoltre divieto al titolare dei dati di utilizzare i dati personali prontamente disponibili per trarne delle informazioni sull'utente in un qualsiasi modo che possa danneggiare la posizione commerciale dell'utente nei mercati in cui l'utente è attivo. Per quanto riguarda invece la generalità dei dati non personali, l'art. 4(14) DA prevede che i titolari dei dati possano metterli a disposizione di terzi purché al fine dell'esecuzione del loro contratto con

l'utente, e che, in questo caso, i titolari dei dati debbano vincolare contrattualmente i terzi a non condividere ulteriormente i dati da essi ricevuti. L'art. 5 prevede il diritto dell'utente di chiedere al titolare dei dati di mettere i dati prontamente disponibili, e i pertinenti metadati, a disposizione di terzi senza spese per l'utente. L'art. 5 prevede che le imprese qualificate come gatekeeper ai sensi dell'art. 3 del Regolamento (UE) 2022/1925, c.d. Digital Markets Act ("**DMA**") [sulla designazione dei gatekeeper v. in questa Rubrica la notizia n. 12 *infra* in questo numero [2023/4(12)RA] e la notizia n. 3 del numero 3/2023 [2023/3(3)RA]: http://www.personaemercato.it/wp-content/uploads/2023/11/Osservatorio.pdf; sul DMA v. in questa Rubrica la notizia n. 2 del numero 4/2022 [2022/4(2)VR]: http://www.personaemercato.it/wp-content/uploads/2023/01/Osservatorio.pdf] non possano godere dei diritti dei terzi ai sensi del medesimo articolo ed è fatto loro divieto sia di sollecitare in qualsiasi modo l'utente affinché l'utente metta loro a disposizione o chieda al titolare dei dati di mettere a disposizione i dati, che di ricevere effettivamente dall'utente i dati che l'utente ha ricevuto in seguito ad una richiesta ex art. 4(1)DA. L'art. 5 DA contiene inoltre, relativamente al diritto dell'utente di condividere i dati prontamente disponibili con i terzi, alcune disposizioni analoghe a quelle dell'art. 4 DA. L'art. 6 DA prevede gli obblighi e i divieti in capo ai terzi ai quali vengono messi a disposizione i dati ai sensi dell'art. 5 DA. È previsto che il trattamento dei dati da parte di questi soggetti debba essere limitato alle finalità e alle condizioni concordate con l'utente, nel rispetto dei diritti della persona interessata, relativamente ai dati personali, e con obbligo di cancellazione dei dati quando essi cessano di essere necessari per la finalità concordata. Tra i divieti è previsto anche in capo ai terzi il divieto di mettere i dati a disposizione di imprese designate come gatekeeper ai sensi del DMA. Infine, l'art. 7 AD dispone che gli obblighi del Capo II DA non si applicano ai dati generati da prodotti realizzati o da servizi correlati prestati da piccole e microimprese (ai sensi dell'art. 2 parr. 2 e 3 dell'allegato della raccomandazione 2003/361/CE).

Il **Capo III** (artt. 8-12) detta alcune regole da osservarsi allorquando i titolari dei dati sono obbligati (o sulla base di quanto previsto nel Capo II o sulla base di altre disposizioni del diritto dell'Unione o degli Stati membri) a mettere i dati a disposizione dei destinatari dei dati. Gli artt. 8 e 9 DA prescrivono che le condizioni della messa a disposizione dei dati da parte dei titolari dei dati in favore dei destinatari dei dati debbano essere eque e non discriminatorie, e che, laddove sia previsto un corrispettivo, esso debba essere ragionevole, senza pregiudizio per altre disposizioni del diritto dell'Unione o del diritto nazionale derivato di escludere o ridurre un simile corrispettivo. È previsto in ogni caso che ai destinatari dei dati aventi le dimensioni di microimprese, piccole o medie imprese (ai senso dell'allegato della Raccomandazione 2003/361/CE) non possa essere chiesto un corrispettivo il cui importo ecceda i costi sopportati dai titolari dei dati per mettere i dati a loro disposizione, salvo che sia diversamente previsto nelle legislazioni di settore. L'art. 10 DA prevede che organi speciali, certificati dagli Stati membri, siano dedicati alla risoluzione di controversie tra i titolari di dati e i destinatari di dati aventi ad oggetto la determinazione delle condizioni di messa a disposizione dei dati ai sensi degli articoli 8 and 9.

Il **Capo IV** (composto del solo art. 13) intitolato "clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo tra imprese" riguarda le clausole contrattuali concernenti l'accesso a dati o l'uso di dati o la responsabilità e i rimedi per l'inadempimento o l'estinzione di obblighi relativi a dati, che siano "imposte unilateralmente" da imprese a microimprese, piccole o medie imprese (come definite nell'allegato alla raccomandazione 2003/361/CE). L'art. 13(1) DA prevede che simili clausole non sono vincolanti se *(i)* sono state imposte unilateralmente da un'impresa ad un'altra impresa, e *(ii)* se sono abusive. Quanto al primo requisito, l'art. 13(6) DA stabilisce che esso ricorre quando un contraente inserisce una clausola senza che l'altro contraente sia stato in grado di influenzarne il contenuto malgrado un tentativo di negoziarla, e pone a carico del predisponente l'onere di provare l'assenza di imposizione. Quanto al secondo requisito, lo strumento del test di abusività prevede una definizione generale di abusività (una clausola è abusiva se "il suo utilizzo si discosta considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza" [art.13(3) DA] e due elenchi di clausole, uno relativo a clausole da intendersi in ogni caso abusive (tra cui quelle che consentono al predisponente di determinare la "conformità dei dati al contratto") [art.13(4) DA] e l'altro di clausole che si presumono abusive [art.13(5) DA]. L'art. 41 DA (contenuto nel Capo IX) prevede che la Commissione debba predisporre e raccomandare clausole contrattuali tipo relative all'accesso ai dati e al relativo uso, nonché per i contratti di cloud computing, come strumento di ausilio alle parti

nella redazione e negoziazione di contratti con diritti e doveri contrattuali equilibrati.

Il **Capo V** (artt. 14-22) è inteso a creare un quadro armonizzato di regole per l'acquisizione e l'utilizzo da parte di enti pubblici, la Commissione, la Banca centrale europea o organismi dell'Unione di dati detenuti da imprese in situazioni nelle quali si riscontra una esigenza eccezionale dei dati richiesti. Diversamente da quanto prevedeva la Bozza di Regolamento, è stata prevista una diversificazione tra dati personali e non personali, tale per cui la richiesta di dati personali può avvenire solo in caso di necessità eccezionale di utilizzare determinati dati per rispondere ad una «emergenza pubblica», come definita nell'art. 2, n. 29 DA, e l'autorità richiedente non può ottenere i dati con mezzi alternativi in modo tempestivo ed efficace a condizioni equivalenti [art. 15(1)(a) DA], mentre più ampia è la casistica che consente di chiedere dati non personali [art. 15(1)(b) DA].

La definizione di «**emergenza pubblica**» è la seguente: "una situazione eccezionale, limitata nel tempo, come un'emergenza di sanità pubblica, un'emergenza derivante da calamità naturali, una grave catastrofe di origine antropica, compreso un grave incidente di cibersicurezza, che incide negativamente sulla popolazione dell'Unione o su tutto o parte di uno Stato membro, con il rischio di ripercussioni gravi e durature sulle condizioni di vita o sulla stabilità economica, sulla stabilità finanziaria, o di un sostanziale e immediato degrado delle risorse economiche nell'Unione o nello Stato membro o negli Stati membri interessati e che è determinata o dichiarata ufficialmente in conformità delle pertinenti procedure previste dal diritto dell'Unione o nazionale".

È previsto che nei casi di necessità eccezionale di rispondere ad una emergenza pubblica ex art. 15(1)(a) DA, i dati dovranno essere messi a disposizione gratuitamente. Negli altri casi di necessità eccezionale ex art. 15(1)(b) DA, il titolare dei dati che mette i dati a disposizione ha diritto a una remunerazione comprensiva dei costi più un margine ragionevole. Per evitare abusi, è previsto che le richieste debbano essere proporzionate, che esse debbano indicare chiaramente gli obiettivi che si intendono perseguire e che rispettino gli interessi dei titolari dei dati che mettono i dati a disposizione. È previsto che autorità competenti *ad hoc* siano investiti del compito di assicurare la trasparenza e la pubblicazione di tutte le richieste e di gestire le relative eventuali doglianze. Fermo restando che, per quanto riguarda i dati personali, il DA non costituisce nemmeno in relazione alla disciplina del Capo V una nuova base giuridica per il trattamento dei dati personali - e che dunque deve aversi riguardo all'art. 6(1)(e) GDPR e al ruolo del diritto dell'Unione ex art. 6(3) GDPR [cfr. **Considerando 69 Data Act**] – il DA prevede cautele specifiche per la protezione dei dati personali e riflette una preferenza per la raccolta di dati non personali o pseudonomizzati o anonimizzati. In particolare, l'art. 17(1)(g) DA prevede che: "qualora siano richiesti dati personali" il richiedente debba specificare "le misure tecniche e organizzative necessarie e proporzionate per attuare i principi di protezione dei dati e le garanzie necessarie, quali la pseudonimizzazione, come anche la possibilità o meno, per il titolare dei dati, di applicare l'anonimizzazione prima di mettere i dati a disposizione".

Il Capo **VI** (artt. 23-31 DA) prevede in capo ai fornitori di servizi di trattamento dei dati (quali servizi *cloud* ed *edge*) una serie di requisiti di natura contrattuale, commerciale e tecnica (di cui agli artt. 23, 25, 26, 27, 29 e 30 DA) al fine di consentire il «**passaggio**» tra servizi (come definito all'art. 2, n. 34 DA) ovvero di eliminare gli ostacoli all'effettivo passaggio. In particolare, il Regolamento mira ad assicurare che i clienti conseguano una «**equivalenza funzionale**» (come definita all'art. 2, n. 37 DA) nell'utilizzazione del servizio dopo che essi hanno ottenuto il passaggio ad un altro fornitore del servizio. Il contrasto alle «**tariffe di passaggio**» (come definite all'art. 2, n. 36 DA) è al centro delle disposizioni dell'art. 29 DA, che prevede una loro abolizione graduale, con un divieto a decorrere dal 12 gennaio 2027 ed un regime di tariffe ridotte nel triennio precedente (dall'11.1.2024 al 12.1.2027).

Il **Capo VII** (composto del solo art. 32 DA) mira a contrastare un illegittimo accesso governativo internazionale e di paesi terzi ai dati non personali detenuti nell'Unione da fornitori di servizi di trattamento dei dati offerti nel mercato dell'Unione, o un illegittimo trasferimento di tali dati fuori dalla UE. Al riguardo sono previsti in capo ai fornitori di servizi di trattamento dei dati una serie di obblighi di salvaguardia di natura tecnica, legale e organizzativa, ivi comprese condizioni e limitazioni per il riconoscimento o l'esecutività di provvedimenti di organi giurisdizionali ed amministrativi di paesi extra UE.

Il **Capo VIII** (artt. 33-36 DA) prevede alcune prescrizioni relative alla «**interoperabilità**» (come definita nell'art. 2, n. 40 DA). Sono prescritti una serie di requisiti essenziali relativamente all'interoperabilità dei dati, dei meccanismi e servizi di condivisione dei dati, degli spazi comuni europei di dati (art. 33 DA) e dei servizi di trattamento dei dati (art. 35 DA). L'art. 34 DA prevede l'applicazione di alcune norme in materia di passaggio ai casi di uso in parallelo dei servizi di

trattamento dei dati, e regola le «**tariffe di uscita di dati**» (come definita all'art. 2, n. 35 DA). Infine, l'art. 36 DA fissa alcuni requisiti essenziali relativi agli smart contract per l'esecuzione degli accordi di condivisione dei dati.
Il **Capo IX** (artt. 37-42 DA) prevede *inter alia* che gli Stati membri designino una o più autorità competenti per l'applicazione delle disposizioni del Regolamento, per l'esame di doglianze nonché per l'irrogazione di sanzioni per il caso di violazioni delle medesime disposizioni.
Il **Capo X** (composto del solo art. 43 DA) prevede che il diritto *sui generis* di cui alla direttiva sulle banche di dati (Direttiva 96/9/CE) non si applichi alle banche di dati ottenute o generate dall'uso di un prodotto connesso o di un servizio correlato. Tale previsione mira ad evitare che possano essere compromessi i diritti degli utenti ai sensi degli artt. 4 e 5 DA.
Infine, il **Capo XI** (artt. 44-50) prevede alcune disposizioni finali. L'art. 44 DA prevede la salvezza degli obblighi specifici disposti in, o sulla base di atti giuridici dell'Unione entrati in vigore fino all'11.1.2024, e dispone che il DA non pregiudica la normativa UE di settore. L'art. 45 DA autorizza la Commissione ad adottare atti delegati per introdurre un meccanismo di monitoraggio sulle tariffe di passaggio e al fine di specificare i requisiti essenziali riguardanti l'interoperabilità. L'art. 50 DA prevede che il Regolamento si applichi a decorrere dal **12.9.2025**, e che alcune disposizioni si applicheranno in relazione a prodotti immessi sul mercato o ad obblighi o rapporti giuridici sorti in date successive rispetto a tale data.

SALVATORE ORLANDO

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:L_202302854

2023/4(2)SO

2. Annunciato l'accordo politico sull'AI Act

Con un comunicato stampa del 9 dicembre 2023, il Parlamento europeo (**PE**) ha annunciato che nella notte tra l'8 e il 9 dicembre i negoziatori del PE e del Consiglio hanno concluso un accordo politico su un testo dell'AI Act (il "**Comunicato Stampa**"). La proposta dell'AI Act risale all'aprile 2021 (la "**Proposta della Commissione**": v. su questa Rubrica notizia n. 1 sul numero 2/2021 http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf [2021/2(1)SO]; nonché, sugli emendamenti votati dal PE la scorsa estate, v. notizia n. 4 sul numero 2/2023 http://www.personaemercato.it/wp-content/uploads/2023/08/Osservatorio.pdf [2023/2(4)SO]).
Il Comunicato Stampa si sofferma sui punti essenziali concordati, e che dovranno essere riflessi nel testo definitivo del regolamento (di seguito anche il "**Regolamento**"), ossia: sulle applicazioni proibite e sulle eccezioni relative ad esigenze di contrasto di certi reati; sugli obblighi inerenti ai sistemi di IA c.d. ad alto rischio; sulle nuove norme relative ai c.d. sistemi e ai modelli di IA per finalità generali; sulle misure di supporto per l'innovazione e le piccole e medie imprese; nonché sulle sanzioni e sull'entrata in vigore.
In conseguenza di un nuovo Titolo dedicato alle nuove norme relative ai c.d. sistemi e ai modelli di IA per finalità generali, il Regolamento dovrebbe comporsi di tredici Titoli.
Il **Titolo I** è dedicato alle disposizioni generali. In esso sono contenute anche le definizioni. L'ultima definizione di sistemi di IA – modificata rispetto a quella proposta dalla Commissione – dovrebbe riprendere ed ulteriormente sviluppare quella accolta in ambito OCSE: «un sistema automatizzato [*a machine-based system*] progettato per operare con livelli di autonomia variabili, che può mostrare adattabilità dopo essere stato reso operativo, e che, per obiettivi espliciti o impliciti, inferisce, dall'*input* che riceve, come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».
Il **Titolo II** è dedicato ai divieti assoluti di «immissione sul mercato, messa in servizio» e/o di «uso» di determinati sistemi di IA individuati o tipologicamente o relativamente all'ambito di applicazione (i.e. alcuni sistemi di IA sono assoggettati al divieto solo relativamente a determinati ambiti di applicazione, es. i sistemi di identificazione biometrica da remoto in tempo reale, il cui uso è vietato solo nell'ambito del *law enforcement*, o i sistemi di riconoscimento delle emozioni la cui immissione sul mercato, messa in servizio e uso sono vietati solo nei luoghi di lavoro e negli istituti di educazione).
Il **Titolo III** è dedicato ai sistemi di IA ad alto rischio. Si preannuncia una nuova tecnica di qualificazione e si conferma il ruolo centrale dell'allegato contenenti elenchi di sistemi di IA (e anche di casi d'uso, in realtà) divisi in 8 aree: **Biometrica**; **Infrastrutture critiche**; **Istruzione**; **Occupazione**; **Servizi essenziali**; **Attività di contrasto**; **Migrazione**; **Amministrazione della giustizia e processi democratici**. In questo Titolo, il più corposo del regolamento, si trovano le disposizioni tipiche delle discipline UE dei prodotti

(sicurezza-normazione-valutazione della conformità-accreditamento-organismi notificati-marchio CE), in particolare di quelle del c.d. Nuovo Quadro Legislativo (*New Legislative Framework*, "NLF": cfr. Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio del 9.7.2008 su un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE; regolamento (UE) 2019/1020 2019/1020 sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011), adattate alle particolarità dei sistemi di IA.

Il **Titolo IV** riguarda i c.d. doveri di trasparenza e si applica a particolari sistemi di IA, molti dei quali qualificabili «ad alto rischio» ed inoltre anche a sistemi che impiegano modelli di IA c.d. *general purpose* ossia disegnati e impiegabili per finalità generali. Essi costituiscono la novità che il legislatore europeo ha dovuto fronteggiare – in corso d'opera - con l'avvento di ChatGPT e dei modelli impiegati per primo da Open AI.

Il **Titolo successivo, nuovo rispetto alla Proposta della Commissione** riguarda proprio questi modelli, e pone specifici obblighi ai relativi fornitori distinguendo ulteriormente i modelli che presentano un rischio sistemico, come appositamente definito.

Il **Titolo seguente** riguarda gli spazi di sperimentazione normativa (*regulatory sandbox*).

Il **Titolo seguente** riguarda le istituzioni a cui è affidata la governance. Oltre all'Ufficio europeo per l'IA e le autorità nazionali, spicca la novità del collegio scientifico di esperti indipendenti che dovrebbero essere incaricati in particolare di seguire le tematiche relative ai modelli di IA per finalità generali, a conferma dell'attenzione speciale verso questo sviluppo tecnologico.

Il **Titolo seguente** è dedicato alla banca dati dei sistemi di IA ad alto rischio.

Il **Titolo seguente** «Monitoraggio successivo all'immissione sul mercato, condivisioni di informazioni e vigilanza del mercato», contiene un nuovo capo, intitolato «rimedi» che tra l'altro prevede un potere individuale di qualunque persona fisica o ente di inoltrare una doglianza su presunte violazioni del regolamento, al fine di attivare i controlli e le eventuali sanzioni previste dal regolamento e il c.d. diritto alla spiegazione, ricalcato sul modello della dottrina formatasi sull'art. 22 GDPR.

Il **Titolo seguente** prevede i codici di condotta che possono essere elaborati ed osservati su base volontaria relativamente ai sistemi non ad alto rischio.

Il **Titolo seguente** contiene i doveri di riservatezza e le sanzioni (incrementate e modificate rispetto alla Proposta della Commissione: fino a 35 milioni di euro o al 7% del fatturato globale o fino a 7,5 milioni di euro o al 1,5 % del fatturato, a seconda della natura della violazione e della dimensione della società).

Vi sono poi **gli ultimi due Titoli** dedicati alle deleghe di poteri e alle disposizioni finali, quest'ultimo con la previsione di quando il regolamento sarà applicabile generalmente, e la specificazione che alcune disposizioni saranno applicabili in tempi diversi (termine generale di applicazione fissato a 24 mesi dall'entrata in vigore, con alcune disposizioni applicabili già dopo sei mesi, ed altre ancora dopo 36 mesi).

SALVATORE ORLANDO

https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

2023/4(3)CR

3. Il secondo parere dell'EDPS sulla proposta di AI Act

Il 23 ottobre 2023 il Garante europeo per la protezione dei dati personali (**EDPS**) ha pubblicato il Parere 44/2023 (di seguito anche il "**Parere**") avente ad oggetto la proposta di Regolamento del Parlamento UE e del Consiglio che stabilisce norme armonizzate sull'Intelligenza Artificiale ("**Artificial Intelligence Act**" o "**AI Act**").

Il Parere segue quello già pubblicato dall'EDPS congiuntamente con l'*European Data Protection Board* (**EDPB**) nel giugno 2021 (di seguito "**Joint Opinion**", su cui v. in questa Rubrica la notizia n. 3 del numero 3/2021: http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf [2021/3(3)CR]) e mira a fornire ulteriori suggerimenti e raccomandazioni in vista delle negoziazioni per il testo finale dell'AI Act.

In primo luogo, l'EDPS ribadisce un punto cruciale evidenziato nella Joint Opinion, ovvero la necessità di vietare gli usi dei sistemi di IA che pongono rischi inaccettabili per i diritti fondamentali delle persone. Tra questi vengono menzionati, in particolare, l'utilizzo dell'IA per effettuare qualsiasi tipo di "social scoring", per il riconoscimento automatico di caratteristiche umane in spazi accessibili al pubblico, per dedurre le emozioni (salvo alcuni casi specifici come usi sanitari o di ricerca, comunque con l'adozione di adeguate misure di salvaguardia) e per effettuare valutazioni

del rischio individuale di persone fisiche al fine di valutare il rischio di reato o di recidiva.
L'EDPS fornisce poi una serie di raccomandazioni con riferimento all'ambito di applicazione del futuro regolamento sull'IA. Da un lato, rispetto ai sistemi di IA, l'EDPS suggerisce di rimuovere la previsione che esclude dall'ambito di applicazione dell'AI Act i sistemi ad alto rischio già presenti sul mercato al momento dell'entrata in vigore del regolamento, salvo che subiscano sostanziali modifiche. Questa esclusione, infatti, avrebbe come conseguenza quella di consentire l'utilizzo di sistemi che presentano rischi elevati per le persone senza l'obbligo di adottare le misure di garanzia previste dal regolamento. Dall'altro lato, rispetto ai soggetti sui quali ricade l'obbligo di rispettare la gran parte delle previsioni dell'AI Act, definiti "*providers*" (fornitori) in relazione allo "sviluppo" di sistemi di IA, l'EDPS chiede che vengano meglio chiarite tali definizioni che, per la loro genericità, potrebbero dar luogo a incertezze e zone grigie.
Una parte significativa del Parere si concentra sul ruolo e sui poteri attribuiti all'EDPS dalla proposta di regolamento. L'AI Act designa, infatti, l'EDPS come organismo notificato e autorità di vigilanza del mercato per valutare la conformità dei sistemi di IA ad alto rischio sviluppati o utilizzati dalle istituzioni europee, nonché come autorità competente per la supervisione della fornitura e dell'uso dei sistemi di IA da parte delle Istituzioni UE.
L'EDPS vede in maniera favorevole l'attribuzione di questi ruoli, ma chiede che i suoi compiti e i suoi poteri vengano definiti in maniera più puntuale dal regolamento e ribadisce la necessità di risorse finanziarie e umane adeguate per svolgere tali nuovi incarichi.
Rispetto invece al diritto di presentare un reclamo in caso di violazione dell'AI Act, L'EDPS ritiene che il regolamento dovrebbe prevedere espressamente la propria competenza a ricevere i reclami. Inoltre, le singole autorità di protezione dei dati personali nazionali dovrebbero essere designate come competenti a vigilare anche sull'applicazione delle disposizioni contenute nel regolamento. Dal momento che le tematiche di protezione dei dati sono strettamente collegate all'utilizzo dell'IA, infatti, tali autorità sono nella posizione migliore, per competenza, esperienza e capillarità, per ricoprire questo ruolo.
Infine, l'EDPS accoglie con favore l'istituzione dell'Ufficio europeo per l'intelligenza artificiale ("**Ufficio AI**") avente l'obiettivo di centralizzare l'applicazione della legge sull'AI e di armonizzarne l'applicazione negli Stati membri. L'EDPS si dichiara pronto a svolgere indagini congiunte su un piano di parità con le autorità di controllo nazionali e a partecipare alle altre attività dell'Ufficio AI. A tal fine, l'autorità ritiene opportuno che le vengano attribuiti i diritti di voto come membro a pieno titolo del consiglio di amministrazione dell'Ufficio AI e chiede di assumere il ruolo di fornitore del segretariato per tale ufficio (ruolo già ricoperto presso l'EDPB).

CHIARA RAUCCIO

https://edps.europa.eu/data-protection/our-work/publications/opinions/2023-10-23-edps-opinion-442023-artificial-intelligence-act-light-legislative-developments_en

2023/4(4)TDMCDV

4. La dichiarazione del Summit di Bletchey Park sulla IA del 1-2.11.2023

Nelle giornate dell'1 e 2 novembre 2023 si è tenuto, presso la tenuta di Bletchley Park a Bletchley nel Buckinghamshire in Inghilterra, il primo Summit globale sulla sicurezza dell'Intelligenza Artificiale (*global AI Safety Summit*), che ha riunito i rappresentanti delle nazioni leader nel campo dell'IA, aziende tecnologiche, ricercatori e gruppi della società civile per il dichiarato fine di dare impulso ad uno sviluppo sicuro e responsabile dell'IA a livello globale. Ventotto paesi di tutto il mondo (Australia, Brasile, Canada, Cile, Cina, Francia, Germania, India, Indonesia, Irlanda, Israele, Italia, Giappone, Kenya, Arabia Saudita, Paesi Bassi, Nigeria, Filippine, Corea, Rwanda, Singapore, Spagna, Svizzera, Turchia, Ucraina, Emirati Arabi, Regno Unito e Irlanda del Nord, Stati Uniti) e l'Unione Europea hanno approvato la Dichiarazione di Bletchley sulla sicurezza dell'IA (di seguito anche la "**Dichiarazione**"), che riconosce l'urgente necessità di comprendere e gestire congiuntamente i rischi potenziali legati a questa tecnologia attraverso un rinnovato impegno internazionale per garantire che l'IA venga sviluppata e impiegata in modo sicuro e responsabile a beneficio della comunità globale (link alla notizia: https://www.aisafetysummit.gov.uk/). Di seguito i tratti salienti del contenuto della Dichiarazione.
L'IA offre enormi opportunità a livello globale. Essa ha il potenziale per trasformare e migliorare il benessere, la pace e la prosperità dell'umanità. Infatti, l'IA è già presente in molti ambiti della vita quotidiana – come le abitazioni, il lavoro, i trasporti, l'istruzione, la salute, l'accessibilità e la

giustizia, e la sua diffusione è destinata ad aumentare. A tal fine, però, è necessario che l'IA sia progettata, sviluppata, implementata e utilizzata in maniera sicura, incentrata sull'uomo (*human-centric*), affidabile (*trustworthy*) e responsabile (*responsible*). Per tale ragione, vengono accolti con favore gli sforzi di cooperazione fatti sinora dalla comunità internazionale per promuovere la crescita economica inclusiva, lo sviluppo sostenibile, l'innovazione, la protezione dei diritti umani e delle libertà fondamentali e per favorire la fiducia nei sistemi di IA. Si riconosce che l'umanità si trova in un momento unico per agire nella direzione di affermare la necessità di uno sviluppo sicuro dell'IA affinché le sue opportunità trasformative vadano a beneficio di tutti e in modo inclusivo. Tali azioni devono includere servizi pubblici come salute ed educazione, la sicurezza alimentare, la scienza, l'energia pulita, la biodiversità e il clima, al fine di garantire il godimento dei diritti umani e raggiungere gli obiettivi di sviluppo sostenibile delle Nazioni Unite.

Nella Dichiarazione si riconosce che, oltre alle opportunità, lo sviluppo e l'impiego dell'IA comportano però anche significativi rischi che richiedono di essere affrontati con urgenza. I partecipanti, perciò, accolgono con favore i rilevanti sforzi internazionali fatti per esaminare e affrontare l'impatto potenziale dei sistemi di IA, riconoscendo altresì la necessità di tutelare i diritti umani, la trasparenza, la giustizia, la responsabilità, la regolamentazione, la sicurezza, la supervisione umana, l'eticità, la riduzione dei *bias*, la privacy e la protezione dei dati. Si reputa necessario identificare i rischi imprevisti legati alla capacità di manipolare contenuti o generare contenuti ingannevoli. Particolari rischi sorgono, poi, dai modelli di IA per finalità generali (*general-purpose AI*), compresi i modelli di base (*foundation models*), capaci di eseguire una vasta gamma di compiti, così come da alcuni modelli di IA per finalità specifiche (*narrow AI*) che potrebbero manifestare potenzialità dannose.

Rischi significativi sono identificati in relazione alla difficile comprensibilità circa le concrete capacità dell'IA, che le rende difficili da prevedere e da allineare con la volontà umana. I partecipanti concordano nel ritenere particolarmente preoccupanti i rischi che possono verificarsi in settori come la cybersicurezza e la biotecnologia, nonché i settori in cui i sistemi di IA possono amplificare rischi esistenti, come la disinformazione. Data la rapida e incerta evoluzione dell'IA e il contesto di accelerazione degli investimenti nella tecnologia, viene riconosciuta la necessità di approfondire la comprensione di questi potenziali rischi e delle azioni per affrontarli, tenendo conto che molti di essi hanno carattere intrinsecamente internazionale e, perciò, richiedono forme di cooperazione tra diversi stati.

In quest'ottica, gli stati firmatari si impegnano a lavorare insieme in modo inclusivo per garantire una IA *human-centric*, affidabile, responsabile, sicura e a sostegno del bene di tutti. In tal modo, i paesi dovrebbero considerare l'importanza di un approccio di *governance* e regolamentazione proporzionato che massimizzi i benefici e tenga conto dei rischi associati all'IA. Questo potrebbe includere, laddove opportuno, classificazioni e categorizzazioni del rischio basate sulle specifiche esperienze e legislazioni nazionali, anche se è da evidenziare la rilevanza della cooperazione nello sviluppo di principi comuni e codici di condotta condivisi. Per quanto riguarda i rischi specifici più probabili legati all'IA, è stato dichiarato l'impegno di intensificare e sostenere la cooperazione e ad allargarla ad ulteriori paesi, per identificare, comprendere e, se opportuno, agire attraverso le attuali organizzazioni internazionali e altre iniziative rilevanti, compresi futuri Summit internazionali sulla sicurezza dell'IA.

In definitiva, è stato riconosciuto che tutti gli attori globali hanno un ruolo da svolgere per garantire la sicurezza dell'IA: nazioni, organizzazioni internazionali e altre realtà, come aziende, società civile e università. Riconoscendo l'importanza di un'IA inclusiva e del superamento del *digital divide*, è stato dichiarato che la cooperazione internazionale dovrà impegnarsi a coinvolgere un'ampia gamma di partner e accogliere approcci e politiche orientati allo sviluppo, in modo da aiutare i paesi in via di sviluppo a potenziare la formazione sull'IA e sfruttare il suo ruolo per sostenere la crescita sostenibile e affrontare il divario nello sviluppo.

Pur riconoscendo l'importanza della sicurezza lungo l'intero ciclo di vita dell'IA, si è specificato che gli attori che sviluppano IA "di frontiera" – cioè, quei sistemi di IA eccezionalmente potenti e potenzialmente dannosi – hanno una responsabilità peculiare nel garantire la sicurezza di tali sistemi attraverso accurati test di sicurezza, valutazioni e altre misure appropriate, cui deve accompagnarsi un adeguato apparato di trasparenza e monitoraggio per mitigare le potenzialità dannose dell'IA.

Nel contesto di questa cooperazione, è stato concordato che l'agenda per affrontare i rischi dell'IA di frontiera si concentrerà su due aspetti particolari:

1) identificare rischi di interesse comune, costruire una comprensione scientifica condivisa e basata su prove (*evidence-based*) di questi rischi, e aggiornare

tale comprensione man mano che le capacità dei sistemi aumentano;
2) attuare politiche basate sul rischio nei rispettivi paesi per garantire la sicurezza alla luce dei rischi identificati, collaborando nel rispetto della diversità e della specificità degli approcci e delle singole esperienze nazionali.
Per perseguire gli obiettivi posti da questa agenda, i firmatari si sono impegnati a costruire una rete internazionale di ricerca scientifica sulla sicurezza dell'IA di frontiera, che completi e implementi le iniziative esistenti e favorisca nuove forme di collaborazione e un dialogo globale inclusivo.
Infine, la Dichiarazione si chiude con l'auspicio dei firmatari di incontrarsi nuovamente nel 2024.

TOMMASO DE MARI CASARETO DAL VERME

https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

2023/4(5)FDA

5. Le disposizioni in materia di IA e di meccanismi automatizzati impiegati per l'adozione delle decisioni della PA contenute nella legge spagnola sulla parità di trattamento e sulla non discriminazione (Ley 15/2022)

Con la legge n. 15 del 12 luglio 2022 il parlamento di Spagna ha adottato un corpo di norme che recano i principi fondamentali del "*diritto spagnolo antidiscriminatorio*" (così il § II del preambolo).
La nuova legislazione persegue un duplice obiettivo: da un lato prevenire ed eliminare ogni forma di discriminazione, cercando di coniugare un approccio preventivo con quello riparativo (così il § III del preambolo: "*La ley persigue un doble objetivo: prevenir y erradicar cualquier forma de discriminación y proteger a las víctimas, intentando combinar el enfoque preventivo con el enfoque reparador*"); dall'altro promuovere il diritto alla parità di trattamento di ogni individuo (art. 1, co. 1: "*derecho a la igualdad de trato*"), indipendentemente dalla sua nazionalità (art. 2, co. 1: "*con independencia de su nacionalidad*"), tanto nei luoghi di vita pubblica come in quelli privati (art. 3).
Nelle intenzioni del legislatore spagnolo il testo normativo dovrebbe sia costituire uno "*instrumento eficaz contra toda discriminación que pueda sufrir cualquier persona*" (così il § II del preambolo), sia rafforzare il "*derecho a la igualdad*" e il "*disfrute de todos los derechos fundamentales y libertades públicas*" (così il § I del preambolo); motivo per cui il concetto di discriminazione che vi è accolto abbraccia "*toda disposición, conducta, acto, criterio o práctica que atente contra el derecho a la igualdad*" (art. 4, co. 1).
Ciò detto, la legge spagnola si segnala perché declina il descritto principio di non discriminazione anche al campo dell'intelligenza artificiale e dei meccanismi decisionali automatizzati nella pubblica amministrazione.
In particolare è l'art. 23 – rubricato "*Inteligencia Artificial y mecanismos de toma de decisión automatizados*" – a stabilire al comma 1 che gli algoritmi utilizzati nelle decisioni amministrative devono essere impostati secondo criteri che riducano al minimo eventuali pregiudizi per i terzi e siano controllabili ove tecnicamente fattibile: "*las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente*" (formula, quest'ultima, che a una prima lettura appare non particolarmente felice e risulta anzi volutamente ambigua, necessitando della mediazione giurisprudenziale in funzione interpretativa).
A tal fine è dovere di ogni amministrazione assicurare la trasparenza del processo decisionale automatizzato e, in particolare, l'intellegibilità dell'algoritmo (così il comma 2: "*Las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos*"), affinché l'uso dell'intelligenza artificiale sia etico e rispetti i diritti individuali (così il comma 3: "*Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales*").
A completare il sistema la legge spagnola prevede forme di compensazione economica a favore dei danneggiati in tutti i casi di violazioni accertate con sentenza dell'autorità giudiziaria (artt. 27-30); e istituisce un'apposita autorità amministrativa indipendente "*para la Igualdad de Trato y la No Discriminación*" con poteri di vigilanza e sanzionatori (art. 40).

FILIPPO D'ANGELO

https://www.boe.es/buscar/act.php?id=BOE-A-2022-11589#a2-5

2023/4(6)DI

6. La legge francese sulla *vidéosurveillance algorithmique* per le Olimpiadi e Paralimpiadi Paris 2024

In vista dei Giochi della XXXIII Olimpiade che si terranno a Parigi dal 26 luglio all'11 agosto 2024 (Paris 2024), il Parlamento francese ha adottato lo scorso 19 maggio 2023 la *Loi n° 2023-380 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions* (*Loi n° 2023-380*). Tra i vari argomenti connessi a Paris 2024, questa legge interviene anche rispetto al tema della sicurezza e a tal fine contiene una disciplina in tema di trattamento algoritmico delle immagini registrate da videocamere (c.d. *vidéosurveillance algorithmique*). In particolare, l'articolo 10 della *Loi n° 2023-380* prevede che, in via sperimentale e fino al 31 marzo 2025, possono essere oggetto di trattamento algoritmico le immagini acquisite, conformemente al *Code de la sécurité intérieure* (Codice di sicurezza interna), mediante sistemi di videoregistrazione o di telecamere installate su aeromobili e raccolte all'interno nonché in prossimità dei luoghi che ospitano gli eventi olimpici, nei veicoli e nelle strutture di trasporto pubblico e sulle strade che li servono.
Tale impiego algoritmico delle immagini aumenta notevolmente la quantità e l'accuratezza delle informazioni che possono essere estratte da esse e tale analisi può essere impiegata per rilevare e segnalare determinati eventi o comportamenti. Si prenda l'ipotesi di una telecamera che registri la discesa e la salita di passeggeri in una stazione della metropolitana: il *software* di *vidéosurveillance algorithmique* analizza in tempo reale i movimenti delle persone all'arrivo del treno, così da segnalare l'eventuale persona che non compie il movimento statisticamente più diffuso e atteso. Su tale *vidéosurveillance algorithmique* si era pronunciata nel luglio del 2022 la *Commission nationale de l'informatique et des libertés* (CNIL), che, tra le altre cose, aveva rilevato come, per essere attuati legalmente, simili trattamenti richiedessero, in conformità all'art. 23 del GDPR e all'art. 34 della Costituzione francese, l'esistenza di un testo legislativo o regolamentare che li autorizzi. Non solo, più di recente e con una decisione tesa a vagliare proprio la costituzionalità della *Loi n° 2023-380*, era intervenuto anche il *Conseil Constitutionnel*, riconoscendo la legittimità del ricorso alla *vidéosurveillance algorithmique* per ragioni di pubblica sicurezza, nonché la necessità di garanzie per salvaguardare il diritto al rispetto della vita privata (2023-850 DC - 17 mai 2023).
Orbene, l'art. 10 della *Loi n° 2023-380* soddisfa tale necessità connessa al trattamento algoritmico delle immagini. Esso, innanzitutto, fissa gli obiettivi del ricorso alla *vidéosurveillance algorithmique*, ammettendola al solo scopo di garantire la sicurezza di eventi olimpici e paralimpici (sportivi, ricreativi o culturali) che, per l'entità della loro partecipazione o per le circostanze in cui si svolgono, sono particolarmente esposti al rischio di atti di terrorismo o di gravi minacce alla sicurezza personale. A tutela del pubblico, l'art. 10 della *Loi n° 2023-380* prevede, da un lato, che le persone partecipanti agli eventi olimpici siano preventivamente informate di tali trattamenti delle immagini raccolte (salvo che le circostanze lo vietino o che tale informazione sia in contrasto con gli obiettivi perseguiti) e, dall'altro, che questi non possano utilizzare sistemi di identificazione biometrica, elaborare dati biometrici o applicare tecniche di riconoscimento facciale. La medesima disposizione chiarisce che i trattamenti algoritmici delle immagini sono utilizzati esclusivamente per richiamare l'attenzione, limitandosi strettamente a indicare l'evento o gli eventi predeterminati che sono stati programmati per rilevare, senza poter produrre alcun altro risultato e neanche poter costituire, di per sé, la base per una decisione o azione giudiziaria individuale.
La *Loi n° 2023-380* afferma poi che il ricorso al trattamento algoritmico è autorizzato da un decreto emanato previa consultazione della *CNIL*, teso a fissarne le caratteristiche essenziali, come ad esempio l'indicazione eventi predeterminati che il trattamento ha lo scopo di segnalare. Lo sviluppo del trattamento così autorizzato deve avvenire in modo conforme ai requisiti previsti dalla *Loi n° 2023-380*, come quello che richiede che i dati di apprendimento, convalida e test scelti siano pertinenti, adeguati e rappresentativi. Nel caso in cui il trattamento sia sviluppato o fornito da un terzo, quest'ultimo deve fornire una documentazione tecnica completa e presentare garanzie di competenza, continuità, assistenza e controllo umano al fine, in particolare, di correggere eventuali errori o distorsioni durante la sua attuazione e di evitare che si ripetano. Per quanto riguarda gli eventi che si svolgeranno a Parigi, la *Loi n° 2023-380* individua nel *préfet de police* il soggetto deputato ad autorizzare l'utilizzo del trattamento algoritmico delle immagini, affermando che tale decisione, motivata e pubblicata, possa

esser concessa solo se l'uso del trattamento è proporzionato alla finalità prevista. Tale atto conterrà le specifiche relative all'evento, il luogo e la durata del trattamento.

DANIELE IMBRUGLIA

LOI n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions
Décision 2023-850 DC - 17 mai 2023
CNIL : Déploiement de caméras « augmentées » dans les espaces publics

2023/4(7)AF

7. Verso l'euro digitale: la decisione del Consiglio direttivo della BCE del 18.10.2023

Il 18 ottobre 2023 il Consiglio direttivo della Banca centrale europea (**BCE**) ha deciso di dare avvio alla fase successiva del progetto sull'euro digitale, anche più nota come fase di preparazione. La decisione fa seguito al termine della fase istruttoria, durata due anni e dedicata all'indagine dei possibili modelli di progettazione e distribuzione per un euro digitale (sulla decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto sull'euro digitale, v. in questa Rubrica la notizia n. 7 del numero 3/2021: http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf [2021/3(7)AF]). La BCE ha fornito una panoramica generale dei risultati ottenuti nella fase istruttoria circa una sua possibile configurazione.

L'euro digitale costituirebbe una forma digitale di contante. Come anche indicato dalla Proposta di regolamento relativo all'istituzione dell'euro digitale presentata dalla Commissione europea il 28 giugno 2023 (sulla quale v., in questa Rubrica, la notizia n.2 del numero 2/2023: http://www.personaemercato.it/wp-content/uploads/2023/08/Osservatorio.pdf [2023/2(2)AF]), all'euro digitale sarebbe attribuito corso legale: ciò comporterebbe un obbligo di accettazione dello stesso nei pagamenti, al pari del contante. Gli utenti potrebbero così regolare all'istante i pagamenti in moneta di banca centrale, avvalendosi di ampie possibilità di uso che ad oggi non sono offerte simultaneamente da nessun altro strumento di pagamento digitale. In particolare, gli utenti potrebbero utilizzare l'euro digitale per i pagamenti da persona a persona, presso i punti vendita, nel commercio elettronico e nelle operazioni con le amministrazioni pubbliche.

L'euro digitale sarebbe ampiamente accessibile agli utenti attraverso la distribuzione da parte di prestatori di servizi di pagamento conformi ai requisiti delineati dalla direttiva (UE) 2015/2366 (c.d. Payment Services Directive 2 anche nota come PSD2). Non occorrerà detenere un conto bancario per accedere all'euro digitale. Gli utenti potranno accedervi via un app dell'Eurosistema o per mezzo dell'interfaccia online del proprio prestatore di servizi di pagamento. Per assicurare l'inclusione finanziaria, gli utenti avranno anche la possibilità di richiedere una carta di pagamento in euro digitale.

Responsabili della relazione con gli utenti sarebbero i prestatori di servizi di pagamento, non l'Eurosistema. Ciò nonostante, l'euro digitale costituirebbe comunque una passività dell'Eurosistema. I prestatori di servizi di pagamento offrirebbero gratuitamente agli individui i servizi di base, così come indicati nella proposta legislativa e nello schema per l'euro digitale. In particolare, le funzionalità di base ricomprenderebbero i servizi di user management, concernenti la relazione con l'utente e l'accesso all'euro digitale; i servizi di liquidity management, relativi alla gestione della liquidità delle disponibilità in euro digitale tramite, ad esempio, versamenti e prelievi; e, infine, i servizi di transaction management, legati alla gestione e all'esecuzione delle transazioni in euro digitale. L'Eurosistema supporterebbe i prestatori di servizi di pagamento provvedendo all'infrastruttura per un euro digitale, in particolare per quanto riguarda le modalità di regolamento delle transazioni online e la ideazione di soluzioni per la distribuzione offline.

Come più volte sottolineato nella fase istruttoria, l'euro digitale potrebbe porre rischi per la stabilità finanziaria e per la trasmissione della politica monetaria, considerato l'elevato grado di sostituibilità con i depositi bancari. Per tale ragione sarebbero previste delle misure di salvaguardia volte ad assicurare un equilibrio adeguato tra l'euro digitale, come moneta di banca centrale, e i depositi bancari. In particolare, sarebbero previsti limiti all'ammontare di euro digitale che gli utenti possono detenere. Nessun limite legato a considerazioni di stabilità finanziaria, invece, sarebbe previsto per le transazioni in euro digitale che gli utenti possono effettuare. Inoltre, le disponibilità in euro digitale non sarebbero remunerate, così che gli utenti percepiscano l'euro digitale come complemento al contante e non anche come riserva di valore.

Da ultimo, l'euro digitale garantirebbe gli standard più elevati di riservatezza: l'Eurosistema non sarebbe in grado di accedere ai dati personali degli utenti e le informazioni sui pagamenti non

sarebbero riconducibili a singoli individui. Se utilizzato offline, l'euro digitale offrirebbe inoltre un livello di privacy paragonabile a quello del contante.
La fase di preparazione costruirà le fondamenta per un eventuale euro digitale così come configurato sulla base dei risultati ottenuti nella fase istruttoria. La fase di preparazione avrà una durata iniziale di due anni e vedrà l'esecuzione di test e sperimentazioni volti ad assicurare che le caratteristiche dell'euro digitale rispondano alle esigenze dell'Eurosistema e degli utenti. In particolare, la fase di preparazione riguarderà sia la selezione dei fornitori per lo sviluppo della piattaforma e delle infrastrutture, sia la elaborazione di un manuale di norme relativo all schema per l'euro digitale. Per quanto riguarda quest'ultimo, l'Eurosistema ha già istituito durante la fase istruttoria il Rulebook Development Group, composto da esperti dell'Eurosistema ed esponenti del mercato, con il compito di coadiuvare l'elaborazione di un corpus unico di regole, prassi e standard per l'euro digitale. In particolare, la funzione del rulebook sarà quella di specificare con procedure e standard tecnici le norme di alto livello contenute nella proposta di regolamento. Una prima versione del rulebook è stata già redatta. In particolare, la prima versione prevede regole aventi ad oggetto i modelli funzionali e operativi su cui si baserà l'euro digitale, dando una panoramica dei servizi di base di access management, liquidity management e transaction management.
L'avvio della fase di preparazione non implica una decisione in merito all'emissione di un euro digitale. Tale decisione sarà presa eventualmente in considerazione dal Consiglio direttivo della BCE una volta completato l'iter legislativo.

ALICE FILIPPETTA

A stocktake on the digital euro - Summary report on the investigation phase and outlook on the next phase
Update on the work of the digital euro scheme's Rulebook Development Group

2023/4(8)CAT

8. Verso il Regolamento UE sullo spazio europeo dei dati sanitari: le basi giuridiche per il *secondary use* di dati personali sanitari

Il 7 e il 13 dicembre 2023, rispettivamente, il Consiglio UE (**Consiglio**) e il Parlamento europeo (**PE**), in vista delle imminenti negoziazioni secondo la procedura legislativa ordinaria, hanno adottato separate modifiche alla proposta della Commissione europea COM(2022) 197 final del 3 maggio 2022, avente ad oggetto il regolamento sullo "European Health Data Space" (EHDS), lo "Spazio Europeo dei Dati Sanitari" (rispettivamente: il "**Testo rivisto di compromesso del Consiglio**", gli "**Emendamenti del PE**", la "**Proposta**" e il "**Regolamento EHDS**").
Il Regolamento EHDS si incardina come parte della *data strategy* europea, il cui obiettivo finale è rendere l'Unione europea leader nell'ambito della *data-driven society*: in continuità con il regolamento (UE) 2022/868, c.d. Data Governance Act (**DGA**), che si propone di disciplinare le basi fondative di un sistema di circolazione dei dati basato sulla fiducia, in particolare disciplinando il riutilizzo dei dati "protetti" delle pubbliche amministrazioni e i cd. "servizi di intermediazione dei dati" (sul DGA v., in questa Rubrica la notizia n. 1 del numero 2/2022: http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf [2022/2(1)RA]), la Proposta mira a istituire uno spazio europeo dei dati sanitari sicuro e interconnesso.
Secondo la Proposta, il Regolamento EHDS sarà strutturato in modo da prevedere: (1) un maggiore accesso e controllo dei dati sanitari personali delle singole persone; (2) il sostegno a un mercato unico riguardante sistemi elettronici di cartelle cliniche e dispositivi medici; (3) un utilizzo coerente, affidabile ed efficiente dei dati sanitari a fini di ricerca, innovazione, elaborazione delle politiche e attività normative, nell'ambito del c.d. "uso secondario dei dati", uno dei temi più rilevanti del corpo normativo.
Il *secondary use* consiste nell'elaborazione dei dati (sanitari) per scopi diversi da quelli iniziali per cui sono stati raccolti. Il capitolo IV del Regolamento EHDS dovrà stabilire le regole applicabili all'"uso secondario" dei dati sanitari elettronici.
È previsto che i "detentori dei dati" (o "detentori dei dati sanitari": l'espressione e la relativa definizione mutano nei diversi testi), come meglio definiti all'art. 2, debbano rendere disponibili una vasta gamma di categorie specifiche di dati sanitari elettronici (a titolo esemplificativo e non esaustivo, si pensi ai dati contenuti nelle cartelle cliniche elettroniche oppure a quelli provenienti da studi clinici o da dispositivi medici) per un uso secondario da parte di terzi, denominati "utenti dei dati".
In particolare, la Proposta specifica che i dati sanitari elettronici "*che comportano proprietà intellettuale protetta e segreti commerciali da*

imprese private devono essere resi disponibili per l'uso secondario", anche se in tali casi la Proposta prevede (alquanto genericamente) che devono essere adottate "*tutte le misure necessarie per preservare la riservatezza dei diritti di proprietà intellettuale e dei segreti commerciali*" (Art. 33(4)). Il testo degli Emendamenti del PE elimina tale previsione e propone l'emendamento 315, contenente un intero nuovo articolo dedicato alla questione, che contempla una procedura articolata e specifica, con organismi ad hoc e accordi specifici. Anche il Testo rivisto di compromesso del Consiglio prevede un nuovo articolo ad hoc con disposizioni intese a tutelare le informazioni protette da proprietà intellettuale e/o segreti commerciali.

Per accedere ai dati per un uso secondario, qualsiasi persona fisica o giuridica può presentare una domanda di accesso ai dati all'ente di accesso ai dati sanitari per gli scopi indicati all'articolo 34 (Art. 45(1) della Proposta). Una disposizione sostanzialmente equivalente si legge nel Testo rivisto di compromesso del Consiglio. Invece, nel testo degli Emendamenti del PE è previsto che chi fa la domanda di accesso possa essere qualsiasi persona fisica o giuridica "*con un collegamento professionale dimostrabile all'area della sanità, della salute pubblica o della ricerca medica*". Tra gli scopi indicati dall'art. 34 della Proposta, vi sono la ricerca scientifica correlata ai settori della salute o dell'assistenza, le attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla salute pubblica o alla sicurezza sociale, o garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei prodotti medicinali o dei dispositivi medici e formazione, test e valutazione di algoritmi, compresi quelli dei dispositivi medici, sistemi di intelligenza artificiale e applicazioni di salute digitale, che contribuiscono alla salute pubblica o alla sicurezza sociale, o garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei prodotti medicinali o dei dispositivi medici (Art. 34(1)(e)-(g)) Si tratta di previsioni sostanzialmente confermate (sia pure con specificazioni) anche nei richiamati testi del Consiglio e del PE.

Punto di discussione è rappresentato dall'individuazione della base giuridica fondante il trattamento dei dati sanitari per un uso secondario. Tale questione è affrontata nel Considerando 37, che differisce nei tre testi (Proposta, Testo rivisto di compromesso del Consiglio, e testo degli Emendamenti del PE). Nel testo della Proposta si trova affermato che il regolamento "*fornisce la base giuridica in conformità dell'articolo 9, paragrafo 2, lettere g), h), i) e j), del GDPR per l'uso secondario dei dati sanitari, stabilendo le garanzie per il trattamento, in termini di finalità legittime, una governance affidabile per fornire l'accesso ai dati sanitari (attraverso organismi responsabili dell'accesso ai dati sanitari) e il trattamento in un ambiente sicuro, nonché modalità per il trattamento dei dati, stabilite nell'autorizzazione ai dati. Al tempo stesso il richiedente dovrebbe dimostrare una base giuridica, ai sensi dell'articolo 6 del regolamento (UE) 2016/679, che gli consenta di richiedere l'accesso ai dati a norma del presente regolamento e dovrebbe soddisfare le condizioni stabilite nel capo IV. Più precisamente, per il trattamento di dati sanitari elettronici detenuti dal titolare dei dati a norma del presente regolamento, quest'ultimo introduce l'obbligo giuridico, ai sensi dell'articolo 6, paragrafo 1, lettera c), del regolamento (UE) 2016/679, secondo cui il titolare dei dati è tenuto a comunicare i dati agli organismi responsabili dell'accesso ai dati sanitari, mentre la base giuridica per la finalità del trattamento iniziale (ad es. la prestazione di assistenza) è inalterata.*". Inoltre, è previsto che tale processo sarà consentito tramite autorizzazioni rilasciate da un organismo responsabile dell'accesso ai dati in ambienti sicuri di trattamento, che vi provvederà, in particolare, attraverso l'applicazione di meccanismi di anonimizzazione.

Quindi la Proposta menziona tra le basi giuridiche per l'uso secondario: pubblico interesse, medicina preventiva, o ricerca scientifica, lasciando invece poco spazio al consenso dell'interessato.

Il rapporto congiunto del 28.11.2023 della Commissione del PE per l'ambiente, la sanità pubblica e la sicurezza alimentare (ENVI) e della Commissione del PE per le libertà civili, la giustizia e gli affari interni (LIBE) ha identificato questa mancanza e ha proposto un emendamento al testo della Proposta: al fine di rafforzare il controllo dei propri dati da parte degli interessati, l'emendamento propone che abbiano la possibilità di fare opt-out nel caso di uso secondario di dati personali (https://www.europarl.europa.eu/legislative-train/theme-promoting-our-european-way-of-life/file-european-health-data-space). Tuttavia, secondo European Digital Rights (EDRi), l'opt-out porrebbe indebitamente l'onere della conoscenza, comprensione e decisione di tale trattamento ulteriore sulle persone assistite, le quali si troverebbero a doversi eventualmente opporre in un secondo momento. In tal senso, il Position Paper di EDRi (https://edri.org/wp-content/uploads/2023/03/EHDS-EDRi-position-final.pdf) si spinge oltre, proponendo che si dia la possibilità di fare opt-in anziché opt-out e, dunque, che per tali trattamenti sia necessaria la previa

espressione di volontà delle persone interessate. Si comprende dunque come l'interazione tra il GDPR e l'EHDS sia ancora una volta una questione non del tutto risolta dal testo normativo. Infatti, la Proposta non sembra creare una base giuridica ai sensi del GDPR, in quanto, piuttosto, gli utenti dei dati hanno la responsabilità di identificare tale base giuridica ai sensi della legislazione dell'UE o degli Stati membri. Attualmente nell'UE, i diversi Stati membri – a ciò autorizzati ai sensi dell'art. 9(4) GDPR - adottano approcci diversi per quanto riguarda la necessità di ottenere il consenso dei pazienti per l'utilizzo dei dati a fini di ricerca (art. 9(2)(a) GDPR) o la possibilità per le organizzazioni di avvalersi dell'esenzione dalla ricerca di cui agli artt. 9(2)(j) e 89(1) GDPR. In tal senso, la Proposta non appare risolutiva nel senso di armonizzare le differenti impostazioni sull'annosa questione della base giuridica. Questo sembra essere stato il motivo dell'integrazione al Considerando 37 che si legge nel Testo rivisto di compromesso del Consiglio, a tenore del quale: "*[…] gli Stati membri non possono mantenere o introdurre ai sensi dell'articolo 9(4) del [GDPR] ulteriori condizioni, incluse limitazioni e specifiche previsioni che rendono necessario il consenso delle persone fisiche con riferimento al trattamento per uso secondario dei dati personali sanitari in virtù di questo Regolamento*". Nel testo degli Emendamenti del PE è stato infine introdotto un Considerando separato (emendamento 39) ed alcune modifiche agli articoli (emendamenti 311 e 312) nel senso di prevedere un doppio meccanismo, tale per cui ai pazienti interessati è sempre generalmente consentito l'opt-out, mentre l'opt-in è necessario per alcuni categorie di dati i quali, vuoi per la loro natura di dati particolarmente sensibili (è il caso dei "*human genetic, genomic and proteomic data*" e dei dati "*from biobanks*") o per la particolare natura della loro utilizzazione tipica (è il caso dei dati derivanti dalle applicazioni "*wellness*") rendono opportuno prevedere che il loro uso secondario possa avvenire soltanto dopo il consenso della persona fisica interessata ai sensi dell'art. 4(11) del GDPR. Evidentemente la questione della base giuridica dovrà essere risolta in modo concordato nel testo finale del Regolamento EHDS, che si attende per l'anno in corso.

CARMINE ANDREA TROVATO

Proposta della Commissione del 3.5.2022:
https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2022/0197/COM_COM(2022)0197_EN.pdf

Testo rivisto di compromesso del Consiglio del 7.12.2023:
https://data.consilium.europa.eu/doc/document/ST-16048-2023-REV-1/en/pdf

Emendamenti del PE del 13.12.2023:
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0462_IT.pdf

2023/4(9)LC

9. Le considerazioni dell'OMS del 19.10.2023 sugli aspetti regolatori della IA nel settore della salute

L'Organizzazione Mondiale della Sanità (di seguito, **OMS**, WHO in inglese) ha pubblicato il 19 ottobre 2023 un documento contenente alcune considerazioni sugli aspetti regolatori dell'intelligenza artificiale nel settore della salute: *Regulatory considerations on artificial intelligence for health*. Tale documento si inserisce nella *strategia globale sulla salute digitale 2020-2025* portata avanti dall'OMS e sottolinea l'importanza di stabilire regole certe sulla sicurezza e l'efficacia dei sistemi di intelligenza artificiale, per renderli rapidamente disponibili, purché adeguati ai principi etici che informano il settore e al rispetto della privacy, promuovendo il dialogo tra tutte le parti interessate, inclusi sviluppatori, produttori, tutti gli *stakeholders in medical devices ecosystems*, oltre al coinvolgimento di operatori sanitari e pazienti stessi.
Con la crescente disponibilità di dati sanitari e il rapido progresso delle tecniche analitiche – siano esse di apprendimento automatico (*machine learning*), basate sulla logica (*logic-based*) o statistiche (*statistical*) – i sistemi di intelligenza artificiale potrebbero rivoluzionare il settore sanitario. Un simile potenziale di implementazione dell'intero comparto è espressamente riconosciuto dall'OMS, laddove afferma che: «WHO […] recognizes the potential of Artificial Intelligence (AI) in accelerating the digital transformation of health care». Grazie ai sistemi di intelligenza artificiale sarà possibile, ad esempio, rafforzare i risultati sanitari e gli studi clinici; migliorare la diagnosi medica, il trattamento, la cura e l'assistenza incentrate sulla persona; integrare le conoscenze, le abilità e le competenze degli operatori sanitari. Inoltre, tali sistemi potrebbero essere utili in contesti in cui mancano specialisti, come nell'interpretazione delle scansioni retiniche e delle immagini radiologiche.

E tuttavia, tali tecnologie vengono così rapidamente implementate che talvolta difetta una piena e reale comprensione del loro funzionamento, il che potrebbe condurre ad esiti indesiderati e, in ultima analisi, danneggiare gli utenti finali, compresi i pazienti. Quando i sistemi di intelligenza artificiale hanno accesso a dati sanitari e informazioni personali sensibili occorrerebbero solidi *frameworks* normativi per salvaguardare la privacy, la sicurezza e l'integrità della persona soggetta a trattamento.

Nel documento in commento, infatti, viene, sottolineato fin dalla premessa che «[t]his document provides an overview of regulatory considerations on AI for health that covers key general topic areas, namely: documentation and transparency, risk management and AI systems development lifecycle approach, intended use and analytical and clinical validation, AI related data quality, privacy and protection, and engagement and collaboration»; punti che, come vedremo, ne riflettono la relativa struttura.

A margine di questa pubblicazione, lo stesso direttore generale dell'OMS, Dr. Tedros Adhanom Ghebreyesus, ha affermato che «[a]rtificial intelligence holds great promise for health, but also comes with serious challenges, including unethical data collection, cybersecurity threats and amplifying biases or misinformation». Ed ha aggiunto: «[t]his new guidance will support countries to regulate AI effectively, to harness its potential, whether in treating cancer or detecting tuberculosis, while minimizing the risks».

In risposta alla crescente esigenza dei Paesi di gestire in modo responsabile la rapida ascesa delle tecnologie sanitarie basate sull'intelligenza artificiale, questo documento delinea, dunque, le seguenti sei *topic areas of regulatory considerations* cui attingere per il consolidamento di *frameworks* normativi e lo sviluppo di *best practices* in questo settore: ***i.*** *documentation and transparency*, per promuovere la fiducia; ***ii.*** *risk management and artificial intelligence systems development lifecycle approach*, per gestire i possibili rischi durante tutto l'arco di vita dei sistemi; ***iii.*** *intended use and analytical and clinical validation*, per garantire la sicurezza e facilitare la regolamentazione; ***iv.*** *data quality*, per evitare *bias* ed errori; *v. privacy and data protection*, per garantire la *compliance* ai plessi normativi esistenti; *vi. engagement and collaboration*, per accelerare i processi di implementazione e di miglioramento dei sistemi.

Queste sei aree riflettono la complessità dei sistemi di intelligenza artificiale, che discende non solo, *ex ante*, dalla progettazione del codice con cui vengono costruiti, ma anche dai dati con cui, *ex post*, vengono addestrati. In considerazione di queste diverse fasi, una migliore regolamentazione può aiutare a gestire i rischi che l'intelligenza artificiale è potenzialmente in grado di amplificare e questa nuova risorsa messa a disposizione dall'OMS è volta a individuare i principi chiave cui i governi e le autorità di regolamentazione possono ispirarsi per sviluppare nuove linee guida, politiche legislative e prassi adattive, a livello nazionale o regionale. In quest'ottica, il contributo si chiude con un'utile appendice contenente un glossario delle più importanti definizioni e dei concetti fondamentali dell'AI applicata all'*healthcare*.

LUCIO CASALINI

https://iris.who.int/bitstream/handle/10665/373421/9789240078871-eng.pdf

2023/4(10)SB

10. Le linee guida 2/2023 dello EDPB sull'art. 5(3) della direttiva ePrivacy sottoposte a consultazione pubblica

Il 14 novembre 2023 l'EDPB – European Data Protection Board ha pubblicato la versione provvisoria delle linee guida 2/2023 sull'ambito tecnico di applicazione dell'art. 5(3) della direttiva e-privacy ("**ePD**"), cioè la Direttiva 2002/58/CE "*relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)*" come da ultimo modificata dalla Direttiva 2009/136/CE. La ePD è stata recepita nell'ordinamento italiano nell'ambito del Codice in materia di protezione dei dati personali di cui al d.lgs. 196 del 2003 (il "**Codice privacy**"), e il paragrafo 3 dell'articolo 5 in esame ha trovato collocazione nell'art. 122 del Codice privacy. La bozza delle linee guida è stata sottoposta a pubblica consultazione, che si è chiusa il 18 gennaio 2024.

L'art. 5 ePD tutela la riservatezza "*delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico*", e il par. 3 dispone che "*l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo ... tra l'altro sugli scopi del trattamento*".

L'archiviazione/memorizzazione o l'accesso a tali informazioni senza consenso è ammissibile solo in due casi: "*al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio*".
L'articolo si prefigge, quindi, di tutelare la riservatezza delle informazioni raccolte tramite una tecnica di tracciamento delle informazioni stesse.
Le linee guida non si caratterizzano per il loro carattere innovativo ma, è bene ricordarlo, non è questo il loro obiettivo; lo scopo perseguito dall'EDPB nel pubblicare le linee guida è stato piuttosto quello di (cercare di) fugare ogni dubbio circa la portata dell'art. 5(3) eDP e la sua applicazione anche alle nuove modalità tecniche di tracciamento delle informazioni.
Non è la prima volta che le autorità europee avvertono l'esigenza di prendere posizione sulle modalità tecniche di accesso alle informazioni e alla loro archiviazione. Già all'epoca del WP29 - Working Party 29 (il gruppo di lavoro consultivo, istituito dall'art. 29 – da qui il nome dell'organo – dell'allora direttiva 95/46/CE, composto dai rappresentanti delle autorità degli Stati membri per la tutela dei dati personali, e oggi sostituito dall'EDPB) erano stati emessi due pareri relativi all'applicazione dell'art. 5 in esame: l'*opinion* 4/2012 sul consenso al trattamento dei dati tramite i c.d. *cookies*, e l'*opinion* 9/2014 sulle tecnologie di trattamento dei dati attraverso tecnologie di rilevamento delle impronte digitali (c.d. *fingerprinting*).
L'evoluzione delle tecnologie relative alla raccolta/accesso ai dati personali di un utente o abbonato e alla loro archiviazione hanno indotto l'EDPB ad emettere le linee guida al fine di chiarire che anche le nuove tecniche di tracciamento delle informazioni ricadono nell'ambito di applicazione dell'articolo in questione, ciò al superiore fine di evitare che attraverso tali nuove modalità di tracciamento possa essere eluso l'obbligo di raccolta del consenso.
Le linee guida sono strutturate a due livelli. Da un lato, una parte generale in cui l'EDPB richiama i principi consolidati sulla nozione e interpretazione di "informazioni", "archiviazione/memorizzazione", "accesso" ad informazioni già archiviate, "apparecchiatura terminale" di un utente o abbonato e di "trasmissione di una comunicazione" su una rete di comunicazione elettronica; dall'altro lato, vengono presi in esame, senza pretesa di completezza, specifiche modalità tecniche di tracciamento, che, secondo l'EDPB, rientrano nell'ambito di applicazione del detto par. 3.
Circa la parte generale, le linee guida riprendono nozioni già ampiamente note, vuoi perché di matrice normativa, vuoi perché nozioni di derivazione giurisprudenziale o già oggetto di disamina nell'ambito delle linee guida emesse all'epoca dei lavori del WP29.
E così, quanto alla nozione di apparecchiatura o dispositivo terminale, o a quella di comunicazione elettronica, le linee guida rinviano, rispettivamente, alla Direttiva 2008/63/CE "*relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni*" (ed il cui art. 1(1) detta la definizione di apparecchiatura terminale) e alla Direttiva (UE) 2018/1972, c.d. Codice europeo delle comunicazioni elettroniche, il cui art. 2(1) definisce le reti di comunicazione elettronica e le relative comunicazioni.
Quanto alla nozione di "informazioni", le linee guida ricordano che essa ha una portata più ampia rispetto a quella di "dato personale", ciò alla luce del Considerando 24 della ePD, dell'art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea e dell'interpretazione fornita dalla CGUE nel caso Planet 49. la CGUE ha, infatti, sottolineato come la tutela accordata dall'art. 5 eDP "*… si applica a qualsiasi informazione archiviata in tale apparecchiatura terminale, indipendentemente dal fatto che si tratti o meno di dati personali ed è volta, in particolare … a tutelare gli utenti dal rischio che identificatori occulti o altri dispositivi analoghi si introducano nell'apparecchiatura terminale dell'utente a sua insaputa*" (così, CGUE, 1 ottobre 2019, *Planet 49*, C-673/17, par. 70).
Per ciò che riguarda l'accesso e l'archiviazione/memorizzazione delle informazioni, le linee guida riprendono quanto già stabilito all'epoca dell'adozione dell'Opinion WP29 9/2014, riaffermando che, per l'applicabilità dell'art. 5(3) ePD, non è necessario che l'archiviazione/memorizzazione e l'accesso alle informazioni siano cumulativamente presenti. La tutela è accordata anche in caso di una sola delle dette attività e, quindi, si avrà applicazione dell'art. 5(3) ePD, sia quando si sia in presenza della sola attività di memorizzazione di dati sul dispositivo terminale dell'utente o dell'abbonato (come ad es. tramite i c.d. *cookies*), sia quando vi sia unicamente l'accesso (o, per essere più precisi, il tentativo di accesso) al dispositivo finale dell'utente o dell'abbonato.
Per ciò che concerne l'analisi di alcune specifiche modalità tecniche di tracciamento delle informazioni, le linee guida si soffermano sull'esame dell' *URL pixel tracking*, del *local*

processing, sul tracciamento basato solo su IP (*tracking based on IP only*), sulla segnalazione intermittente e mediata da parte di dispositivi IoT (*Internet of Things*), sui sistemi di tracciamento e rilevamento delle informazioni tramite identificatore unico (*unique identifier*), per concludere che anche tali mezzi di tracciamento rientrano in linea di principio nell'ambito di applicazione dell'art. 5(3) eDP.
Per quanto riguarda in particolare i dispositivi IoT (interessati anche dal Data Act: v. *supra* prima notizia in questo numero della Rubrica [2023/4(1)SO]), viene specificato che essi devono essere considerati quali apparecchiature terminali quando sono connessi ad una rete pubblica di comunicazione, mentre quando sono collegati alla rete attraverso un altro dispositivo che opera la ritrasmissione (*relay device*) - es. smartphone, hub dedicato etc. – quest'ultimo sarà considerato l' apparecchiatura terminale ai sensi dell'art. 5(3) eDP, con la conseguenza che le informazioni ricevute dal *relay device* saranno considerate archiviate da un'apparecchiatura terminale e l'art. 5(3) ePD si applicherà non appena a questo dispositivo di ritrasmissione sarà data l'istruzione di inviare l'informazione ad un server remoto.

STEFANO BARTOLI

https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en

2023/4(11)SO-SM

11. La Commissione mette online la banca dati prevista dal DSA sulla moderazione dei contenuti (*DSA Transparency Database*) e una banca dati sulle condizioni d'uso delle piattaforme e dei servizi online (*Digital Services and Conditions Database*)

Il regolamento (UE) 2022/2065 (**DSA**) ha previsto, *inter alia*, che la Commissione europea (la **Commissione**) debba istituire e rendere pubblica una banca dati sulla moderazione dei contenuti, l'altra sulle condizioni di uso delle piattaforme e servizi online.
La motivazione si trova nel Considerando 66 DSA: "Al fine di garantire la trasparenza, di consentire il controllo delle decisioni relative alla moderazione dei contenuti dei fornitori di piattaforme online e di monitorare la diffusione di contenuti illegali online, la Commissione dovrebbe mantenere e pubblicare una banca dati contenente le decisioni e le motivazioni dei fornitori di piattaforme online quando rimuovono le informazioni o limitano in altro modo la loro disponibilità e l'accesso alle stesse. Al fine di mantenere costantemente aggiornata la banca dati, i fornitori di piattaforme online dovrebbero presentare, in un formato standard, le decisioni e le motivazioni senza indebito ritardo dopo l'adozione di una decisione, al fine di consentire aggiornamenti in tempo reale se tecnicamente possibile e proporzionato ai mezzi della piattaforma online in questione. La banca dati strutturata dovrebbe consentire l'accesso alle informazioni pertinenti e l'estrazione di tali informazioni, in particolare per quanto riguarda il tipo di presunto contenuto illegale di cui trattasi".
L'art. 24(5)DSA prevede quindi che i fornitori di piattaforme online debbano fornire alla Commissione, senza indebito ritardo, le decisioni e le motivazioni di cui all'art. 17(1) DSA per l'inserimento in una banca dati leggibile meccanicamente e disponibile al pubblico gestita dalla Commissione. L'art. 24(5)DSA aggiunge che i fornitori di piattaforme online debbano provvedere affinché le informazioni trasmesse non contengano dati personali.
Le motivazioni di cui all'art. 17(1) DSA sono quelle che i prestatori di servizi di memorizzazione di informazioni devono fornire a tutti i destinatari del servizio interessati in modo chiaro e specifico per far comprendere per quali ragioni le informazioni da essi fornite costituirebbero contenuti illegali o sarebbero incompatibili con le proprie condizioni generali, e dunque per giustificare l'adozione di una delle seguenti restrizioni del servizio: a) eventuali restrizioni alla visibilità di informazioni specifiche fornite dal destinatario del servizio, comprese la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione dei contenuti; b) la sospensione, la cessazione o altra limitazione dei pagamenti in denaro; c) la sospensione o la cessazione totale o parziale della prestazione del servizio; d) la sospensione o la chiusura dell'account del destinatario del servizio.
La Commissione ha dunque istituito e messo online il **DSA Transparency Database** (https://transparency.dsa.ec.europa.eu/) contenente le informazioni da essa ricevute relative alle decisioni sulla moderazione dei contenuti delle piattaforme online.
Particolarmente interessanti sono le statistiche che si trovano nella prima pagina web del DSA Transparency Database, dove **alla data del 17.2.2024** si trovavano pubblicati questi dati:

- **quasi 4 miliardi e mezzo di motivazioni** (*statements of reasons*) fornite alla Commissione (4.485.574.690);
- **percentuale di decisioni totalmente automatizzate: 73%**;
- numero di piattaforme attive: 16;
- violazioni contestate con maggiore frequenza: (1) ambito del servizio di piattaforma [*scope of platform service*]; (2) linguaggio illegale o dannoso [*illegal or harmful speech*]; (3) prodotti non sicuri e/o illegali;
- restrizioni maggiormente applicate: (1) disabilitazione dell'accesso ai contenuti; (2) rimozione di contenuti; (3) altre.

Successivamente al lancio della DSA Transparency Database, la Commissione ha assunto l'iniziativa di creare e pubblicare online una banca dati sulle condizioni contrattuali dei servizi digitali: **il Digital Services Terms and Conditions Database** (https://platform-contracts.digital-strategy.ec.europa.eu/).

Questa banca dati fa dichiaratamente leva su alcune disposizioni del DSA e del **Regolamento P2B** [regolamento (UE) 2019/1150 sull'equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online], in particolare sugli obblighi dei prestatori di servizi intermediari di rendere i propri contratti disponibili in un formato facilmente accessibile e leggibile da una macchina (art. 14 DSA) e sugli obblighi di pubblicare contratti chiari e completi previsti sia per gli utenti professionali (art. 3 Regolamento P2B) sia per gli utenti finali (art. 14 DSA). Indicizzando automaticamente i contratti, il database offre la possibilità di facilitare analisi ed approfondimenti sulle clausole dei contratti aventi ad oggetto servizi digitali.

Il database utilizza un software open source sviluppato da **Open Terms Archive**, un'iniziativa francese sotto il patrocinio politico dell'ambasciatore francese per gli affari digitali (https://opentermsarchive.org/about), con il sostegno del programma **Next-Generation Internet** della Commissione (https://www.ngi.eu/).

SALVATORE ORLANDO / SERENA MIRABELLO

https://transparency.dsa.ec.europa.eu/

https://platform-contracts.digital-strategy.ec.europa.eu/

2023/4(12)RA

12. La nomina di tre nuovi VLOPs ai sensi del DSA

Lo scorso 20 dicembre 2023, la Commissione europea (la **Commissione**)ha designato un secondo gruppo di piattaforme online di dimensioni molto grandi (o VLOPs) ai sensi del regolamento (UE) 2022/2065 (**DSA**), includendovi i siti *Pornhub*, *Stripchat* e *XVideos* (per quanto riguarda la designazione del primo gruppo di piattaforme, v. in questa Rubrica notizia n. 5 nel numero 2/2023: http://www.personaemercato.it/wp-content/uploads/2023/08/Osservatorio.pdf [2023/2(5)RA]).

La designazione quali VLOPs è il risultato di indagini, portate avanti dalla Commissione, dalle quali è emerso che i tre siti superano la soglia dei 45 milioni di utenti medi mensili nell'UE prevista all'art. 33(1) DSA.

A carico dei soggetti così designati troveranno ora applicazione – oltre agli obblighi previsti, in generale, dal Capo III del DSA – gli "*obblighi supplementari*" stabiliti dalla Sezione 5 del Capo III del DSA, la quale prevede, tra l'altro, che:

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

DSA). Ove la revisione risulti non positiva, i fornitori di VLOPs "*tengono debitamente conto delle raccomandazioni operative ad essi rivolte al fine di adottare le misure necessarie per attuarle*" (art. 37(6) DSA);

- i fornitori di piattaforme *online* di dimensioni molto grandi devono assicurare "*almeno un'opzione per ciascuno dei loro sistemi di raccomandazione, non basata sulla profilazione come definita nell'articolo 4, punto 4), del regolamento (UE) 2016/679*" (art. 38 DSA);
- tali soggetti "*compilano e rendono accessibile al pubblico in una specifica sezione della loro interfaccia online, mediante uno strumento consultabile e affidabile che consente ricerche attraverso molteplici criteri e attraverso le interfacce di programmazione delle applicazioni, un registro contenente* [talune] *informazioni* [relative alla pubblicità effettuata], *per l'intero periodo durante il quale presentano pubblicità e fino a un anno dopo la data dell'ultima presentazione dell'annuncio pubblicitario sulle loro interfacce online*" (art. 39 DSA);
- i fornitori di VLOPs "*forniscono al coordinatore dei servizi digitali del luogo di stabilimento o alla Commissione, su loro richiesta motivata ed entro un termine ragionevole specificato in detta richiesta, l'accesso ai dati necessari per monitorare e valutare la conformità al presente regolamento*", al fine di adottare eventuali provvedimenti a ciò finalizzati (art. 40(1) DSA);
- tali soggetti devono istituire "*una funzione di controllo della conformità indipendente dalle loro funzioni operative*" volta a: "*a) collaborare con il coordinatore dei servizi digitali del luogo di stabilimento e con la Commissione ai fini del presente regolamento; b) assicurare che tutti i rischi di cui all'articolo 34 siano identificati e adeguatamente segnalati e che siano adottate misure di attenuazione dei rischi ragionevoli, proporzionate ed efficaci a norma dell'articolo 35; c) organizzare e sovrintendere alle attività del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi relative alle revisioni indipendenti a norma dell'articolo 37; d) informare e consigliare i dirigenti e i dipendenti del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi in merito ai pertinenti obblighi a norma del presente regolamento; e) monitorare la conformità del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi agli obblighi derivanti dal presente regolamento; f) se del caso, monitorare la conformità del fornitore della piattaforma online di dimensioni molto grandi o del motore di ricerca online di dimensioni molto grandi agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 o dei protocolli di crisi di cui all'articolo 48*" (art. 41(1) e (3) DSA);
- la "*Commissione addebita ai fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi un contributo annuale per le attività di vigilanza al momento della loro designazione a norma dell'articolo 33*" (art. 43(1) DSA).

Pornhub, *Stripchat* e *XVideos* dovranno dunque adeguarsi alle disposizioni poc'anzi illustrate al fine di garantire la conformità al DSA. Il rispetto di tali disposizioni dovrebbe garantire una moderazione dei contenuti più diligente, una migliore protezione dei minori e degli altri soggetti particolarmente vulnerabili, nonché una maggiore trasparenza dei servizi offerti sul *web*.

RICCARDO ALFONSI

https://ec.europa.eu/commission/presscorner/detail/it/ip_23_6763

2023/4(13)SO-RA

13. I ricorsi di ByteDance, Meta ed Apple contro le designazioni di gatekeeper ai sensi del DMA e l'ordinanza del 9.2.2024 relativa al ricorso di ByteDance

Il 16.11.2023 la società ByteDance Ltd. (**ByteDance**) – che gestisce la piattaforma TikTok – ha presentato un ricorso davanti al Tribunale dell'UE (organo della CGUE dell'UE) avverso la decisione della Commissione europea C/2023/552 (la "**Designazione ByteDance**") di designarla quale gatekeeper con riferimento al suo servizio di social network online **TikTok** ai sensi del regolamento (UE) 2022/1925, c.d. Digital Markets Act (**DMA**) (v. in questa Rubrica notizia n. 3 nel numero 3/2023: http://www.personaemercato.it/wp-

content/uploads/2023/11/Osservatorio.pdf [2023/3(3)RA]).

Analoghi ricorsi sono stati proposti il 15.12.2023 da Meta Platforms Inc. (**Meta**) contro la decisione della Commissione C/2023/1092 (la "**Designazione Meta**") e da Apple Inc. (**Apple**) contro la decisione della Commissione C/2023/548 (la "**Designazione Apple**"). Apple ha proposto anche un separato ricorso contro la decisione della Commissione del 5.9.2023 (caso DMA.100022) di avviare un'indagine di mercato relativamente a iMessage (la "**Decisione su iMessage**").

Alle cause sono stati dati numeri progressivi:

- C-1077/23 per il ricorso di ByteDance (il "**Ricorso ByteDance**");
- C-1078/23 per il ricorso di Meta (il "**Ricorso Meta"**);
- C-1079/23 e C-1080/23 per i due ricorsi di Apple (il "**Primo Ricorso Apple**" e il "**Secondo Ricorso Apple**" e, collettivamente, i "**Ricorsi Apple**").

Sul sito della CGUE della UE (**CURIA**) risulta che il Ricorso ByteDance è stato deciso in data 9.2.2024 apparentemente con due provvedimenti, dei quali risulta allo stato pubblicamente disponibile solo uno di natura provvisoria (il "**Ordinanza su ByteDance**").

Sullo stesso sito sono disponibili i testi del Ricorso Meta e dei Ricorsi Apple. Per il Ricorso ByteDance faremo qui di seguito riferimento, oltre che all' Ordinanza su ByteDance, anche ad un comunicato stampa della medesima società del 16 novembre 2023 (il "**Comunicato Stampa ByteDance**").

Nel Comunicato Stampa, la società cinese – dopo essersi detta favorevole ai "*principi del DMA*" – ha dedotto di non occupare una "*posizione consolidata e duratura*" nell'ambito del mercato di riferimento, ai sensi dell'art. 1(1)(c) del DMA, posto che TikTok sarebbe non già un attore consolidato bensì un "*challenger*" che continua "*a subire una forte pressione competitiva da parte di alcune delle aziende più grandi e di successo a livello mondiale*" e che "*porta nuova e importante competizione*".

Inoltre, secondo ByteDance, TikTok non raggiungerebbe neppure la soglia di ricavi stabilita all'art. 3(2) DMA al fine di presumere che i requisiti di cui al par. 1 del medesimo articolo siano soddisfatti. Sul punto, secondo la società ricorrente, la Commissione avrebbe errato nel calcolare i ricavi di TikTok effettuando una "*capitalizzazione di mercato globale della casa madre*", basandosi "*non solo sulle performance commerciali di TikTok nella regione*" europea, ma anche su quelle "*di linee di business che nemmeno operano in Europa*".

Infine, ByteDance ha lamentato la scarsa disponibilità della Commissione a valutare "*le ampie prove fornite*" a sostegno della propria posizione nel corso del procedimento di designazione, segnalando altresì il difetto di una "*indagine*" volta ad accertare accuratamente la posizione di TikTok nel proprio mercato di riferimento.

Dall'Ordinanza su ByteDance, si deduce che la ricorrente, nelle more del procedimento attivato per l'annullamento della decisione sulla sua designazione come gatekeeper, aveva proposto in via cautelare istanza di sospensione della medesima decisione ai sensi degli artt. 278 e 279 TFUE. Il Presidente del Tribunale, dopo aver richiamato la giurisprudenza della medesima CGUE che evidenzia la natura eccezionale dei provvedimenti cautelari ex art. 278 TFUE, ha motivatamente negato la ricorrenza nel caso di specie di motivi di urgenza, dichiarando di conseguenza di ritenere superflui l'accertamento del requisito della fondatezza *prima facie* del ricorso e il test del bilanciamento degli interessi, e respingendo quindi l'istanza.

Dalla lettura delle conclusioni del Ricorso Meta, si evince che la società ha chiesto in via principale di annullare la Designazione Meta nelle parti in cui in tale decisione si dichiara che i seguenti servizi di piattaforma di base di Meta costituiscono un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali ai sensi dell'articolo 3(1)(b) DMA:

- il servizio di comunicazione interpersonale indipendente dal numero **Messenger** di Meta;
- il servizio di intermediazione online **Marketplace** di Meta; e
- il servizio di social network online **Facebook** di Meta.

Infine, dalla lettura delle conclusioni dei Ricorsi Apple, si evince che la società ha chiesto in via principale:

- di annullare la Decisione su iMessage con cui la Commissione ha deliberato di avviare un'**indagine di mercato in relazione a iMessage** ai sensi degli artt. 16 e 17(3) DMA, nella parte in cui tale decisione si basa erroneamente sulla constatazione che iMessage è un servizio di comunicazione interpersonale indipendente dal numero ai sensi del DMA e della direttiva (UE) 2018/1972 istitutivo del codice europeo delle comunicazioni elettroniche (Primo Ricorso Apple);
- di annullare la Designazione Apple con cui la Commissione ha designato la ricorrente gatekeeper e ha qualificato il **sistema operativo iOS di Apple** come un punto di

accessoimportante affinché gli utenti commerciali raggiungano gli utenti finali, nella parte in cui la medesima decisione impone alla Apple di sottostare all'obbligo di rispettare gli **obblighi di interoperabilità** di cui all'art. 6(7)DMA; nonché nella parte in cui la decisione stabilisce che il servizio di intermediazione online **App Store di Apple** è un singolo servizio di piattaforma di base che costituisce un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali; nonché, infine, nelle parti in cui in tale decisione conclude erroneamente che **iMessage** è un servizio di comunicazione interpersonale indipendente dal numero ai sensi DMA e della direttiva (UE) 2018/1972 istitutiva del codice europeo delle comunicazioni elettroniche.

SALVATORE ORLANDO/RICCARDO ALFONSI

Decisione della Commissione C/2023/552 per ByteDance:
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C_202300552

Comunicato stampa ByteDance per Tiktok:
https://newsroom.tiktok.com/it-it/tiktok-fa-ricorso-contro-la-designazione-quale-gatekeeper-ai-sensi-del-digital-markets-act

Ordinanza di rigetto dell'istanza di sospensione di ByteDance:
https://curia.europa.eu/juris/document/document.jsf;jsessionid=A9564682E913BA4E6273018A8D36F659?text=&docid=282703&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1350153

Decisione della Commissione C/2023/1092 per Meta:
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C_202301092

Ricorso di Meta:
https://curia.europa.eu/juris/document/document.jsf?text=&docid=281095&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1&cid=2228366

2023/4(14)GDI

14. La decisione vincolante urgente dello EDPB del 27.10.2023 sul trattamento da parte di Meta di dati personali per finalità di pubblicità comportamentale

Il 27 ottobre 2023 il Comitato europeo per la protezione dei dati personali (EDPB) ha emesso una decisione vincolante e urgente, la n. 01/2023, affinché l'Autorità di controllo irlandese (Irish Data Protection Commission – di seguito **DPC**) vieti definitivamente a Meta Ireland Limited (di seguito **Meta**) di trattare i dati personali dei propri utenti per fini di pubblicità comportamentale sulla base del contratto e del legittimo interesse.
Tale decisione è stata adottata sulla base della richiesta, *ex* art. 66(2) del Regolamento UE 2016/679 (in seguito, anche, **Regolamento** o **GDPR**), dell'Autorità di controllo norvegese (di seguito anche **Datatilsynet**) che, con suo provvedimento d'urgenza del 14 luglio 2023, aveva temporaneamente vietato a Meta di profilare gli utenti dei suoi servizi Facebook e Instagram per fini di pubblicità comportamentale (*behavioural advertising*) (su questa decisione v. in questa Rubrica la notizia n. 8 del numero 2023/1 [2023/3(8)GDI]:
http://www.personaemercato.it/wp-content/uploads/2023/11/Osservatorio.pdf).
L'Autorità norvegese era intervenuta a seguito di alcuni avvenimenti di rilievo.
Sinteticamente:

- i pareri vincolanti nn. 3 e 4 del 5 dicembre 2022 con i quali l'EDPB aveva censurato la scelta di Meta di sostituire il consenso dell'interessato *ex* art. 6(1)(a) del Regolamento con il contratto *ex* art. 6(1)(b) dello stesso Regolamento quale base giuridica della pubblicità comportamentale (su cui v. in questa Rubrica notizia 6 nel numero 2023/1 [2023/1(6)GDI] http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf);
- i provvedimenti della DPC del 31 dicembre 2022, contro i servizi Facebook e Instagram, e quello del 12 gennaio 2023, contro il servizio WhatsApp, con i quali l'Autorità irlandese aveva sanzionato Meta per un totale di 396 milioni di euro per la violazione degli artt. 5(1)(a), 6(1)(b), 12(1) e 13(1)(c) del Regolamento (su cui v. in questa Rubrica notizia 6 nel numero 2023/1 [2023/1(6)GDI] http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf);
- il "*compliance report*" del 3 aprile 2023 con il quale Meta palesava l'intenzione di passare dal contratto al legittimo interesse *ex* art. 6(1)(f) del Regolamento quale base giuridica per la pubblicità comportamentale;
- da ultimo, la sentenza del 4 luglio 2023 con la quale la CGUE UE, nel caso C-252/21 *Facebook Inc. v. Bundeskartellamnt*, nel riconoscere la possibilità per le autorità nazionali per la concorrenza di applicare, in via incidentale, il

GDPR, ha ritenuto che Meta non potesse ricorrere al legittimo interesse quale base giuridica per la pubblicità personalizzata (su questa sentenza v. in questa Rubrica la notizia 7 nel numero 2023/3 [2023/3(7)CAT] http://www.personaemercato.it/wp-content/uploads/2023/11/Osservatorio.pdf).
Già in data 5 maggio 2023 la Datatilsynet aveva formalmente chiesto alla DPC di vietare a Meta il trattamento per finalità di pubblicità comportamentale sulla base del legittimo interesse sicché la precitata sentenza della CGUE ha rafforzato il convincimento della Datatilsynet di agire in via d'urgenza. L'Autorità norvegese ha così rivolto, in data 14 luglio 2023, a Meta l'ordine di non trattare i dati dei cittadini norvegesi per fini di pubblicità comportamentale ai sensi degli artt. 6(1)(b) e 6(1)(f) del Regolamento. Si trattava però di un ordine limitato nel tempo, al periodo di tre mesi dal 4 agosto 2023 al 3 novembre 2023, e nello spazio, al solo territorio della Norvegia. Da qui la richiesta, del 26 settembre 2023, all'EDPB di adottare una decisione urgente e vincolante per l'adozione di misure definitive e riguardanti l'intero territorio dello Spazio economico europeo (SEE).
All'esito di tali vicende, nella sua decisione vincolante e urgente, l'EDPB rileva innanzitutto la violazione dell'art. 6(1) del Regolamento per l'inappropriato affidamento al contratto e al legittimo interesse per il trattamento dei dati sulla posizione e di interazione pubblicitaria raccolti sui prodotti Meta per finalità di pubblicità comportamentale.
In altre parole, Meta non aveva ottemperato alle decisioni della DPC e pertanto si poneva in violazione del dovere di conformarsi alle decisioni delle autorità di vigilanza.
Conseguentemente e a causa del rischio di danni gravi e irreparabili in assenza di misure finali urgenti, si rileva la necessità di derogare agli ordinari meccanismi di cooperazione e coerenza per ordinare misure definitive.
Inoltre, l'EDPB ha ritenuto che l'urgenza potesse essere presunta sulla base dell'art. 61(8) GDPR, cosa che corroborava ulteriormente la necessità di derogare ai meccanismi regolari di cooperazione e coerenza.
Tutto ciò ha portato l'EDPB ad ordinare alla DPC l'adozione di misure definitive consistenti nel divieto di trattamento, ai sensi dell'art. 58(2)(f) GDPR, indirizzato a Meta e riguardante il trattamento dei dati personali per scopi di pubblicità comportamentale in tutto lo SEE.
In conclusione, con la decisione ad oggetto l'EDPB ha incaricato la DPC di ordinare a Meta la cessazione dei suoi trattamenti per finalità di pubblicità comportamentale. La DPC ha quindi ottemperato notificando a Meta la decisione finale, del 10 novembre 2023, contenente il divieto di trattare dati personali a fini di pubblicità comportamentale sulla base del contratto e del legittimo interesse in tutta l'area dello Spazio economico europeo.

GUIDO D'IPPOLITO

https://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en

2023/4(15)BP

15. Il ricorso di NOYB del novembre 2023 al Garante privacy austriaco per la pratica di Meta "*Pay or Okay*"

Nel novembre 2023, NOYB, associazione austriaca senza scopo di lucro attiva nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, ha proposto, ai sensi del combinato disposto degli artt. 77 e 80 GDPR, ricorso contro Meta all'autorità per la protezione dei dati personali austriaca (il **Garante privacy austriaco**), lamentando la violazione degli artt. 6, par. 1, 7, par. 4 e 5, par. 1, lett. a) GDPR e invocando la procedura d'urgenza di cui all'art. 66 GDPR.
La condotta contestata riguarda l'adozione, da parte della nota società americana, di una pratica che trova efficace sintesi nella formula "*Pay or Okay*". All'utente di Facebook e Instagram, interessato reclamante per il tramite di NOYB, viene imposta da Meta un'alternativa per poter continuare ad accedere ai *social network* a far data dal primo di marzo del 2024: pagare la somma di € 20,99 al mese (€ 251,88 all'anno) o prestare il proprio consenso al trattamento dei dati personali per finalità di pubblicità personalizzata.
Si tratta di condotta che altro non rappresenta che l'inevitabile precipitato del fallimento dei precedenti tentativi da parte del colosso americano di rinvenire una valida base giuridica per il trattamento di profilazione finalizzato alla somministrazione di pubblicità mirata ora nella necessità per la esecuzione del contratto *ex* art. 6, lett. b) GDPR, ora nel legittimo interesse di cui all'art. 6, lett. f) GDPR: esclusa nel dicembre 2022 dal Garante privacy irlandese, su parere vincolante del Comitato europeo per la protezione dei dati personali (EDPB), la prima possibilità (v. in questa Rubrica la notizia 6 nel numero 2023/1

[2023/1(6)GDI] http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf) e censurata la seconda nel luglio 2023 dal Garante privacy norvegese in forza di quanto già sostenuto dalla CGUE UE in una pronuncia dello stesso mese nel caso C-252/21 (v. in questa Rubrica le notizia 7 e 8 nel numero 2023/3 [2023/3(7)CAT] [2023/3(8)GDI] http://www.personaemercato.it/wp-content/uploads/2023/11/Osservatorio.pdf), Meta, invero, non poteva che tornare a far leva sul consenso dell'interessato di cui all'art. 6, lett. a), GDPR.

Come detto, però, oggetto di contestazione non è di per sé (ed evidentemente) la base giuridica, bensì l'avere configurato la prestazione del consenso quale obbligatorio alternativo strumento rispetto al pagamento in denaro per potere avere accesso ai servizi offerti dalla piattaforma.

Sulla premessa, secondo la tesi proposta dalla reclamante, di una contrarietà della pratica in parola al principio della inalienabilità d ei diritti fondamentali, giacché «*linking consent under Article 6(1)(a) GDPR to a payment has the exact opposite effect: the fundamental right is relinquished in exchange for a payment (or the avoidance of payment)*» (§ 4.2 del reclamo), la violazione delle disposizioni del Regolamento già sopra richiamate e, dunque, l'illiceità del trattamento sarebbero, in estrema sintesi, da ravvisarsi nella mancata prestazione di un consenso "libero" (§ 4.3 del reclamo).

Dopo avere rilevato (§ 4.3.1 del reclamo) la significativa discrepanza che dai sondaggi empirici emerge tra l'effettiva volontà degli utenti della rete di non vedere i propri dati trattati per finalità di pubblicità comportamentale (circa il 90% degli utenti lo avrebbe dichiarato) e la fattuale prestazione del consenso (circa il 99% lo presterebbe) – in proposito nel ricorso risulta menzionato in nota un sondaggio dell'Istituto Gallup del 2019 – e dopo avere evidenziato la maggiore facilità tecnica accordata per la prestazione del consenso rispetto alla opzione del pagamento in denaro (§ 4.3.2. del reclamo), NYOB ne denuncia la mancanza di libertà sulla base di ulteriori indici. Più in particolare, viene rilevata in primo luogo la mancanza di un'alternativa sul mercato rispetto ai servizi offerti dalla società. Non soltanto, si segnala (§ 4.3.4. del reclamo, ove si parla di un "*abuse of market dominance*"), Facebook è senz'altro il più diffuso *social network*, ma, di più e appunto perciò, i contatti, gli amici e i conoscenti dell'interessato non possono essere trovati se non su quella piattaforma: si tratta del c.d. "*network effect andlock-in effect*". Ancora, richiamando un *obiter dictum* della recente pronuncia della CGUE UE nel caso C-252/21, cui abbiamo fatto già sopra riferimento (sulla quale, v. in questa Rubrica la notizia 7 nel numero 2023/3 [2023/3(7)CAT] http://www.personaemercato.it/wp-content/uploads/2023/11/Osservatorio.pdf), ove si ammette che all'utente possa essere presentata «*an equivalent alternative* [...], *if necessary for an appropriate fee*», la reclamante argomenta che, in ogni caso, la prestazione in denaro richiesta all'interessato da Meta in alternativa al consenso non può considerarsi una «*reasonable remuneration*» (§ 4.3.5 del reclamo). Se, infatti, da un generale punto di vista economico - ritiene NOYB- tale sarebbe un prezzo che, coprendo i costi, assicuri un margine di profitto, il quale possa compensare il mancato guadagno dato dall'impossibilità di ricorrere alla pubblicità personalizzata, ebbene, si rileva, premesso che i costi di fornitura di un *social network* non sono affatto elevati e che la differenza di profitto tra la pubblicità comportamentale e quella, non personalizzata, c.d. "contestuale", non supera il 4%, appare senz'altro "*non appropriate*" richiedere un pagamento annuo tanto elevato quanto quello richiesto, alla luce peraltro altresì della inadeguatezza della uniforme forfettarietà del prezzo (€ 251,88 all'anno, per tutti), che non tiene in considerazione l'effettivo e variabile utilizzo che del *social network* viene fatto da persona a persona. Richiamando, poi, sul piano particolare, la personale situazione dell'interessato (§ 4.4. e 2.3 del reclamo), caratterizzata da un'accentuata vulnerabilità economica, NOYB evidenzia come la scelta tra la prestazione del consenso e il pagamento del prezzo equivalga in definitiva alla scelta tra «*either paying for his food or his debts or giving up his fundamental right to data protection*».

Infine, dopo avere, per vero piuttosto sbrigativamente, altresì ipotizzato una violazione dei requisiti di specificità e informazione del consenso (§ 4.5 del reclamo), un ultimo argomento viene speso facendo leva sulle potenziali conseguenze di più ampia portata alle quali condurrebbe una mancata censura della pratica in parola: se questa dovesse considerarsi lecita, è verosimile che tutti i fornitori di servizi digitali decidano di farvi ricorso; da un approssimativo calcolo, potrebbe risultare che il prezzo annuo da corrispondere per evitare il trattamento dei propri dati giunga a superare gli € 10,000, con la conseguenza che «*without a clear rejection of a "pay or Ok" system, the right to the protection of personal data will degenerate into a luxury good*» (§ 4.6. del reclamo).

Alla luce di quanto riportato, NOYB, suggerendo altresì l'inflizione di una sanzione amministrativa ai sensi dell'art. 83 GDPR (§ 5.4. del reclamo), chiede al Garante austriaco che (§ 5.2. del reclamo), dichiarata la violazione dell'art. 6, par. 1, dell'art. 7, par. 4 e dell'art. 5, par. 1, lett. a) GDPR, sia ordinato a Meta di (a) astenersi definitivamente dal trattare i dati personali del reclamante a fini di pubblicità personalizzata ai sensi dell'art. 58, par. 2, lett. f) GDPR; (b) cancellare i dati personali del reclamante trattati a fini di pubblicità personalizzata ai sensi dell'art. 58, par. 2, lett. g) GDPR in combinato disposto con l'art. 17, par. 1, lett. d) GDPR e informare tutti i destinatari di tale cancellazione ai sensi dell'art. 58, par. 2, lett. g) GDPR in combinato disposto con l'art. 19 GDPR; (c) rendere le proprie operazioni di trattamento conformi al GDPR ai sensi dell'art. 58, par. 2 lett. d), GDPR e, in particolare, ottenere un consenso valido dall'interessato reclamante.

BENIAMINO PARENZO

https://noyb.eu/en/noyb-files-gdpr-complaint-against-meta-over-pay-or-okay

2023/4(16)TB

16. I due ricorsi di NOYB del 16.11.2023 contro la Commissione europea (davanti a EDPS) e del 14.12.2023 contro X (davanti alla DPA olandese) per le pratiche di online microtargeting a supporto di una pubblicità commissionata dalla Commissione europea

L'associazione austriaca NOYB (acronimo di *None Of Your Business*), fondata nel 2017 dall'avvocato ed attivista privacy Max Schrems – già promotore dei ricorsi avanti la CGUE dell'Unione Europea sfociati nelle sentenze "Schrems I" e "Schrems II" – prosegue nella sua *mission* di esperire procedimenti giudiziali e lanciare campagne mediatiche strategiche allo scopo di sostenere la corretta applicazione del Regolamento EU 2016/679 ("**GDPR**") e di sensibilizzare l'opinione pubblica in merito.

L'ultima denuncia di NOYB ha ad oggetto una campagna di *microtargeting* condotta nel mese di settembre 2023 dalla Commissione Europea tramite la piattaforma X (già Twitter), finalizzata a promuovere tra gli utenti della stessa la Proposta di regolamento della Commissione sul contrasto agli abusi sui minori e sulla circolazione di materiale pedopornografico (la "**Proposta**" COM/2022/209). Tale Proposta è stata oggetto di numerose critiche sin dalla sua pubblicazione, in quanto prevede che ove vi sia un sospetto di disseminazione via chat di contenuti di tal sorta, i fornitori dei servizi di messaggistica debbano intraprendere un'attività di sorveglianza massiva di messaggi, video e foto scambiati tramite i loro servizi.

Secondo la ricostruzione di NOYB, la campagna della Commissione sarebbe stata progettata in modo tale da mostrare annunci pubblicitari relativi alla Proposta solamente ad utenti di X non interessati a parole chiave come *#Qatargate, Brexit, Marine Le Pen, Alternative für Deutschland, Vox, Christian, Christian-phobia o Giorgia Meloni;* in particolare, uno di tali annunci avrebbe avuto lo scopo di influenzare l'opinione degli utenti facendo leva sulla maggiore importanza che i soggetti coinvolti in un sondaggio sulla questione avrebbero pretesamente attribuito alla individuazione di abusi su minori rispetto al tema del diritto alla privacy online.

NOYB ha quindi intrapreso un'iniziativa a doppio binario, in qualità di rappresentante di un reclamante di nazionalità olandese cui era stato mostrato l'annuncio pubblicitario sopra descritto, nei confronti dei due attori protagonisti di tale campagna: l'associazione ha infatti presentato un reclamo dapprima, il 16.11.2023, avanti il Garante Europeo per la Protezione dei Dati Personali (ossia l'autorità competente ad indagare i trattamenti di dati personali condotti dalle istituzioni europee) contro la Commissione Europea, come primo contitolare del trattamento; successivamente, ha promosso, in data 14.12.2023, un secondo reclamo contro X, in qualità di altro contitolare, avanti la *data protection authority* olandese.

Nel reclamo nei confronti della Commissione, NOYB censura, in particolare, l'utilizzo da parte della stessa di dati relativi alle opinioni politiche ed alle credenze religiose degli utenti – protette come "categorie particolari di dati" ai sensi dell'art. 10(1) del regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati (corrispondente all'art. 9(1) del regolamento (UE) 2016/679, di seguito **GDPR**) – in assenza di un'adeguata base giuridica.

Peraltro, la campagna di microtargeting in commento sarebbe secondo NOYB del tutto in contrasto con una precedente Proposta di Regolamento già pubblicata dalla Commissione, ossia quella relativa alla trasparenza ed al targeting della pubblicità politica (COM 2021/731), la quale prevede un divieto all'utilizzo di tecniche di targeting per finalità di pubblicità politica che

coinvolgano il trattamento di particolari categorie di dati personali.
Nel reclamo contro X, NOYB lamenta il trattamento da parte di X di dati di categorie particolari degli utenti in assenza di alcuna delle esimenti previste dall'art. 10(2) del regolamento (UE) 2018/1725 (corrispondente all'art. 9(2) GDPR) e, pertanto, in violazione del divieto generale di trattamento di tali dati disposto dall'art. 10(1) del regolamento (UE) 2018/1725 (corrispondente all'art. 9(1) GDPR).
NOYB evidenzia inoltre che siffatta condotta risulta in violazione anche dell'art. 26(3) del DSA (Digital Services Act: regolamento (UE) 2022/2065), che vieta alle piattaforme di *presentare pubblicità ai destinatari del servizio basate sulla profilazione […] utilizzando le categorie speciali di dati personali* di cui all'art. 9(1) GDPR, nonché in contrasto con le linee guida pubblicitarie della stessa X, nelle quali quest'ultima afferma che l'affiliazione politica ed il credo religioso degli utenti non dovrebbero essere utilizzati per il targeting degli annunci.
In attesa delle decisioni di EDPS e della DPA olandese, la Commissione appare avere già dismesso – secondo le dichiarazioni rilasciate da un avvocato di NOYB – la campagna pubblicitaria incriminata.

TIMOTEO BUCCI

Ricorso contro la Commissione promosso davanti all'EDPS:
https://noyb.eu/sites/default/files/2023-11/13112023%20-%20Complaint%20EC%20microtargeting_Final%20Version%20-%20REDACTED.pdf

Ricorso contro X promosso davanti alla DPA olandese:
https://noyb.eu/it/gdpr-complaint-against-x-twitter-over-illegal-micro-targeting-chat-control-ads

2023/4(17)IT

17. Adottato il 6.12.2023 il regolamento Consob per la finanza sulle piattaforme DLT

Il 6 dicembre 2023**,** con Delibera n. 22923, la Consob ha adottato il Regolamento sull'emissione e circolazione in forma digitale di strumenti finanziari di attuazione del decreto-legge 17 marzo 2023, n. 25, convertito, con modificazioni, dalla legge 10 maggio 2023, n. 52 (di seguito, rispettivamente, il **Regolamento Consob** e il **Decreto FinTech**).
Il Decreto Fintech ha attuato il regolamento (UE) 2022/858 (c.d. DLT Pilot Regime) che stabilisce un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito e ha introdotto un nuovo regime di forma e circolazione per taluni strumenti finanziari, che va ad affiancarsi alle tradizionali forme cartolare e dematerializzata, come disciplinata dal d.lgs. 24 febbraio 1998, n. 58 (**TUF**).
La forma digitale prevede il ricorso alle tecnologie a registro distribuito per l'emissione e il trasferimento di strumenti finanziari. Il Decreto FinTech disciplina le condizioni per il ricorso a tale nuovo regime di forma e circolazione e definisce la legge di circolazione degli strumenti in questione. In particolare, l'emissione e il trasferimento degli strumenti finanziari digitali sono eseguiti attraverso scritturazioni su un registro per la circolazione digitale.
Il Decreto Fintech ammette la possibilità di avvalersi della forma digitale anche per strumenti finanziari che non siano destinati alla negoziazione in una delle sedi di negoziazione contemplate dal regime MiFID e, quindi, esclusi dall'ambito di applicazione del regolamento DLT Pilot. In particolare, nei casi non ricompresi nell'ambito di applicazione del citato regime pilota, il legislatore nazionale ha previsto la necessità di avvalersi di registri per la circolazione digitale tenuti da responsabili del registro iscritti in un apposito elenco della Consob.
Possono rivestire la qualifica di responsabile del registro i soggetti individuati all'articolo 19, commi 1 e 2, del Decreto FinTech:
a) le banche, le imprese di investimento e i gestori di mercati stabiliti in Italia;
b) gli intermediari finanziari iscritti nell'albo di cui all'articolo 106, del d.lgs. 1° settembre 1993, n. 385 (**TUB**), gli istituti di pagamento, gli istituti di moneta elettronica, i gestori come definiti all'articolo 1, comma 1, lettera q-bis), del TUF, e le imprese di assicurazione o riassicurazione stabiliti in Italia, esclusivamente con riferimento a strumenti finanziari digitali emessi dagli stessi o da componenti del gruppo di appartenenza stabiliti in Italia;
c) gli emittenti diversi dai precedenti che intendono svolgere l'attività di responsabile del registro esclusivamente con riferimento a strumenti finanziari digitali emessi dagli stessi;
d) i soggetti stabiliti in Italia diversi dai precedenti (che intendono svolgere l'attività per conto terzi);

e) gli ulteriori soggetti eventualmente individuati con regolamento dalla Consob, d'intesa con la Banca d'Italia;
f) i depositari centrali italiani che intendono svolgere l'attività di responsabile del registro in via accessoria, previa autorizzazione ai sensi degli articoli 16 e 19 del regolamento (UE) 909/2014.
Il Regolamento Consob è stato emesso successivamente allo svolgimento di una consultazione pubblica nell'ambito della quale è stata illustrata la "strategia per fasi" adottata dall'Istituto per l'esercizio delle numerose deleghe regolamentari attribuite alla Consob dal Decreto FinTech. In questa prima fase il Regolamento Consob ha ad oggetto gli ambiti strettamente funzionali all'avvio immediato dell'elenco dei responsabili del registro. A seguire la Consob valuterà l'esercizio delle ulteriori potestà regolamentari, anche alla luce dei casi d'uso e delle prassi di mercato che andranno a formarsi.
Le disposizioni del Regolamento Consob confermano l'impianto prospettato in sede di consultazione e in particolare:

(i) definiscono i principi e i criteri relativi alla formazione e alla tenuta dell'elenco dei responsabili del registro e alle relative forme di pubblicità;
(ii) disciplinano le forme e le modalità di presentazione dell'istanza e la procedura per l'iscrizione nel citato elenco, individuando le possibili cause di sospensione e interruzione del procedimento;
(iii) stabiliscono il contenuto minimo delle informazioni che il responsabile del registro deve mettere a disposizione del pubblico circa le modalità operative del registro e i dispositivi a tutela della sua operatività.

È interessante richiamare che nel corso della consultazione pubblica la Consob ha raccolto le indicazioni del mercato non solo sul testo del Regolamento, ma anche riguardo alle materie che potranno essere oggetto di disciplina secondaria in una fase successiva.
Al riguardo, diversi rispondenti si sono espressi a favore dell'estensione della nuova normativa sull'impiego della DLT per l'emissione e la circolazione di derivati cartolarizzati e quote di S.r.l.
È stato chiesto inoltre di:
a) eliminare, in alcune ipotesi, il divieto previsto dall'articolo 19, comma 4, del Decreto FinTech per le banche e le imprese di investimento e i membri del gruppo di appartenenza, di esercitare i servizi di negoziazione per conto proprio e di sottoscrizione a fermo per strumenti finanziari scritturati nel registro di cui sono responsabili, poiché tale divieto ostacolerebbe l'accesso al mercato da parte degli intermediari tradizionali;
b) introdurre esenzioni specifiche, incluso dall'obbligo di stabilimento in Italia, per i soggetti che si qualifichino quali Crypto Asset Service Provider ai sensi del regolamento (UE) 2023/1114 (**MiCAR**), che intendano assumere anche il ruolo di responsabile del registro ai sensi del Decreto FinTech.
Nella stessa direzione, alcuni rispondenti hanno proposto di ampliare il novero dei soggetti che possono essere iscritti nell'elenco anche a soggetti non stabiliti in Italia, ma comunque facenti parte di un gruppo che include soggetti stabiliti in Italia; Un rispondente ha altresì richiesto alla Consob di definire degli standard di riferimento per gli *smart contract* che possano permettere all'Istituto di intervenire attivamente *ex ante*.
La Consob terrà conto delle indicazioni raccolte nelle valutazioni relative all'eventuale esercizio delle ulteriori potestà regolamentari accordate dal Decreto Fintech.

IRENE TAGLIAMONTE
Avvocato, Ufficio Analisi di Impatto della Regolamentazione,
Divisione Strategie Regolamentari, Consob
Le idee e le opinioni espresse in questo articolo sono da attribuire unicamente all'autore e non coinvolgono l'istituzione di appartenenza

https://www.consob.it/web/area-pubblica/bollettino/documenti/bollettino2023/d22923.htm

2023/4(18)VC

18. Il provvedimento interpretativo del Garante privacy del 26.10.2023 sul diritto di accesso degli eredi e dei chiamati all'eredità ai nominativi dei beneficiari delle polizze vita accese dal *de cuius*

Il 26 ottobre 2023 il Garante per la protezione dei dati personali ha reso un provvedimento interpretativo in tema di esercizio del diritto di accesso, da parte degli eredi e dei chiamati all'eredità, ai dati identificativi dei beneficiari di polizze vita stipulate dalla persona deceduta, *ex* art. 15 Regolamento (UE) 2016/679 ("**GDPR**") e art. 2-*terdecies* d.lgs. 30-06-2003, come modificato dal d.lgs. 10 agosto 2018, n. 101 ("**cod. priv.**") (reg.

provv. n. 520 del 26-10-2023, in G.U. n. 281 del 1-12-2023).

Il provvedimento muove dalla posizione del quadro normativo di riferimento. Si richiamano, in primo luogo, le disposizioni eurounitarie che includono nella nozione di dato personale «qualsiasi informazione riguardante una persona fisica determinata o determinabile» e attribuiscono all'interessato il diritto di accedere e ottenere copia dei dati personali che lo riguardano (artt. 4 e 15 GDPR). Tale diritto d'accesso, aggiunge il Garante, di norma non consente di conoscere informazioni riguardanti persone diverse dall'interessato. Tuttavia la disciplina nazionale, in attuazione del Considerando 27 GDPR, legittima all'esercizio dei diritti sui dati riguardanti persone decedute «chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di tutela» (art. 2-*terdecies*, co. 1, cod. priv.), ossia soggetti diversi dall'interessato, che acquistano il diritto di conoscere le stesse informazioni che avrebbe potuto conoscere quest'ultimo.

I dubbi sull'applicabilità di tali norme alla richiesta di accesso ai dati identificativi dei beneficiari di polizze assicurative accese in vita dal defunto riguardano sia il profilo sostanziale (*i.e.* il fondamento normativo della pretesa dell'erede o del chiamato all'eredità), sia quello procedurale (*i.e.* l'oggetto della verifica imposta al titolare del trattamento).

La giurisprudenza di merito viene ordinata in due filoni:

(i) quello che afferma l'obbligo dell'assicuratore di comunicare l'identità del beneficiario designato dal *de cuius* nella polizza, attesa la strumentalità della conoscenza di tale informazione all'esercizio di un diritto dell'erede o del chiamato. Posta la prevalenza, in linea generale, del diritto alla tutela giurisdizionale sull'interesse alla riservatezza del soggetto al quale i dati si riferiscono, nel caso di specie la conoscibilità dell'informazione sul beneficiario è argomentata in base all'art. 2-*terdecies* cod. priv. e all'ampia estensione semantica della nozione di dato personale *ex* art. 4 GDPR. Quanto ai profili procedurali, al titolare del trattamento si impone un controllo "in negativo" sulla non manifesta pretestuosità della richiesta, ossia sulla mancanza anche solo in astratto di una posizione di diritto sostanziale per la cui tutela sia necessaria la conoscenza dei dati (su punto il Garante richiama Trib. Verona 1-02-2011, n. 53; Trib. Rovereto, 13-02-2019, n. 39; Trib. Treviso, 27-02-2020; Trib. Marsala, 3-11-2020; Trib. Forlì, sez. lav., 27-01-2022, n. 440; Trib. Milano, 10-11-2021; Trib. Firenze, 25-02-2022; Trib. Roma, 22-11-2022);

(ii) quello che limita l'obbligo dell'assicuratore alla comunicazione dei dati relativi al defunto, con esclusione di quelli di terzi, fra cui i beneficiari della polizza vita. Questo orientamento muove dalla terzietà del beneficiario rispetto al rapporto fra assicurato e assicuratore e dalla natura *iure proprio* dell'acquisto del diritto ai vantaggi dell'assicurazione, i quali non compongono l'asse ereditario (art. 1920, co. 3, c.c.). Di qui l'idea che l'identità del beneficiario non possa dirsi informazione che riguarda, né direttamente né indirettamente, la persona deceduta (lo stipulante a favore del terzo). Inoltre, mentre la conoscenza dell'esistenza della polizza e dell'ammontare dei premi versati è indispensabile per ricostruire l'asse ereditario, poiché il loro pagamento è donazione indiretta oggetto di collazione e riduzione, conoscere il nome dei beneficiari rileverebbe solo se si dimostrasse l'entità della lesione della propria quota di legittima e l'insufficienza a reintegrarla con le disposizioni testamentarie (ascritte a questo filone Trib. Roma, 12-01-2016; Trib. Enna, 30-9-2021, n. 320; Trib. Brescia, 8-10-2021, n. 25; Trib. Bologna, 29-01-2022).

La premessa dell'orientamento di merito contrario all'ostensione dei dati del beneficiario risale alla giurisprudenza di Cassazione; la quale però, concorde nel postulato, diverge anch'essa negli esiti. Un primo arresto trae dalla terzietà del beneficiario il diniego dell'accesso: «il diritto di accesso riconosciuto dalle predette disposizioni [*ratione temporis*, art. 7-9 cod. priv.] ha ad oggetto i dati personali che riguardano direttamente la persona richiedente che, per legge è l'unica titolare dell'interesse, meritevole di tutela, a ricevere quelle informazioni. Una diversa conclusione, al fine di consentire l'accesso ai dati di terze persone, non è giustificabile alla luce del citato terzo comma dell'art. 9, il quale, attribuendo al richiedente il diritto di accedere ai "dati personali concernenti persone decedute", fa chiaro ed esclusivo riferimento ai dati della persona deceduta [...] ma non autorizza l'accesso ai dati personali non riferiti al *de cuius*, come i terzi beneficiari dei contratti stipulati dal primo, i quali, nel caso di assicurazione sulla vita, acquistano un diritto proprio ai vantaggi dell'assicurazione (art. 1920, co. 3, c.c.)» (Cass. 8-09-2015, n. 17790). Una seconda pronuncia, sull'analogo caso dell'aderente a fondo pensione complementare, pur concordando sulla terzietà del beneficiario e, di lì, sull'eccentricità della disciplina sull'accesso ai dati di persone decedute, reputa fondata la pretesa a conoscere dati *di terzi*, quando ciò sia necessario per la difesa giurisdizionale di un

diritto dell'istante. Attesa la prevalenza di quest'ultimo interesse su quello alla riservatezza, la richiesta di accesso è fondata direttamente nell'art. 6(1)(f) GDPR e non nel diritto all'esercizio dei diritti sui dati di persone decedute *ex* art. 2-*terdecies* cod. priv.

A questo frastagliato quadro giurisprudenziale si aggiungono le linee guida emanate dall'European Data Protection Board ("**EDPB**") in tema di diritto d'accesso ai propri dati personali (n. 1/2022, efficaci dal 28-03-2023: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_it).

Il Garante richiama, in particolare, i passaggi in cui l'EDPB afferma:

(i) la possibile rilevanza promiscua o condivisa dei dati personali, che possono riferirsi *contemporaneamente* a più persone, sicché il diritto di accesso *ex* art. 15 GDPR, se non è esercitabile con riguardo a dati che si riferiscono *solo* a qualcun altro, potrebbe esserlo con riguardo a dati che riguardino *anche* qualcun altro (§ 4.2.1, nn. 104-105);

(ii) la soggezione, in ogni caso, della decisione sull'ostensione dei dati personali che si riferiscano a più persone al giudizio di bilanciamento *ex* art. 15(4) GDPR e al principio di minimizzazione, entrambi declinati come condotte doverose del titolare del trattamento (§ 6.2, nn. 168 e 173).

Delineato il quadro normativo, giurisprudenziale e regolatorio, il Garante esprime il suo parere nel senso che «tra i dati ai quali è possibile accedere ai sensi del combinato disposto tra gli art. 15 [GDPR] e 2-*terdecies* [cod. priv.], rientr[a]no anche i dati personali dei beneficiari di polizze assicurative accese in vita da una persona deceduta, in presenza di determinati presupposti e previa attenta valutazione comparativa tra gli interessi in gioco effettuata dall'impresa assicuratrice titolare del trattamento». Quest'ultima deve contemperare tutela della riservatezza dei dati personali e interesse a difendersi in giudizio esercitato dal richiedente attraverso «un "controllo in negativo"» sulla non manifesta pretestuosità della richiesta d'accesso. A tal fine «il titolare dovrà verificare la sussistenza dei presupposti di seguito indicati:

1) che il soggetto che esercita il diritto di accesso ai dati del defunto sia portatore di una posizione di diritto soggettivo sostanziale in ambito successorio, corrispondente alla qualità di chiamato all'eredità o di erede;
2) che l'interesse perseguito sia concreto e attuale, cioè realmente esistente al momento dell'accesso ai dati, strumentale o prodromico alla difesa di un proprio diritto successorio in sede giudiziaria».

Ai sensi dell'art. 57(1), lett. b), d) e v) GPDR e dell'art. 154, co. 1, cod. priv., il Garante invita i titolari del trattamento, oltreché ad attenersi all'interpretazione così data agli artt. 15 GDPR e 2-*terdecies* cod. priv., a valutare l'adeguatezza delle dell'informativa resa al contraente e al beneficiario designato (art. 13 e 14(1), lett. e), GDPR).

VALERIA CONFORTINI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9954881

2023/4(19)RMo

19. La sentenza della CGUE del 7.12.2023 nelle cause riunite C-26/22 e C-64/22 (caso SCHUFA sul controllo giurisdizionale sulle decisioni delle DPA e sulla cancellazione di dati personali relativi all'esdebitazione)

Il 7 dicembre 2023 la Corte di Giustizia dell'Unione europea (d'ora in poi **CGUE** o **la Corte**) ha pronunciato una decisione nelle cause riunite C- 26/22 e C-64/22 (d'ora in poi la **Sentenza**), avente ad oggetto una pluralità di domande di pronuncia pregiudiziale ai sensi dell'articolo 267 TFUE, vertenti sull'interpretazione degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (d'ora in poi la **Carta**), nonché degli articoli 6(1)(f), 17(1)(d), 40, 77(1), e 78(1) del regolamento (UE) 2016/679 (d'ora in poi **GDPR** o anche il **Regolamento**).

Le suddette domande sono state presentate dal *Verwaltungsgericht Wiesbaden* (tribunale amministrativo di Wiesbaden, Germania, d'ora in poi **Tribunale di Wiesbaden**), nell'ambito di due controversie che oppongono due interessati, UF e AB, al Land Hessen (Land dell'Assia) in merito al rifiuto dello *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (Commissario per la protezione dei dati e la libertà di informazione del Land dell'Assia, d'ora in poi **HBDI**) di ingiungere alla SCHUFA Holding AG (d'ora in poi **SCHUFA**) di procedere alla cancellazione di dati personali conservati da quest'ultima, relativi alle esdebitazioni di UF e di AB.

UF e AB conseguivano un'esdebitazione anticipata sulla base di due ordinanze pronunciate all'esito di procedure di insolvenza che li riguardavano. La cancellazione dei dati relativi a tali decisioni dal

registro pubblico informatizzato sulle procedure d'insolvenza (d'ora in poi **registro pubblico informatizzato**) avveniva decorsi sei mesi dalla loro adozione, in linea con quanto previsto all'art. 9(1) dell'I*nsolvenzordnung* (legge sulle procedure di insolvenza) del 5 ottobre 1994 e all'art. 3(1) e (2) della *Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet* (regolamento sulle pubblicazioni su Internet nelle procedure d'insolvenza) del 12 febbraio 2002 (d'ora in poi "**InsoBekV**").

SCHUFA è una società di diritto privato tedesco che *inter alia* registra e archivia nelle proprie banche dati informazioni provenienti da registri pubblici, in particolare informazioni relative a esdebitazioni anticipate, che poi fornisce alle proprie controparti commerciali. SCHUFA cancella tali informazioni una volta trascorsi tre anni dal loro inserimento nel registro pubblico informatizzato, conformemente al codice di condotta elaborato in Germania da un'associazione che riunisce società che forniscono informazioni commerciali, approvato dall'autorità di controllo competente.

UF e AB chiedevano a SCHUFA la cancellazione dei dati relativi alle decisioni di esdebitazione di cui erano stati oggetto. SCHUFA rigettava tale richiesta, asserendo che *i)* il trattamento di tali dati aveva luogo nel rispetto del GDPR; *ii)* il termine di sei mesi relativo alla cancellazione dei dati nel registro pubblico informatizzato, previsto all'articolo 3(1) InsoBekV, non fosse applicabile al caso di specie.

Sia UF che AB proponevano reclamo all'HBDI, quale autorità di controllo competente, che però riteneva lecito il trattamento dei dati effettuato da SCHUFA, rigettando i reclami, con decisioni, rispettivamente, del 1.3.2021 e del 9.7.2021.

UF e AB presentavano ricorso avverso le decisioni dell'HBDI dinanzi al Tribunale di Wiesbaden e l'HBDI presentava controricorso rilevando che:

- il diritto di presentare un reclamo, previsto all'articolo 77(1) GDPR, è un mero diritto di petizione e il relativo sindacato giurisdizionale non verte sulla correttezza nel merito della decisione emanata a seguito del reclamo, essendo tale sindacato limitato a verificare che l'autorità di controllo abbia trattato il reclamo e informato il reclamante dello stato e dell'esito dello stesso;
- i dati ai quali le società che forniscono informazioni commerciali hanno accesso possono essere conservati per tutto il tempo necessario in vista delle finalità per i quali vengono trattati e, inoltre, il codice di condotta, elaborato dall'associazione che raggruppa le società che forniscono tali specie di informazioni ed approvato dall'autorità di controllo, dispone la cancellazione di tali dati decorsi tre anni dall'iscrizione nel registro pubblico informatizzato.

Le due cause venivano riunite e il Tribunale di Wiesbaden decideva di sospendere il giudizio e di proporre alla CGUE una serie di questioni pregiudiziali ai sensi dell'articolo 267 TFUE, di seguito esaminate.

La prima questione: l'ampiezza del sindacato giurisdizionale esercitato su una decisione adottata da un'autorità di controllo all'esito di un reclamo dell'interessato

Con la prima questione, il Tribunale di Wiesbaden ha chiesto se l'articolo 78(1) GDPR debba essere interpretato nel senso che il sindacato giurisdizionale esercitato su una decisione adottata da un'autorità di controllo all'esito di un reclamo sia limitato a stabilire se tale autorità abbia trattato il reclamo, adeguatamente indagato sull'oggetto di quest'ultimo e informato il reclamante della conclusione dell'esame, o se, invece, tale decisione debba essere oggetto di un sindacato giurisdizionale completo, il quale includa il potere del giudice adito di imporre all'autorità di controllo di adottare una specifica misura.

In merito a tale questione, la CGUE ha innanzitutto delineato oggetto, funzione e limiti del sindacato giurisdizionale ai sensi degli artt. 78(1) e (2), e 79(1) GDPR, nonché il rapporto tra un simile sindacato ed i poteri riconosciuti all'autorità di controllo dall'art. 58 GDPR, argomentando come segue:

i) ogni interessato ha il diritto a un ricorso giurisdizionale «effettivo», conformemente all'articolo 47 della Carta;
ii) in base all'art.78(1) GDPR, fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica può proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda;
iii) secondo tale disposizione, come interpretata alla luce del Considerando 143 del Regolamento, i giudici investiti di un ricorso avverso una decisione di un'autorità di controllo hanno piena giurisdizione su tutte le questioni di fatto e di diritto relative alla controversia ad essi sottoposta (cfr. sentenza del 12 gennaio 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, punto 41); tale giurisdizione non è limitata alla questione se l'autorità di controllo abbia trattato il reclamo, indagato in modo adeguato

sull'oggetto di quest'ultimo e informato il reclamante della conclusione dell'esame;

iv) le disposizioni del Regolamento offrono diversi mezzi di ricorso ai soggetti che lamentano una violazione dello stesso, fermo restando che ciascuno di tali mezzi di ricorso deve poter essere esercitato «fatto salvo» ogni altro (cfr. sentenza del 12 gennaio 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, punto 34)

v) i rimedi previsti rispettivamente dall'articolo 78(1) GDPR (concernente, come detto, il diritto dell'interessato ad un rimedio giurisdizionale effettivo avverso una decisione vincolante di un'autorità di controllo), e dall'articolo 79(1) GDPR (relativo, invece, al diritto ad accedere ad un ricorso giurisdizionale effettivo nei confronti del titolare o del responsabile del trattamento, quando una posizione giuridica soggettiva dell'interessato sia stata lesa da un trattamento non conforme al GDPR) possono essere esercitati in modo concomitante e indipendente (cfr. sentenza del 12 gennaio 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, punto 35 e dispositivo); ciò, infatti, rafforza l'obiettivo enunciato al Considerando 141 del Regolamento, consistente nel garantire che qualsiasi interessato, "qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato [...]", abbia accesso ad un ricorso giurisdizionale effettivo secondo l'articolo 47 della Carta;

vi) il riconoscimento del diritto ad un ricorso giurisdizionale effettivo avverso il titolare o il responsabile del trattamento in base all'art. 79(1) GDPR non dispiega alcuna incidenza sulla portata del sindacato giurisdizionale avente ad oggetto una pronuncia vincolante dell'autorità di controllo ai sensi dell'art. 78(1) GDPR;

vii) inoltre, conformemente all'articolo 8(3) della Carta, nonché agli artt. 51(1) e 57(1)(a) GDPR (secondo i quali l'autorità deve vigilare e dare applicazione al GDPR ed è responsabile per la protezione delle libertà e dei diritti fondamentali dell'interessato), le autorità nazionali di controllo sono incaricate di vigilare sul rispetto delle norme dell'Unione relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (cfr. sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, punto 107);

viii) l'autorità di controllo deve trattare con la dovuta diligenza i reclami proposti, ai sensi dell'articolo 77(1) GDPR, dall'interessato il quale ritenga che i propri diritti siano stati lesi da un trattamento non conforme al Regolamento (cfr. sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, punto 109); tuttavia, quanto alla adozione dei rimedi elencati all'articolo 58(2) GDPR, la medesima autorità dispone di un margine di discrezionalità nella scelta di un mezzo appropriato e necessario (cfr. sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, punto 112);

ix) il giudice nazionale investito di un ricorso ai sensi dell'articolo 78, paragrafo 1, del GDPR, il cui sindacato si estende a tutte le questioni di fatto e di diritto relative alla controversia di cui trattasi, non è legittimato a sostituire la propria valutazione delle misure correttive appropriate e necessarie alla scelta in merito esercitata dall'autorità di controllo, ma può sempre verificare che tale autorità abbia rispettato i limiti del suo potere discrezionale.

Alla luce delle suindicate argomentazioni, la CGUE ha risposto alla prima questione nei modi seguenti: l'articolo 78(1) GDPR deve essere interpretato nel senso che una decisione su reclamo adottata da un'autorità di controllo è soggetta a un sindacato giurisdizionale completo.

Le ulteriori questioni: il legittimo interesse alla conservazione di dati sulle esdebitazioni di persone fisiche in banche dati di società che forniscono informazioni a imprese del settore creditizio, per un periodo eccedente il termine nel quale è consentita, in base al diritto nazionale, la conservazione di tali dati in un registro pubblico informatizzato

Con le questioni dalla seconda alla quinta, esaminate dalla CGUE congiuntamente, il Tribunale di Wiesbaden ha chiesto:

– I) se sia conforme all'art. 5(1)(a) GDPR, in combinato disposto con l'art. 6(1)(f)GDPR, una prassi di una società che fornisce informazioni commerciali, consistente nel conservare, nelle proprie banche dati, informazioni provenienti da un registro pubblico informatizzato, relative alla concessione di esdebitazioni a favore di persone fisiche, e nel cancellare tali informazioni al termine

di un periodo di tre anni, conformemente a un codice di condotta ai sensi dell'art. 40 GDPR, mentre il periodo di conservazione di dette informazioni nel registro pubblico informatizzato, secondo la disciplina nazionale, è di sei mesi; e

– II) se l'articolo 17(1)(c) e (d) GDPR debba essere interpretato nel senso che una società che fornisce informazioni commerciali, che abbia tratto da un registro pubblico informazioni relative alla concessione di esdebitazioni a favore di persone fisiche, sia tenuta a cancellarle.

Sub I)

Nel pronunciarsi sulla questione sub I), la CGUE ha in primo luogo chiarito le condizioni di liceità di un trattamento di dati personali concernenti esdebitazioni di persone fisiche, compiuto da società che forniscono informazioni a imprese del settore creditizio e basato sull'art. 6(1)(f) GDPR, secondo cui un trattamento di dati personali è lecito se persegue un legittimo interesse del titolare del trattamento o di un terzo. Inoltre, la Corte: *a)* ha precisato i criteri per valutare la liceità di un trattamento di tale natura, che abbia una durata superiore a quella prevista dal diritto nazionale regolante il registro pubblico informatizzato delle esdebitazioni, alla luce del principio di necessità del trattamento rispetto al legittimo interesse perseguito dal titolare o da un terzo, nonché tenuto conto della possibilità che tale interesse possa essere ragionevolmente realizzato con un periodo più breve di conservazione di tali dati; *b)* ha infine statuito che un codice di condotta ai sensi dell'art. 40 GDPR non può predeterminare l'esito della ponderazione dei contrapposti interessi, che deve invece compiersi alla luce del caso concreto, secondo l'art. 6(1)(f) GDPR.

Le argomentazioni dispiegate dalla CGUE in merito alla questione sub I) possono riassumersi come segue:

i) ai sensi dell'articolo 5(1)(a) GDPR, i dati personali devono essere trattati in modo lecito, corretto e trasparente;

ii) per poter essere considerato lecito, un trattamento deve rientrare in uno dei casi previsti dall'articolo 6(1) del Regolamento [cfr. sentenza del 4 luglio 2023, Meta Platforms e a. (Condizioni generali di utilizzo di un social Network), C-252/21, punto 90 e giurisprudenza citata];

iii) nel caso di specie, la liceità del trattamento di dati personali deve essere valutata alla luce dell'articolo 6(1)(f) GDPR, secondo cui il trattamento di dati personali è lecito solo se ricorrono tre condizioni cumulative, vale a dire, in primo luogo, il perseguimento di un legittimo interesse da parte del titolare del trattamento o di un terzo, in secondo luogo, la necessità del trattamento dei dati personali per la realizzazione di tale interesse e, infine, che gli interessi o i diritti e le libertà fondamentali dell'interessato non prevalgano sul suddetto legittimo interesse [sentenza del 4 luglio 2023, Meta Platforms e a. (Condizioni generali di utilizzo di un social Network), C-252/21, punto 106 e giurisprudenza citata];

iv) premesso che un'ampia gamma di interessi possono, in linea di principio, qualificarsi "legittimi", la condizione della necessità del trattamento dei dati personali per la realizzazione di un interesse di tale natura sussiste allorché esso non possa ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti agli artt. 7 e 8 della Carta. Ciò implica una ponderazione dei diritti e degli interessi contrapposti, che dipende, in linea di principio, dalle circostanze del caso concreto e che, di conseguenza, spetta al giudice del rinvio compiere tenendo conto di tali circostanze [sentenza del 4 luglio 2023, Meta Platforms e a. (Condizioni generali di utilizzo di un social Network), C-252/21, punti 108 e 110];

v) ai sensi del Considerando 47 GDPR, gli interessi e i diritti fondamentali dell'interessato possono prevalere sugli interessi del titolare del trattamento quando i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un siffatto trattamento, nonché tenuto conto della portata del trattamento e dell'incidenza di quest'ultimo su tale persona;

vi) nel caso di specie, vengono in rilievo l'interesse commerciale di SCHUFA e quello delle sue controparti contrattuali a poter valutare il merito creditizio dei consumatori con cui intendono concludere contratti connessi ad un credito, anche al fine di adempiere all'obbligo di valutare il merito creditizio dei consumatori, ai sensi della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori e della direttiva 2014/17/UE sui contratti di credito ai consumatori relativi a beni immobili residenziali;

vii) tuttavia, come osservato dal Tribunale di Wiesbaden, tale trattamento implica una

duplicazione di banche dati, quella del registro pubblico informatizzato delle esdebitazioni previsto dal diritto tedesco, e la banca dati delle società, come SCHUFA, che forniscono informazioni commerciali. Tali società procedono alla conservazione dei dati non in occasione di un caso concreto, bensì nell'eventualità che le proprie controparti contrattuali chiedano loro informazioni. In secondo luogo, dette società conservano tali dati per tre anni, e ciò sulla base di un codice di condotta adottato e approvato dall'autorità di controllo, ai sensi dell'art. 40 GDPR, mentre la normativa nazionale prevede, per il registro pubblico informatizzato, un periodo di conservazione di soli sei mesi;

viii) SCHUFA sostiene che non sarebbe in grado di fornire informazioni in tempo utile, se fosse tenuta ad attendere una specifica richiesta di un partner contrattuale prima di poter iniziare a raccogliere dati e che ciò basterebbe a qualificare il trattamento come necessario alla realizzazione del proprio legittimo interesse;

ix) secondo la CGUE, invece, "una conservazione parallela di tali dati nelle banche dati di siffatte società", pur quando limitata nella durata ai sei mesi consentiti dal diritto nazionale, "costituisce nondimeno un'ingerenza nei diritti sanciti agli articoli 7 e 8 della Carta. A tal riguardo, la Corte ha già dichiarato che la presenza degli stessi dati personali in più fonti rafforza l'ingerenza nel diritto della persona alla vita privata (v. sentenza del 13 maggio 2014, Google Spain e Google, C-131/12, punti 86 e 87)"

x) alla luce di tali considerazioni, spetta al giudice del rinvio verificare se la conservazione dei dati di cui trattasi da parte di SCHUFA nelle proprie banche dati sia confinata allo stretto necessario alla realizzazione del proprio legittimo interesse, ed una simile valutazione va compiuta considerato che i dati di cui trattasi possono essere consultati nel registro pubblico anche senza che un'impresa commerciale abbia chiesto informazioni in un caso concreto;

xi) occorre poi verificare se, alla luce di una ponderazione dei diritti e degli interessi contrapposti in gioco, gli interessi legittimi perseguiti dal titolare del trattamento non possano ragionevolmente essere raggiunti con un periodo di conservazione più breve di tali dati;

xii) secondo la CGUE, occorre al riguardo considerare che il trattamento di dati relativi alla concessione di un'esdebitazione concerne informazioni sensibili sulla vita privata dell'interessato (cfr. sentenza del 13 maggio 2014, Google Spain e Google, C-131/12, punto 98) e che l'esdebitazione è prevista dalla legge al fine di consentire al beneficiario di partecipare nuovamente alla vita economica;

xiii) la realizzazione di tale obiettivo verrebbe compromessa se le società che forniscono informazioni commerciali potessero, al fine di valutare la situazione economica di una persona, conservare dati relativi ad un'esdebitazione e utilizzare siffatti dati in sede di valutazione del merito creditizio di tale persona, anche una volta che essi siano stati cancellati dal registro pubblico informatizzato;

xiv) un indice rilevante in merito è desumibile proprio dalla previsione contenuta nel diritto tedesco, all'art. 3(1) e 2 InsoBekV, per cui, decorso un termine di sei mesi, i diritti e gli interessi della persona coinvolta prevalgono su quelli dei creditori ad accedere a informazioni relative alle esdebitazioni;

xv) un trattamento di dati personali come quello di cui trattasi, protratto oltre il termine di conservazione dei dati nel registro pubblico informatizzato, non può quindi dirsi giustificato sulla base degli interessi del settore creditizio;

xvi) una diversa interpretazione, nel caso di specie, non potrebbe essere giustificata alla luce del codice di condotta adottato ai sensi dell'art. 40 GDPR ed approvato dall'autorità di controllo competente, che autorizza la conservazione dei suddetti dati per un periodo di tre anni, giacché una simile previsione non è in grado di derogare all'art. 6(1)(f) GDPR, e non può dunque essere presa in considerazione nella ponderazione da effettuarsi in forza di tale disposizione.

Alla luce delle suddette argomentazioni, la CGUE ha risposto alla questione sub I) nel seguente modo: l'art. 5(1)(a) GDPR, in combinato disposto con l'articolo 6(1)(f) GDPR dev'essere interpretato nel senso che osta ad una prassi di società che forniscono informazioni commerciali, consistente nel conservare nelle proprie banche dati informazioni provenienti da un registro pubblico informatizzato relative alla concessione di esdebitazioni a favore di persone fisiche, al fine di poter fornire informazioni sul merito creditizio di tali persone, per un periodo che va oltre quello durante il quale i dati possono essere conservati in tale registro pubblico.

Sub II)
La CGUE ha infine tracciato i corollari della decisione assunta sulle questioni innanzi illustrate, chiarendo le condizioni in presenza delle quali sussiste il diritto dell'interessato alla cancellazione dei propri dati, trattati da società che forniscono alle controparti commerciali informazioni sulla esdebitazione di persone fisiche.
Le argomentazioni utilizzate in merito dalla CGUE possono riassumersi come segue:

i. conformemente all'art. 17(1)(d) GDPR, l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione, senza ingiustificato ritardo, dei dati personali che lo riguardano e il titolare del trattamento ha l'obbligo di cancellare tali dati personali senza ingiustificato ritardo, qualora i dati personali siano stati trattati illecitamente;
ii. nel caso di specie, dunque, SCHUFA è tenuta a cancellare i dati personali illecitamente trattati oltre il termine di conservazione di sei mesi previsto per il registro pubblico fallimentare;
iii. invece, nell'ipotesi in cui il giudice del rinvio dovesse concludere che il trattamento entro il periodo di sei mesi sia conforme all'art. 6(1)(f) GDPR, troverebbe applicazione l'art. 17(1)(c), GDPR, secondo il quale i dati debbono essere cancellati quando l'interessato si oppone al trattamento ai sensi dell'art. 21(1) GDPR e non sussiste alcun «motivo legittimo prevalente per procedere al trattamento»;
iv. la prevalenza di un motivo legittimo per procedere al trattamento, rispetto agli interessi, diritti e libertà dell'interessato, deve essere dimostrata dal titolare del trattamento;
v. pertanto, se questi non giunge a fornire una siffatta prova, l'interessato che si sia opposto al trattamento conformemente all'art. 21(1) GDPR, ha il diritto di ottenere la cancellazione di tali dati sulla base dell'art. 17(1)(c) GDPR;
vi. nel caso di specie, compete al giudice del rinvio esaminare se sussistano, in via eccezionale, motivi legittimi prevalenti del titolare in grado di giustificare il trattamento.

Alla luce delle suddette argomentazioni, la CGUE ha risposto alla questione sub II) nel seguente modo:

- l'art. 17(1)(d) GDPR deve essere interpretato nel senso che il titolare del trattamento è tenuto a cancellare, senza ingiustificato ritardo, i dati personali oggetto di un trattamento illecito;
- l'art. 17(1)(c) GDPR deve essere interpretato nel senso che l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione, senza ingiustificato ritardo, dei dati personali che lo riguardano qualora si opponga al trattamento ai sensi dell'articolo 21(1) GDPR e non sussistano motivi legittimi prevalenti che possano giustificare, in via eccezionale, il trattamento in esame.

ROBERTA MONTINARO

https://curia.europa.eu/juris/document/document.jsf;jsessionid=05D6FB6CD55C0DEC3F568D132380FF39?text=&docid=280436&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=7920300

2023/4(20)RMo

20. La sentenza della CGUE del 7.12.2023 nella causa C-634/21 (caso SCHUFA sul credit scoring automatizzato)

Il 7 dicembre 2023 la Corte di Giustizia dell'Unione europea (d'ora in poi **CGUE** o la **Corte**) ha pronunciato una decisione nella causa C-634/21 (d'ora in poi la **Sentenza**), avente ad oggetto due domande di pronuncia pregiudiziale ai sensi dell'art. 267 TFUE, vertenti sull'interpretazione degli artt. 6(1) e 22 del Regolamento (UE) 2016/679 (d'ora in poi **GDPR** o **Regolamento**).
Le domande di pronuncia pregiudiziale sono state proposte dal *Verwaltungsgericht Wiesbaden* (tribunale amministrativo di Wiesbaden, Germania, d'ora in poi **Tribunale di Wiesbaden**), nell'ambito di una controversia promossa dall'interessato OQ contro il Land Hessen (Land dell'Assia) in merito al rifiuto dello *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (Commissario per la protezione dei dati e la libertà di informazione per il Land Assia, Germania, d'ora in poi **HBDI**) di ingiungere alla SCHUFA Holding AG (d'ora in poi **SCHUFA**) di accogliere una richiesta presentata da OQ, avente ad oggetto l'accesso e la cancellazione di propri dati personali trattati da SCHUFA.
Quest'ultima è una società di diritto tedesco che fornisce ai *partner* contrattuali informazioni sul merito creditizio di terzi, in particolare di consumatori. A tal fine, SCHUFA stabilisce un pronostico sulla probabilità di un comportamento futuro di una persona (*score*), come il rimborso di un prestito, a partire da talune caratteristiche di tale

persona, sulla base di procedure matematiche e statistiche. Il calcolo dei punteggi (*scoring*) si basa sul presupposto che assegnando una persona a un gruppo di altre persone con caratteristiche comparabili, che si sono comportate in un certo modo, si può prevedere un comportamento analogo.
Nel caso esaminato dalla CGUE, a OQ, consumatore, veniva negata la concessione di un prestito da parte di un terzo dopo essere stato oggetto di uno *score* negativo da parte di SCHUFA, comunicato da quest'ultima a tale terzo. OQ allora esercitava il diritto di accesso ai propri dati personali conservati da SCHUFA, nonché di cancellazione dei dati ritenuti inaccurati. In risposta alla richiesta di accesso, SCHUFA si limitava a comunicare a OQ il relativo punteggio e a "esporre, a grandi linee, le modalità di calcolo dei punteggi", rifiutandosi al tempo stesso di ostendere i dati presi in considerazione ai fini di tale calcolo, nonché la loro ponderazione, in quanto ritenuti protetti da segreto commerciale. SCHUFA, inoltre, eccepiva che la propria attività consiste solamente nel far pervenire informazioni alle proprie controparti contrattuali, le quali poi le impiegano per adottare decisioni di natura contrattuale.
OQ proponeva reclamo all'HBDI, autorità di controllo competente, chiedendole di ingiungere a SCHUFA di accogliere la domanda di accesso ai dati e la loro cancellazione. Il reclamo veniva però rigettato e OQ proponeva ricorso al Tribunale di Wiesbaden, in applicazione dell'art. 78 (1) GDPR.
Il Tribunale di Wiesbaden sollevava due questioni pregiudiziali ai sensi dell'art. 267 TFUE:

1) Se l'art. 22 (1) GDPR debba essere interpretato nel senso che il calcolo automatizzato di un tasso di probabilità relativo alla capacità di un interessato di saldare in futuro un debito costituisce già una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici che riguardano l'interessato o che incide in modo analogo significativamente sulla sua persona, qualora tale tasso, calcolato sulla base di dati personali relativi all'interessato, sia trasmesso dal titolare del trattamento a un terzo titolare del trattamento e quest'ultimo basi prevalentemente su tale tasso la sua decisione sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con l'interessato.
2) In caso di risposta negativa alla prima questione pregiudiziale: se gli artt. 6(1) e 22 GDPR debbano essere interpretati nel senso che ostano a una normativa nazionale ai sensi della quale il ricorso a un tasso di probabilità – nella fattispecie relativo alla solvibilità e alla disponibilità a pagare di una persona fisica, che includa informazioni sui crediti – di un certo comportamento futuro di una persona fisica, allo scopo di decidere sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con tale persona ("*scoring*"), è consentito solo se sono soddisfatte determinate ulteriori condizioni, meglio specificate nella motivazione della domanda di pronuncia pregiudiziale».
Nel rispondere alla questione sub **1)**, la CGUE ha innanzitutto chiarito la portata dell'art. 22(1) GDPR, prendendo in esame le condizioni in presenza delle quali tale disposizione può applicarsi ad un trattamento meramente automatizzato, che venga impiegato in un processo decisionale scandito in fasi distinte, poste in essere da soggetti non appartenenti ad una medesima organizzazione.
L'art. 22(1) GDPR, prevede che un interessato abbia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
Secondo la CGUE, il diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, di cui all'art. 22(1) GDPR deve essere interpretato come un divieto generale e non come un diritto che può essere esercitato dall'interessato.
La CGUE ha dunque aderito alle argomentazioni espresse nelle Conclusioni emesse dall'Avvocato generale Pikämae nella causa in oggetto (d'ora in poi **Conclusioni dell'AG**), secondo le quali "Un'interpretazione [dell'art. 22 GDPR] alla luce del considerando 71 del Regolamento, la quale tenga conto dell'impianto di tale disposizione, in particolare del suo paragrafo 2, che specifica i casi in cui tale trattamento automatizzato è eccezionalmente consentito, suggerisce [...] che tale disposizione stabilisce un divieto generale di decisioni del tipo sopra descritto". Di conseguenza, il titolare di un simile trattamento non è autorizzato ad assumere decisioni basate esclusivamente su trattamenti automatizzati, a meno che non si applichi una delle deroghe individuate nell'art. 22(2) GDPR.
Un simile divieto entra in gioco in presenza di tre condizioni cumulative: *i)* che esista una «decisione», *ii)* che tale decisione sia «basata unicamente su un trattamento automatizzato, compresa la profilazione», e, *iii)*, che essa produca «effetti giuridici [riguardanti l'interessato]» o incida «in modo analogo significativamente» sull'interessato.
Nell'interpretare le suddette condizioni, secondo la CGUE, occorre tenere conto, non soltanto della formulazione testuale dell'art. 22 GDPR, "ma anche

del contesto in cui essa si inserisce nonché degli obiettivi e della finalità che persegue l'atto di cui essa fa parte (sentenza del 22 giugno 2023, Pankki S, C-579/21, punto 38 e giurisprudenza citata)".

La finalità perseguita dall'art. 22 GDPR consiste nel proteggere le persone contro i rischi specifici per i loro diritti e le loro libertà derivanti dal trattamento automatizzato di dati personali, compresa la profilazione. Prova ne è il particolare regime introdotto a tutela dell'interessato dal GDPR: *i)* innanzitutto, i doveri di informazione supplementari aventi ad oggetto la «logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato», in forza degli artt. 13(2)(f), 14(2)(g) e 15(1)(h) GDPR; *ii)* inoltre, il dovere di "prevedere garanzie adeguate e assicurare un trattamento corretto e trasparente nel rispetto dell'interessato, in particolare mediante l'uso di procedure matematiche o statistiche appropriate per la profilazione e mediante l'applicazione di misure tecniche e organizzative adeguate al fine di minimizzare il rischio di errori (punto 59 della Sentenza)". "Tali misure comprendono inoltre quantomeno il diritto dell'interessato di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione adottata nei suoi confronti (punto 66 della Sentenza)".

Per quanto riguarda la prima condizione, la nozione di «decisione» di cui all'art. 22(1) GDPR non è definita dal Regolamento. Tuttavia, dalla formulazione stessa di tale disposizione, risulta che tale nozione è ampia. Invero:

i) può consistere in qualsiasi "misura" implicante valutazione di aspetti personali relativi alla persona fisica interessata da tale trattamento, come chiarito dal Considerando 71 GDPR (punto 58 della Sentenza);
ii) ed include non solo atti che producono effetti giuridici riguardanti il soggetto interessato, ma anche atti che incidono significativamente su di esso in modo analogo;
iii) sempre in base al citato Considerando 71 GDPR, "sono coperti dal termine «decisione», a titolo esemplificativo, il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani" (punto 45 della Sentenza).

Pertanto, per la CGUE, "la nozione di «decisione» ai sensi dell'art. 22(1) GDPR […] è sufficientemente ampia da ricomprendere il risultato del calcolo della solvibilità di una persona sotto forma di tasso di probabilità relativo alla capacità di tale persona di onorare impegni di pagamento in futuro" (punto 46 della Sentenza).

Nel caso di specie, tuttavia, si è in presenza di un atto, la decisione di accogliere o rigettare la domanda di mutuo, formalmente indipendente dalla valutazione negativa elaborata da SCHUFA, che, rispetto al primo atto, assume natura preparatoria. Sorge dunque la questione di stabilire quale dei due atti possa qualificarsi come una «decisione» nel significato di cui all'art. 22(1) GDPR.

Secondo la CGUE: "in circostanze come quelle di cui al procedimento principale, nelle quali il tasso di probabilità stabilito da una società che fornisce informazioni commerciali e comunicato a una banca svolge un ruolo decisivo nella concessione di un credito, il calcolo di tale tasso deve essere qualificato di per sé come decisione che produce nei confronti di un interessato «effetti giuridici che lo riguardano o che incid[e] in modo analogo significativamente sulla sua persona», ai sensi dell'art. 22(1) GDPR (punto 50 della Sentenza)". In una simile evenienza, osserva la Corte "[…] si deve ritenere che anche la terza condizione alla quale è subordinata l'applicazione dell'art. 22(1) GDPR sia soddisfatta, in quanto un tasso di probabilità come quello di cui trattasi nel procedimento principale incide, quanto meno, sull'interessato significativamente" (punto 49 della Sentenza).

Viceversa, se si adottasse una interpretazione restrittiva del termine decisione in un caso come quello di specie, in cui si ha distinzione di fasi nel procedimento decisionale, l'interessato non potrebbe ottenere una tutela effettiva, giacché:

i) "[..] il calcolo di un tasso di probabilità come quello di cui trattasi nel procedimento principale sfuggirebbe ai requisiti specifici previsti all'art. 22, paragrafi da 2 [*il titolare dei dati deve adottare misure adeguate a salvaguardare i diritti dell'interessato*] a 4 [*di regola, un trattamento meramente automatizzato non può essere basato sulle speciali categorie di dati personali, di cui all'art. 9(1)*] GDPR, sebbene tale procedura si basi su un trattamento automatizzato e produca effetti che incidono significativamente sull'interessato, in quanto l'azione del terzo, al quale tale tasso di probabilità è trasmesso, è condizionata in modo decisivo da quest'ultimo" (punto 62 della Sentenza);
ii) inoltre, "come rilevato dall'avvocato generale al paragrafo 48 delle sue conclusioni, da un lato, la persona interessata non potrebbe far valere, presso la società che fornisce informazioni commerciali che calcola il tasso di probabilità che la riguarda, il suo diritto di accesso alle informazioni specifiche di cui all'art. 15(1)(h) GDPR, in assenza di adozione di un processo decisionale automatizzato da parte di tale agenzia.

> Dall'altro lato, anche supponendo che l'atto adottato dal terzo rientri […] nell'ambito di applicazione dell'art. 22(1) GDPR […], tale terzo non sarebbe in grado di fornire tali informazioni specifiche in quanto generalmente non ne dispone" (punto 63 della Sentenza).

La CGUE desume, infine, una serie di corollari dalla suddetta interpretazione: il calcolo di un *credit score*, cadendo nel perimetro dell'art. 22(1) GDPR, è vietato, a meno che: **(i)** non ricorra una delle eccezioni previste all'art. 22(2) GDPR e **(ii)** vengano osservati i requisiti, sopra ricordati, di cui all'art. 22(3) e (4) del Regolamento.

L'art. 31 del *Bundesdatenschutzgesetz* (legge federale sulla protezione dei dati), del 30 giugno 2017 (d'ora in poi **BDSG**), intitolato «Protezione delle operazioni economiche in caso di "scoring" e di informazioni sulla solvibilità», ammette il ricorso al *credit scoring* al fine di decidere circa la stipulazione, esecuzione o cessazione di un contratto con una persona fisica persona, in presenza di date condizioni ivi indicate.

Pertanto, spetta al giudice del rinvio verificare se l'art. 31 BDSG possa essere qualificato come base giuridica, ai sensi dell'art. 22(2)(b) GDPR [per il quale occorre che il trattamento automatizzato sia autorizzato dal diritto dell'Unione europea o dal diritto di uno stato membro al quale l'interessato è assoggettato. In caso affermativo, tale giudice deve accertare se sia osservata la condizione ivi stabilita, vale a dire che siano adottate dalla suddetta normativa nazionale misure adeguate a tutelare i diritti e le libertà, nonché i legittimi interessi della persona oggetto di valutazione, in particolare quando vengano usate le particolari categorie di dati di cui all'art.9 GDPR] (punto 72 della Sentenza).

Aggiunge poi la CGUE che gli Stati membri non possono adottare, ai sensi dell'art. 22(2)(b) GDPR, normative che autorizzino la profilazione in violazione dei requisiti stabiliti dagli articoli 5 e 6 del Regolamento, come interpretati dalla giurisprudenza della Corte.

Per quanto riguarda, in particolare, le condizioni di liceità previste all'art. 6(1)(a), (b) e (f) GDPR, "gli Stati membri non sono autorizzati a prevedere norme complementari per l'applicazione di tali condizioni, dato che una siffatta facoltà, conformemente all'art. 6(3) di tale Regolamento, è limitata ai motivi di cui all'art. 6(1), lettere c) [*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*] ed e) [*il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*] (punto 69 della Sentenza)".

Invece, in merito all'art. 6(1)(f) GDPR [*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*], gli Stati membri non possono discostarsi dall'interpretazione fornita dalla medesima CGUE, nella sentenza gemella del 7 dicembre 2023, pronunciata nel caso UF e AB vs Land Hessen con l'intervento di SCHUFA Holding, C-26/22 e C-64/22 (cfr. contributo precedente in questa Rubrica), stabilendo in modo definitivo il risultato della ponderazione dei diritti e degli interessi in gioco (punto 70 della Sentenza).

Avendo risposto affermativamente alla questione sub **1)**, la CGUE non si è pronunciata sulla questione sub **2)**.

ROBERTA MONTINARO

https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=B267456FF4823EC6FDABD7409D00976F?mode=DOC&pageIndex=0&docid=280426&part=1&doclang=IT&text=&dir=&occ=first&cid=2482431

2023/4(21)ES

21. La causa pilota per danni avviata da NOYB contro CRIF e AZ Direct davanti al Tribunale civile di Vienna in conseguenza di una accertata violazione del GDPR relativamente al trattamento di dati personali per fini di calcolo del merito di credito

In data 4 dicembre 2023 l'organizzazione Noyb, Centro europeo per il diritto digitale (da ora anche "**Noyb**") presieduta da Max Schrems, ha reso noto di aver avviato un'azione giudiziaria nei confronti di Crif GmbH e AZ Direct Osterreich GmbH (da ora anche le "**convenute**") per asserite violazioni da parte di quest'ultime del diritto dei dati e in particolare del Reg. 2016/679/UE (c.d. **"**General Data Protection Regulation" o **"**GDPR").

Noyb è un'organizzazione non profit dedicata alla protezione dei diritti previsti dal GDPR e, in generale, dalla normativa europea in materia di dati e privacy. Si tratta, quindi, di un'associazione che rientra nella nozione dettata dall'art. 80, par. 1 GDPR a cui gli individui possono dare mandato "*di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79*

nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82".

Crif GmbH è una società specializzata in sistemi informativi di credito e business, analisi, servizi di outsourcing ed elaborazione dati, mentre AZ Direct Osterreich GmbH è una società di marketing che raccoglie regolarmente dati come nome, data di nascita e genere dei cittadini austriaci nello svolgimento delle proprie attività.

Nel presente caso, in base a quanto ricostruito nell'atto di citazione diffuso da Noyb, nel dicembre 2012 Crif e AZ Direct (all'epoca denominata Deltavista GmbH) avrebbero sottoscritto un contratto, poi modificato nel maggio 2018, in base a cui Crif avrebbe avuto la possibilità di interrogare la banca dati di AZ Direct ed estrarre dei dati sugli individui austriaci per fini di indagini sulla solvibilità o sull'identità. Senonché, in tal modo i dati sarebbero stati utilizzati per scopi diversi da quelli per cui furono raccolti poiché AZ Direct, che agiva in qualità di responsabile del trattamento ai sensi dell'art. 4, par. 7 GDPR, avrebbe raccolto dei dati per finalità di marketing, che sarebbero stati utilizzati per finalità di credit rating degli individui, e senza il loro consenso al trattamento o al trasferimento dei dati o alle relative modifiche delle finalità del trattamento. Agli interessati non era stata nemmeno fornita l'informativa ex art. 14 GDPR. La presunta violazione potrebbe avere un impatto rilevante nella vita delle persone considerando l'importanza del giudizio sul merito creditizio: esso è in grado di condizionare dalla concessione di un prestito all'erogazione delle utenze domestiche, ma gli individui non avrebbero nemmeno potuto far valere i loro diritti in materia di dati personali perché ignari del trasferimento.

Tale forma di condivisione "segreta" dei dati era già stata stigmatizzata in passato da Noyb e il Garante della protezione dei dati austriaco ("**Datenschutzbehörde**" o "**DSB**") la aveva ritenuta illegittima in decisioni del 2023. Tuttavia, non aveva adottato provvedimenti tali da impedire che una simile situazione si verificasse di nuovo.

Per tale motivo, Noyb, quale mandataria di sette cittadini austriaci i cui dati personali sarebbero stati asseritamente trattati in maniera illegittima, ha agito giudizialmente davanti alla Corte civile regionale di Vienna.

In particolare, la domanda giudiziale è esperita in forza del combinato disposto degli artt. 79 e 82 GDPR: il primo stabilisce il diritto degli interessati a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento; il secondo, invece, prevede che "*chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

Le violazioni riguarderebbero, da un lato, il principio di limitazione delle finalità del trattamento sancito dall'art. 5, comma 1, let. b) GDPR per cui i dati personali devono essere "*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*". Dall'altro, viene in rilievo l'art. 6 GDPR poiché il trasferimentodei dati, e il trattamento da parte di Crif, sarebbe avvenuto senza una base giuridica valida. Come noto, peraltro, secondo la consolidata giurisprudenza della Corte di Giustizia europea "*ogni trattamento di dati personali deve, da un lato, essere conforme ai principi relativi al trattamento dei dati elencati all'articolo 5 del GDPR e, dall'altro, rispondere a uno dei principi relativi alla liceità del trattamento dati elencati all'articolo 6 di detto regolamento*" (cfr. Corte di Giustizia europea, sentenza del 22 giugno 2021, causa C-439/19, ECLI:EU:C:2021:504, par. 96)

In conclusione, Noyb ha ritenuto che la fattispecie descritta integrasse un trattamento illecito dei dati fonte di responsabilità solidale delle convenute ex art. 82, par. 2 e 4 GDPR e ha chiesto un ordine di cessazione della condotta asseritamente illegittima ("*Die 6. betroffene Person … macht darüber hinaus selbst Unterlassungsansprüche gegen die Beklagten gestendo*"), la condanna al pagamento dei danni morali, il calcolo delle somme indebitamente guadagnate da parte delle convenute in forza del trattamento illecito dei dati e il versamento della somma ai sette interessati ("*betroffene Personen … haben Schadenersatzansprüche (immaterieller Schadenersatz), Rechnungslegungsbegehren und Herausgabebegehren gegen die 1. Beklagte und 2. Beklagte (in der Folge auch gemeinsam die „Beklagten") aufgrund von massiven Datenschutzverstößen der Beklagten*"). Noyb, infine, ha fatto sapere che sta valutando la possibilità di intentare una *class action* per i fatti descritti.

EMANUELE STABILE

https://noyb.eu/en/noyb-sues-crif-and-az-direct-illegal-and-secret-data-processing

2023/4(22)GR

22. Le sentenze CGUE nei casi C-300/21 e C-340/21 sul danno non patrimoniale causato da violazione del GDPR

Con due sentenze, la prima del 4 maggio 2023 C-300/21, e la seconda del 14 dicembre 2023 C-340/21, la Corte di Giustizia dell'Unione europea (di seguito anche la **Corte**) ha affermato alcuni presupposti e criteri in tema di risarcimento del danno immateriale derivante dal trattamento di dati personali in violazione del Reg. UE 2016/679 sulla protezione dei dati.

Segnatamente, con la prima decisione (del 4 maggio 2023), la Corte, dopo aver (ri)affermato la primazia del diritto UE, ha stabilito: che la violazione delle disposizioni di cui al Regolamento 2016/679 (di seguito **GDPR** o il **Regolamento**) è condizione necessaria, ma non sufficiente, al perfezionarsi del diritto al risarcimento per il titolare dei dati; che l'obbligazione risarcitoria sorge solo a condizione che sussista un nesso eziologico tra la violazione e il pregiudizio sofferto dal titolare; e che la configurazione del diritto al risarcimento del danno immateriale prescinde dal superamento di una certa soglia di gravità della lesione e del pregiudizio sofferto.

Mentre, con la seconda decisione (del 14 dicembre 2023), la Corte ha ritenuto: che la divulgazione (o l'accesso) di dati personali da parte di un soggetto «*terzo*» non autorizzato, non è sufficiente, di per sé, a ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento non possano ritenersi «adeguate»; che l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento deve essere vagliata di volta in volta dai giudici nazionali, valutando in concreto se la natura, il contenuto e l'attuazione di tali misure risultino adeguate rispetto ai rischi connessi al trattamento nel caso specifico; che, sulla scorta del principio di responsabilità del titolare del trattamento, nell'azione di risarcimento spetta al titolare del trattamento fornire prova dell'adeguatezza delle misure di sicurezza attuate, fermo restando che una perizia giudiziaria non rappresenta un mezzo di prova «*sistematicamente necessario e sufficiente*»; che il titolare del trattamento non può essere affrancato dall'obbligo di risarcire il danno subito dal titolare dei dati per il solo fatto che il danno derivante dalla divulgazione non autorizzata dei dati personali sia stata effettuata da parte di terzi, a meno che il titolare del trattamento non dimostri che il fatto che ha provocato il danno non gli sia in alcun modo imputabile; e, infine, che, a seguito di una violazione del GDPR, il timore del titolare di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi può, di per sé, costituire un «*danno immateriale*» risarcibile.

Queste due decisioni, lette sistematicamente, offrono le prime coordinate per la ricostruzione di una dogmatica europea per il risarcimento del danno immateriale derivante dalla violazione del GDPR.

La decisione del 4 maggio 2023 C-300/21 riguarda un caso di richiesta di risarcimento del danno ex art. 82 GDPR da parte di un cittadino austriaco per il trattamento non autorizzato dei suoi dati personali effettuato dal principale operatore postale austriaco (la *Österreichische Post AG*). Precisamente, a partire dal 2017 la *Österreichische Post* ha raccolto molteplici dati della popolazione austriaca al fine di censirne le affinità con determinati partiti politici. Più nel dettaglio a partire, da tali dati, avvalendosi di un algoritmo, sulla base di criteri sociodemografici, la *Österreichische Post* ha definito degli "indirizzi di gruppi destinatari", allo scopo di cederli, dietro corrispettivo, a differenti organizzazioni intente a realizzare invii propagandistici mirati. Nel corso di tale attività, la *Österreichische Post* ha trattato dati che, per estrapolazione statistica, l'hanno erroneamente indotta ad attribuire a un cittadino un'elevata affinità nei confronti di un determinato partito politico. Questi, però, non aveva acconsentito al trattamento e (nonostante tali dati non fossero stati oggetto di cessione) e per conseguenza lamentava aver sofferto un pregiudizio (un disagio interiore consistente in una perdita di fiducia, in un sentimento di umiliazione) derivante dall'erronea attribuzione di una determinata affinità politica. Così, il cittadino ha proposto ricorso al Landesgericht für Zivilrechtssachen Wien diretto a: ingiungere la *Österreichische Post* a cessare il trattamento dei suoi dati, e condannarla al risarcimento del danno ex art. 82 GDPR (presuntivamente commisurato in euro 1.000,00). Con decisione confermata dall'*Oberlandesgericht Wien*, il giudice ha accolto l'inibitoria, senza accordare il risarcimento. Adito da ambedue le parti in causa, l'*Oberster Gerichtshof* ha rigettato il ricorso della *Österreichische Post* avverso l'inibitoria, ma trattenuto la questione inerente al rigetto della domanda di risarcimento. Data però l'esigenza di interpretare la disciplina europea in materia, la Corte suprema austriaca ha deciso di sottoporre alla Corte di giustizia le seguenti questioni pregiudiziali:

i) se la mera violazione del GDPR sia di per sé sola sufficiente a perfezionare il diritto al risarcimento del danno ex art. 82;
ii) se, oltre ai principi di equivalenza ed effettività, il diritto UE contempli altri criteri ai fini della commisurazione del risarcimento;
iii) se il risarcimento possa essere condizionato al riscontro di una determinata soglia di

gravità della lesione e del danno immateriale subito.

Ai quesiti sollevati dal giudice del rinvio, dopo aver argomentato le ragioni per cui l'art. 82 del Regolamento si presenta quale fattispecie di risarcimento "denazionalizzata" (cosicché la disposizione deve interpretarsi alla luce del solo diritto europeo), la Corte ha risposto:

i) che la violazione del GDPR non determina di per sé sola un diritto al risarcimento occorrendo, invece, tre condizioni cumulative: a) la violazione di una norma del GDPR; b) il verificarsi di un danno derivante dalla violazione; e, quindi, c) un nesso causale tra il danno e la violazione;
ii) che, in ragione del principio di effettività, il diritto al risarcimento non può essere riservato ai soli danni immateriali che raggiungono una certa soglia di gravità;
iii) che spetta ai giudici del singolo Stato membro stabilire i criteri che consentono di calcolare l'entità del risarcimento nel rispetto dei principi di equivalenza e di effettività.

La Corte, pertanto, in primo luogo, stabilisce che il diritto al risarcimento ex art. 82 GDPR dipende dalla dimostrata sussistenza di una violazione del GDPR, dalla riscontrata presenza di un danno materiale o immateriale e dall'esistenza di un nesso eziologico tra danno e violazione. Ne risulta che la mera violazione del GDPR non basta a innescare l'obbligazione risarcitoria. Ciò, secondo la Corte lo si desume dallo stesso Regolamento, che nel distinguere (nel prisma delle funzioni) l'azione risarcitoria (compensativa) ex art. 82 da altri strumenti di ricorso previsti dallo stesso GDPR, tra cui quelli, anzitutto, che consentono l'irrogazione (punitiva) di sanzioni amministrative ex artt. 83 e 84 GDPR, solo per la prima pretende la dimostrazione dell'effettiva esistenza di un danno individuale. La Corte rimarca così la funzione (non punitiva, ma) compensativa del diritto al risarcimento previsto dal GDPR, che mira a garantire la riparazione piena ed effettiva del danno patito.

In secondo luogo, la Corte di giustizia afferma che il diritto al risarcimento non è limitato ai danni immateriali che superano una specifica soglia di gravità, atteso che, per un verso, il GDPR non prevede tale requisito; e che, per altro verso, un limite siffatto rischierebbe di compromettere l'uniforme applicazione a livello UE del sistema previsto dal GDPR (posto che una soglia minima di gravità della lesione potrebbe variare a seconda della valutazione effettuata di volta in volta dai giudici nazionali).

Infine, la Corte osserva che il GDPR non contiene disposizioni relative alla valutazione del risarcimento. Ne deriva che, spetta all'ordinamento di ciascun Stato membro stabilire le modalità e i criteri utili a determinare l'ammontare del risarcimento dovuto, fermo restando il rispetto dei principi di equivalenza ed effettività.

La seconda decisione, qui ricordata, del 14 dicembre 2023, pronunciata nella causa C-340/21, attiene all'interpretazione degli artt. 5(2), 24 e 32, nonché dell'art. 82, del GDPR, e riguarda una controversia tra un cittadino bulgaro e la *Natsionalna agentsia za prihodite* (l'Agenzia nazionale bulgara delle entrate) in merito al risarcimento del danno immateriale che il cittadino lamentava aver subito a causa di una presunta violazione da parte dell'Agenzia degli obblighi legali su questa gravanti in qualità di titolare del trattamento dei dati personali. Precisamente, In data 15 luglio 2019, i *media* hanno dato notizia di un attacco *hacker*, a causa del quale i dati personali di circa 6 milioni di persone archiviati nel sistema informatico della *Natsionalna agentsia za prihodite* sono stati resi visibili *online*. In conseguenza alla violazione dei propri dati personali, un cittadino bulgaro ha presentato ricorso all'*Administrativen sad Sofia-grad* al fine di ottenere il risarcimento del danno immateriale sofferto (commisurato nella somma di euro 510). A seguito del rigetto della domanda risarcitoria, il cittadino bulgaro ha adito il *Varhoven administrativen sad* che, data la necessità di interpretare la normativa europea in materia, ha sottoposto alla Corte di giustizia cinque questioni pregiudiziali. E precisamente:

i) se una divulgazione non autorizzata di dati personali (o un accesso non autorizzato) da parte di «terzi» (ex art. 4 n. 10 GDPR) sia di per sé sufficiente a dimostrare che le misure tecniche e organizzative adottate dal titolare del trattamento non risultassero «adeguate» ai sensi degli artt. 24 e 32 GDPR;
ii) se (il solo accesso o la divulgazione non autorizzata dei dati non fossero ritenuti dalla Corte sufficienti a dimostrare l'inadeguatezza delle misure tecniche adottate dal titolare del trattamento, allora se) l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento (ex art. 32 GDPR) debba essere valutata in concreto dai giudici nazionali tenendo conto dei rischi connessi al trattamento;
iii) se il principio di responsabilità del titolare del trattamento ex artt. 5.2 e 24 GDPR (alla luce del 74° Considerando), debba essere interpretato nel senso che, nell'ambito di un'azione di risarcimento ex art. 82 GDPR, al

incomba sul titolare del trattamento l'onere di dimostrare l'adeguatezza delle misure di sicurezza attuate (ai sensi dell'art. 32 GDPR). Nonché, se una perizia giudiziaria possa costituire un mezzo di prova (necessario e) sufficiente a valutare l'adeguatezza delle misure di sicurezza che il titolare del trattamento ha adottato;

iv) se il titolare del trattamento possa ritenersi esonerato dall' obbligo di risarcire il danno (ex art. 82(3) GDPR) per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di «terzi» (ex art. 4 n. 10 GDPR);

v) se il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento possa, di per sé, costituire un "danno immateriale", ai sensi dell'art. 82 GDPR.

Ai quesiti sollevati dal giudice del rinvio la Corte ha risposto:

i) che, gli artt. 24 e 32 GDPR devono essere interpretati nel senso per cui una divulgazione non autorizzata di dati personali (o un accesso non autorizzato) da parte di «terzi» (ex art. 4 n. 10 GDPR), non sono di per sé sufficienti a dimostrare che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero "adeguate;

ii) che, l'art. 32 GDPR dev'essere interpretato nel senso che l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento dev'essere valutata dai giudici nazionali in concreto, tenendo conto dei rischi connessi al trattamento di cui trattasi e valutando se la natura, il contenuto e l'attuazione di tali misure siano adeguati a tali rischi;

iii) che il principio di responsabilità del titolare del trattamento, enunciato all'art. 5(2) e concretizzato all'art. 24 del Regolamento, deve interpretarsi nel senso che nell'ambito di un'azione di risarcimento fondata sull'articolo 82 GDPR, al titolare del trattamento di cui trattasi incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'arti. 32 GDPR; e che quest'ultima disposizione e il principio di effettività del diritto dell'Unione devono essere interpretati nel senso per cui, al fine di valutare l'adeguatezza delle misure di sicurezza che il titolare del trattamento ha attuato, una perizia giudiziaria non può costituire un mezzo di prova sistematicamente necessario e sufficiente;

iv) che l'art. 82(3) GDPR deve essere interpretato nel senso che il titolare del trattamento non può essere esonerato dall'obbligo di risarcire il danno subito da una persona per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di «terzi» (ai sensi dell'art. 4 n. 10 GDPR), atteso che in tale evenienza il responsabile deve dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile;

v) che l'art. 82(1) GDPR deve essere interpretato nel senso che, a seguito di una violazione del Regolamento, il timore di un potenziale utilizzo abusivo da parte dell'interessato dei suoi dati personali da parte di terzi può, di per sé, costituire un «danno immateriale».

Con questa decisione, la Corte, dopo aver rammentato che le disposizioni di cui agli artt. 24 e 32 GDPR si limitano ad imporre al titolare del trattamento l'adozione di misure tecniche e organizzative destinate (per quanto possibile) ad evitare la violazione dei dati personali, ha evidenziato che l'adeguatezza deve valutarsi in concreto esaminando se le misure siano state adottate tenendo conto di volta in volta delle esigenze di protezione dei dati inerenti al trattamento, così come dei rischi indotti nel caso di specie. Dette norme non possono, quindi, essere intese nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato da parte di un terzo siano sufficienti a rivelare che le misure adottate dal titolare del trattamento non fossero appropriate, senza consentire a quest'ultimo di fornire prova contraria. L'art. 24 GDPR, difatti, prevede espressamente che il titolare del trattamento possa dimostrare la conformità al Regolamento delle misure attuate, possibilità di cui sarebbe privato qualora la presunzione fosse da ritenersi *iuris et de iure* (atteso che, com'è noto, la presunzione assoluta opera già sul piano della fattispecie astratta).

La Corte, inoltre, ha affermato che l'adeguatezza delle misure tecniche e organizzative adottate dal titolare del trattamento deve valutarsi in due momenti distinti. Precisamente: in un primo momento, occorre mettere a fuoco in concreto i possibili rischi derivanti dalla violazione dei dati personali, nonché le eventuali conseguenze per i diritti e le libertà delle persone fisiche, soppesando il grado di probabilità (e di gravità) dei rischi individuati; per poi, in un secondo momento,

verificare se le misure attuate siano adeguate rispetto a tali rischi, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, della portata, del contesto e delle finalità del trattamento (cfr. art. 25 GDPR). Pertanto, secondo la Corte, se da un canto, il titolare del trattamento dispone di un certo margine di discrezionalità nel selezionare le misure tecniche e organizzative adeguate al rischio (ex art. 32(1) GDPR), d'altro canto, un giudice domestico deve poter valutare la complessa ponderazione effettuata dal titolare del trattamento e, così, accertare che le misure adottate siano idonee a garantire al livello di sicurezza preteso dalla disciplina del GDPR, tenendo conto delle circostanze del caso concreto nonché degli elementi di prova di cui dispone.

La Corte, attraverso una lettura sistematica degli artt. 5(2), 24(1) e 32(1) GDPR, evidenzia poi che grava sul titolare del trattamento l'onere di provare che i dati personali sono trattati in modo tale da assicurare un adeguato grado di sicurezza rispetto al rischio. Queste disposizioni stabiliscono una regola di applicazione generale, dunque, che in mancanza di indicazione contraria nel GDPR, occorre applicare anche nell'ambito di un'azione di risarcimento ex art. 82 GDPR.

Più nel dettaglio, la Corte osserva che il Regolamento non prevede norme inerenti all'ammissione e al valore probatorio di un mezzo di prova (qual è, ad es., una perizia giudiziaria), che devono essere applicate dai giudici nazionali investiti di un'azione di risarcimento danni ex art. 82 GDPR. Ne risulta che, in assenza di norme eurounitarie sul punto, è compito del singolo Stato Membro stabilire le modalità utili a garantire la tutela dei diritti spettanti ai singoli in ragione dell'art. 82 GDPR e, in particolare, la disciplina relativa ai mezzi di prova che consentono di valutare l'adeguatezza delle misure tecniche e organizzative adottate dal titolare (o responsabile) del trattamento, sebbene, pur sempre nel rispetto dei principi di equivalenza e di effettività. Sicché, una norma procedurale nazionale sulla scorta della quale risultasse imprescindibile per i giudici nazionali disporre di una perizia giudiziaria potrebbe contrastare con il principio di effettività. Così ad esempio, secondo la Corte, il ricorso sistematico ad una perizia giudiziaria potrebbe rivelarsi superfluo là dove si riscontrasse la presenza di altre prove detenute dal giudice adito, come le risultanze di un controllo circa il rispetto delle misure di protezione dei dati personali effettuato da un'Autorità indipendente.

Secondo la Corte, poi, la disposizione di cui all'art. 82(3) GDPR in linea di principio significa: che il responsabile del trattamento deve risarcire il danno causato da una violazione del GDPR connessa al trattamento; e che, questi può essere esonerato dalla responsabilità solo se fornisce prova che il fatto che ha cagionato il danno non gli sia in alcun modo imputabile. Ne risulta che, quando una violazione di dati personali sia stata commessa da criminali informatici (ossia da "terzi" ex art. 4 n. 10 GDPR), la violazione non può essere imputata al titolare del trattamento, a meno che quest'ultimo non l'abbia resa possibile trasgredendo ad un obbligo (ad es. ex artt. 24 e 32) previsto dal Regolamento medesimo.

Infine, la Corte (in linea con quanto affermato nella decisione del 4 maggio 2023 C-300/21 già menzionata) osserva che l'esistenza di un danno subito rappresenta una tra le condizioni necessarie al sorgere del diritto al risarcimento ex art. 82(1) GDPR (cumulativamente con l'esistenza di una violazione del Regolamento e di un nesso di causa tra danno e violazione). Secondo la Corte la disposizione in parola osta ad una norma o a una prassi nazionale che subordini il risarcimento del danno immateriale alla condizione che la lesione subita dall'interessato abbia raggiunto un certo soglia di gravità. Segnatamente, l'art. 82(1) GDPR non distingue tra fattispecie in cui, a seguito di una violazione accertata del Regolamento, il danno immateriale lamentato dall'interessato risulti collegato: ad un utilizzo abusivo da parte di terzi dei suoi dati personali che si è già verificato alla data della domanda di risarcimento; oppure, alla paura percepita dall'interessato che un utilizzo abusivo dei suoi dati possa verificarsi in futuro. Dalla formulazione della norma, pertanto, non può escludersi che la nozione di "danno immateriale" comprenda una situazione in cui l'interessato invoca, al fine di ottenere un risarcimento ex art. 82 GDPR, il timore che i suoi dati personali siano oggetto di un futuro utilizzo abusivo da parte di terzi, a causa della violazione del Regolamento già avveratasi.

GIORGIO REMOTTI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62021CJ0300

2023/4(23)VR

23. La sentenza CGUE nel caso C-683/21 sulla rilevanza dell'elemento soggettivo nella violazione del GDPR ai fini della sanzione amministrativa pecuniaria

Il 5 dicembre 2023 la Grande Sezione della Corte di Giustizia, in sede di pregiudiziale interpretativa *ex*

art. 267 TFUE, ha reso un'importante sentenza nella causa C-683/21 in merito alle condizioni sostanziali per l'irrogazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 regolamento (UE) 679/2016 (di seguito **GDPR** o il **Regolamento**).

Il caso.

Il 24 marzo 2020, a seguito del divampare della pandemia da COVID-19, il Ministro della Sanità della Repubblica di Lituania incaricava il Centro nazionale per la sanità pubblica istituito presso lo stesso (di seguito **CNSP**) di disporre l'acquisizione immediata di un sistema informatico finalizzato alla registrazione e al monitoraggio dei dati delle persone esposte al virus.

Successivamente, una persona qualificatasi come rappresentante del **CNSP**, comunicava alla società UAB «IT sprendimai sėkmei» (di seguito **ITSS**) che la ITSS era stata selezionata dal CNSP per sviluppare un'applicazione mobile, fornendo altresì indicazioni circa le caratteristiche attese dal software. Al momento della creazione di quest'ultimo, veniva inoltre elaborata una *privacy policy* che designava la ITSS e il CNSP come responsabili del trattamento. L'applicazione (la cui interfaccia menzionava ambo i soggetti) si rendeva disponibile su Google Play Store e Apple App Store nell'aprile del 2020 e rimaneva operativa fino al 26 maggio 2020. In quest'arco di tempo, essa veniva scaricata e utilizzata da 3802 persone, le quali fornivano i dati personali richiesti, quali, ad esempio: tipologia e numero del documento di identità, nome, cognome, numero di telefono, paese di nascita, indirizzo, codice postale.

Il 10 aprile 2020, il Ministro della Sanità lituano affidava al direttore del CNSP il compito di organizzare l'acquisizione del software in questione ai sensi dell'art. 72, par. 2 della legge lituana in materia di appalti pubblici. Il procedimento, tuttavia, non conduceva ad alcuna aggiudicazione, in guisa che nessun rapporto contrattuale veniva a perfezionarsi tra la società e l'Amministrazione. Infatti, il 4 giugno 2020 il CNSP rappresentava alla società che, a causa del mancato finanziamento dell'operazione acquisitiva, si poneva fine alla suddetta procedura.

Nell'ambito di un'indagine avviata il 18 maggio 2020, l'Ispettorato nazionale per la protezione dei dati della Repubblica di Lituania (di seguito **INPD**) accertava che mediante la menzionata applicazione mobile erano stati raccolti numerosi dati personali. Più precisamente, si rilevava che diversi utenti avevano scelto tale strumento come metodo di monitoraggio dell'isolamento reso obbligatorio per legge a fini di contrasto della pandemia da COVID-19, rispondendo alle domande ivi formulate e fornendo conseguentemente informazioni relative, in particolare, al proprio stato di salute e al rispetto delle condizioni di isolamento. Pertanto, con decisione del 24 febbraio 2021, l'INPD comminava al CNSP una sanzione amministrativa pecuniaria di euro 12.000 ai sensi dell'art. 83 GPDR per violazione degli artt. 5, 13, 24, 32 e 35 del Regolamento. Con tale decisione veniva altresì inflitta una sanzione amministrativa pecuniaria di euro 3.000 alla ITSS in qualità di contitolare del trattamento.

Il CNSP impugnava il provvedimento dinanzi al Tribunale amministrativo regionale di Vilnius, sostenendo che solo la ITSS doveva tecnicamente qualificarsi come titolare del trattamento ai sensi dell'art. 4, n. 7 GPDR. La controinteressata ITSS, dal canto suo, replicava di aver agito in qualità di responsabile del trattamento, ai sensi dell'art. 4, n. 8 GPDR, avendo effettuato il trattamento dei dati su istruzione – e dunque per conto – del CNSP, unico titolare dello stesso.

Il giudice del rinvio, nel ricostruire i fatti di causa, premetteva che la creazione dell'applicazione mobile mirava ad attuare l'obiettivo istituzionale del CNSP di gestione della pandemia da COVID-19. Pertanto, il trattamento dei dati personali era previsto a tale fine. Per contro, la ITSS non era intesa perseguire altro scopo oltre a quello lucrativo consistente nella remunerazione per la cessione del prodotto informatico. Inoltre, il Tribunale rilevava che il CNSP aveva fornito indicazioni sulle caratteristiche attese dall'applicazione e, massimamente, sui quesiti da porre agli utenti ai fini del monitoraggio epidemiologico. Tuttavia, emergeva l'inesistenza di un contratto di appalto pubblico tra le parti. Non solo. L'istruttoria evidenziava come il CNSP non avesse acconsentito né altrimenti autorizzato la messa a disposizione del software sui vari negozi online.

Infine, il giudice del rinvio osservava che, durante l'indagine dell'INPD, veniva accertato che la società Juvare Lithuania, amministratrice del sistema informatico di monitoraggio e controllo delle malattie trasmissibili con rischio di propagazione, doveva ricevere le copie dei dati personali raccolti dall'applicazione mobile in questione. Inoltre, al fine di testare quest'ultima, erano stati utilizzati dati fittizi, ad eccezione dei numeri di telefono dei dipendenti di detta società.

Alla luce delle illustrate acquisizioni, il Tribunale sospendeva il processo e sottoponeva alla Corte di Giustizia le seguenti questioni pregiudiziali: 1) se la nozione di «titolare del trattamento» di cui all'art. 4, n. 7 GPDR possa interpretarsi nel senso che deve essere considerato quale titolare del trattamento anche colui che intenda acquistare uno strumento di raccolta di dati mediante appalto pubblico,

nonostante non sia stato concluso un contratto di appalto pubblico e il prodotto creato (applicazione mobile) non sia stato trasferito; 2) se la nozione di «titolare del trattamento» di cui all'art. 4, n. 7 GPDR possa interpretarsi nel senso che deve qualificarsi come tale anche un'amministrazione aggiudicatrice che non ha acquistato il diritto di proprietà sul prodotto informatico creato e che non ne è venuta in possesso, qualora la versione definitiva dell'applicazione creata fornisca link o interfacce a tale ente pubblico e/o l'informativa sulla riservatezza, non ufficialmente approvata o riconosciuta dall'ente pubblico in questione, indichi quest'ultimo quale titolare del trattamento; 3) se la nozione di «titolare del trattamento» di cui all'art. 4, n. 7 GPDR possa interpretarsi nel senso che deve essere considerato quale titolare del trattamento anche colui che non ha effettivamente compiuto alcuna operazione di trattamento di dati, come definita all'art. 4, n. 2 GDPR e/o che non ha dato un'autorizzazione o un consenso chiari al compimento di tali operazioni; se il fatto che il prodotto informatico utilizzato per il trattamento sia stato creato conformemente alle indicazioni dettate dall'amministrazione aggiudicatrice sia rilevante per l'interpretazione della nozione di «titolare del trattamento»; 4) qualora la determinazione delle effettive operazioni di trattamento dei dati sia rilevante per l'interpretazione della nozione di «titolare del trattamento», se la definizione di «trattamento» ai sensi dell'art. 4, n. 2 GPDR debba intendersi nel senso di ricomprendere anche ipotesi di impiego di copie di dati personali per testare i sistemi informatici; 5) se la contitolarità del trattamento dei dati ai sensi dell'art. 4, n. 7 e dell'art. 26, par. 1 GDPR possa interpretarsi esclusivamente nel senso che implica azioni deliberatamente coordinate circa la determinazione della finalità e dei mezzi del trattamento o se tale nozione possa intendersi anche nel senso che la contitolarità ricomprende altresì situazioni in cui manca un chiaro "accordo" al riguardo e/o non vi è coordinamento fra le azioni dei soggetti. Se, ai fini dell'interpretazione della nozione di contitolarità del trattamento dei dati personali, siano giuridicamente rilevanti le circostanze relative alla fase della creazione dei mezzi per il trattamento dei dati personali (applicazione informatica) nella quale sono stati trattati i dati personali e alle finalità della creazione dell'applicazione. Se un "accordo" tra i contitolari possa essere inteso esclusivamente come una predeterminazione chiara e definita delle condizioni che regolano la contitolarità del trattamento dei dati; 6) se la disposizione di cui all'art. 83, par. 1 GDPR secondo cui «le sanzioni amministrative pecuniarie [devono essere] effettive, proporzionate e dissuasive» debba interpretarsi nel senso di ritenere responsabile il «titolare del trattamento» anche quando, nel processo di creazione di un prodotto informatico, lo sviluppatore effettua azioni di trattamento dei dati personali; se le operazioni di trattamento improprie eseguite dal responsabile del trattamento comportino sempre e automaticamente una responsabilità giuridica in capo al titolare dello stesso; se tale disposizione debba ricomprende anche i casi di responsabilità oggettiva del titolare del trattamento.

Le questioni pregiudiziali.

Sulle questioni prima, seconda e terza.

La Corte di Giustizia ha esaminato congiuntamente le questioni prima, seconda e terza, che convocavano a vario titolo l'esatta determinazione della nozione legale di «titolare del trattamento» ai sensi dell'art. 4, n. 7 GDPR. Quest'ultima definisce «titolare del trattamento» «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali». L'ampiezza della formulazione normativa assolve l'obiettivo, ben evidenziato dai Considerando nn. 74 e 79 GDPR, di assicurare un'efficace tutela dei diritti e delle libertà fondamentali delle persone fisiche. In quest'ottica, la giurisprudenza europea ha da tempo chiarito che qualsiasi persona fisica o giuridica che influisca, per fini propri, su operazioni di trattamento partecipando alla determinazione delle finalità e dei mezzi di quest'ultimo può essere considerata titolare di detto trattamento. Ne viene che non devono ritenersi necessarie a tal fine né la predeterminazione delle finalità o dei mezzi mediante orientamenti scritti o istruzioni, né la formale designazione di un soggetto come «titolare del trattamento».

Ebbene, nel caso di specie risultava che la creazione dell'applicazione mobile era stata commissionata dal CNSP e mirava a realizzare il suo scopo istituzionale di gestione della pandemia da COVID-19. Inoltre, veniva accertato che i parametri di tale applicazione, quali i quesiti da porre all'utenza e la loro formulazione, erano stati adattati alle esigenze del CNSP, che aveva ricoperto un ruolo attivo nella loro definizione. Alla luce di ciò, doveva ritenersi che il CNSP avesse effettivamente partecipato alla determinazione delle finalità e dei mezzi del trattamento. In ogni caso, le circostanze che il CNSP non trattava direttamente alcun dato personale, che non esisteva alcun contratto tra CNSP e ITSS e che il CNSP non aveva acquistato il software né autorizzato la sua distribuzione nei negozi online non ostavano alla qualifica di

quest'ultimo come «titolare del trattamento» ai sensi dell'art. 4, n. 7 GDPR.
Sulla scorta di tali rilievi, la Corte ha dichiarato che l'art. 4, n. 7 GPDR deve interpretarsi nel senso che può essere tecnicamente considerato «titolare del trattamento» un ente che abbia incaricato un'impresa di sviluppare un'applicazione informatica mobile partecipando alla determinazione delle finalità e dei mezzi del trattamento dei dati personali effettuato mediante essa. Non rileva, a tal fine, che tale ente non abbia proceduto direttamente a operazioni di trattamento, non abbia fornito esplicito consenso al trattamento effettuato da terzi o alla messa a disposizione del pubblico dell'applicazione mobile e non abbia acquisito la proprietà della stessa. L'unica circostanza ostativa alla qualificazione di «titolare del trattamento» nel caso di specie sarebbe stata una previa ed esplicita opposizione alla messa a disposizione nei confronti del pubblico dell'applicazione e al conseguente trattamento, dal momento che, in quest'ipotesi, quest'ultimo non avrebbe potuto ritenersi effettuato per conto dell'ente. Spetta, tuttavia, al giudice del merito verificare tale circostanza.
Sulla quinta questione.
La quinta questione concerneva la qualificazione di due enti come contitolari del trattamento.
Come rilevato dall'Avvocato Generale al par. 38 delle sue conclusioni, la partecipazione alla determinazione delle finalità e dei mezzi del trattamento può assumere forme diverse, potendo risultare sia da una decisione comune sia da determinazioni convergenti. In quest'ultimo caso, è necessario che dette decisioni si integrino, in modo che ciascuna incida concretamente sulla determinazione delle finalità e dei mezzi del trattamento. Il dato normativo, pertanto, non esige necessariamente un accordo formale tra tali titolari del trattamento.
Beninteso, ai sensi dell'art. 26, par. 1 GPDR, letto alla luce del Considerando n. 79, i contitolari del trattamento devono, mediante accordo tra loro, definire in modo trasparente i loro rispettivi obblighi al fine di garantire il rispetto dei requisiti di tale regolamento. Tuttavia, il perfezionamento di tale accordo costituisce non già una condizione per l'acquisto di tale qualificazione, bensì un obbligo successivo imposto a soggetti già qualificati come contitolari del trattamento.
Pertanto, la Corte ha concluso che gli artt. 4, n. 7 e 26, par. 1 GDPR devono essere interpretati nel senso che la qualificazione di due enti come contitolari del trattamento non presuppone un previo accordo formale tra essi, né sulla determinazione delle finalità e dei mezzi del trattamento, né sulle condizioni di tale contitolarità.
Sulla quarta questione.
Con la quarta questione, in estrema sintesi, si chiedeva se l'uso di dati personali a fini di test informatici di un'applicazione mobile potesse ricomprendersi nella nozione di «trattamento» ai sensi dell'art. 4, n. 2 GDPR. Nel caso di specie, come si è detto, la società lituana che gestiva il sistema informatico di monitoraggio e controllo delle malattie trasmissibili con rischio di propagazione doveva ricevere le copie dei dati raccolti dal software in questione. Per i test informatici, venivano utilizzati dati fittizi, ad eccezione dei numeri di telefono dei dipendenti di detta società.
Orbene, la nozione di «trattamento» fissata dall'art. 4, n. 2 GDPR – *i.e.* «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali» – è sì ampia da rendere irrilevanti le ragioni a fondamento della concreta operazione. Di poi, l'elencazione ivi fornita deve intendersi come un insieme aperto di ipotesi rese a fini esemplificativi e dunque non tassativo. Pertanto, non rileva ai fini della qualificazione di una data operazione come «trattamento» ai sensi dell'art. 4, n. 2 GDPR che i dati personali siano stati utilizzati per eseguire test informatici.
Nondimeno, intanto un'operazione può qualificarsi come «trattamento» in quanto abbia a oggetto «dati personali», secondo l'ampia nozione fornita dall'art. 4, n. 1 GDPR. Alla luce di quest'ultima, non è da ostacolo il fatto che si tratti di «copie di dati personali», laddove esse contengano effettivamente informazioni riferibili a una persona fisica identificata o identificabile. In ogni caso, esulano certamente dalla nozione legale di dato personale i dati fittizi, riferendosi quest'ultimi a una persona che non esiste nella realtà. Lo stesso deve dirsi per i dati anonimi o resi tali, mentre vi rientrano i dati oggetto di pseudonimizzazione (cfr. art. 4, n. 5 e Considerando n. 26 GDPR).
Pertanto, l'uso di dati personali a fini di test informatici di un'applicazione mobile deve qualificarsi come «trattamento» ai sensi dell'art. 4, n. 2 GDPR, salvo che tali dati siano stati resi anonimi in modo da impedire o da non consentire più l'identificazione dell'interessato o che si tratti di dati fittizi che non si riferiscono a una persona fisica esistente.
Sulla sesta questione
La sesta questione interrogava la Corte di Giustizia sulle condizioni sostanziali e sulla latitudine delle fattispecie sanzionatorie di cui all'art. 83 GDPR. Rispettivamente, il giudice del rinvio chiedeva: se

tale disposizione dovesse intendersi nel senso di esigere la commissione delle violazioni di cui ai parr. da 4 a 6 a titolo di dolo o colpa; se la sanzione potesse comminarsi a un titolare del trattamento per operazioni effettuate per suo conto da un responsabile del trattamento.

Più in dettaglio, il primo nodo interpretativo convocava la rilevanza dell'elemento soggettivo nelle violazioni della normativa europea in materia di protezione dei dati personali e il margine di discrezionalità che essa lascia, sul punto, agli Stati membri.

Ebbene, il dato letterale dell'art. 83 GDPR fornisce al riguardo le seguenti indicazioni: 1) le Autorità di controllo nazionali debbono provvedere affinché le sanzioni amministrative pecuniarie siano effettive, proporzionate e dissuasive; 2) nel comminare le stesse «si tiene in debito conto […] del carattere doloso o colposo della violazione»; 3) ai sensi del par. 7, «ogni Stato membro può prevedere norme che stabiliscano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici stabiliti in tale Stato membro»; 4) ai sensi del par. 8, in combinato disposto col Considerando n. 129, «l'esercizio, da parte dell'autorità di controllo, dei poteri attribuitile da tale articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo».

Dai suddetti indici testuali, e massimamente dal rilievo che nel comminare le stesse «si tiene in debito conto […] il carattere doloso o colposo della violazione», la parte attrice inferiva che la norma non richiede necessariamente una violazione commessa a titolo di dolo o colpa, lasciando agli Stati membri un certo margine di discrezionalità nella determinazione dei relativi presupposti sostanziali. In altri termini, la ricostruzione offerta dal ricorrente pareva procedere nel senso che l'elemento soggettivo fosse da intendere come un necessario oggetto di indagine da parte dell'Autorità di controllo ma non anche come un indefettibile coefficiente di imputazione.

La Corte di Giustizia ha rifiutato siffatta interpretazione.

Nel merito, seppur non v'è dubbio che anche le fonti derivate ad efficacia diretta – qual è GDPR – possano richiedere, per la loro compiuta attuazione, misure domestiche di stretta applicazione, nulla nella formulazione dell'art. 83, parr. da 1 a 6 GDPR consente di ritenere che il legislatore europeo abbia inteso lasciare agli Stati membri un margine di discrezionalità in merito alle condizioni sostanziali di irrogazione delle sanzioni amministrative pecuniarie. In altri termini, anche al fine di assicurare «un livello coerente ed elevato di protezione delle persone fisiche» (Considerando 10 GDPR) e «il medesimo livello di […] obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento» (Considerando 13 GDPR), deve ritenersi che la normativa europea abbia assunto il monopolio disciplinare sui presupposti delle violazioni al GDPR, predeterminando compiutamente gli elementi delle fattispecie sanzionabili.

Soccorre in proposito anzitutto l'argomentazione *a contrario*. Il GDPR, come si è detto, consente agli Stati membri di stabilire eccezioni in relazione alle autorità pubbliche e agli organismi pubblici stabiliti nel loro territorio (art. 83(7) GDPR) e regole procedurali per l'irrogazione delle sanzioni (art. 83(8) GDPR). Ne viene logicamente un'assenza di discrezionalità nella determinazione dei presupposti sostanziali di responsabilità dei titolari dei trattamenti. Non solo. L'art. 84(1) GDPR attribuisce espressamene agli Stati membri la competenza a stabilire «le norme relative alle altre sanzioni per le violazioni» del Regolamento, «in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83». Ne deriva che le legislazioni nazionali non sono ammesse a fissare gli elementi costitutivi delle fattispecie sanzionabili a norma dell'art. 83 GDPR, che rientrano pertanto unicamente nell'ambito del diritto dell'Unione. Ciò è confermato altresì dalla formulazione dell'art. 83(2) GPDR, da cui emerge che solo le violazioni commesse colpevolmente dal titolare del trattamento possono condurre all'irrogazione di una sanzione amministrativa pecuniaria.

Soccorrono, infine, secondo la CGUE, ragioni di ordine sistematico. La Corte ha precisato che l'economia generale e la finalità del GPDR corroborano la necessità dell'elemento soggettivo. Non v'è dubbio che un acconcio apparato sanzionatorio produca, in chiave di *public enforcement*, un incentivo per i titolari e i responsabili del trattamento a conformarsi alle prescrizioni di legge. Per il loro effetto dissuasivo, infatti, le sanzioni amministrative pecuniarie contribuiscono a rafforzare la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali e costituiscono quindi un elemento chiave per garantire un livello elevato di protezione. Tuttavia, tale ultimo obiettivo deve coordinarsi con le ulteriori istanze enunciate nel Preambolo del Regolamento. In particolare: il Considerando 10 GDPR impone un canone di coerenza ed omogeneità della normativa europea in materia *data protection*; analogamente, i Considerando 11 e 129 GDPR prescrivono un'applicazione coerente di tale

disciplina, richiedendo che le autorità competenti dispongano di poteri equivalenti di sorveglianza e controllo e di comminazione di sanzioni altrettanto equivalenti. Ebbene, come già evidenziato, l'uniformità e l'effettività della protezione dei dati personali a livello europeo verrebbe gravemente frustrata dalla possibilità per gli Stati membri di prevedere regimi sanzionatori differenziati. Quest'ultimi sarebbero infatti fatalmente alterativi del gioco concorrenziale all'interno dell'Unione, in contrasto con gli obiettivi espressi, in particolare, ai Considerando 9 e 13 GDPR.
Di conseguenza, la Corte ha concluso che l'art. 83 GDPR non consente di irrogare una sanzione amministrativa pecuniaria senza la prova che la violazione sia stata commessa con dolo o colpa dal titolare del trattamento. Ai fini di tale accertamento, merita precisare che un titolare del trattamento può essere sanzionato allorché esso non poteva ignorare il carattere illecito del suo comportamento, a prescindere dalla sua consapevolezza o meno di violare le disposizioni del GPDR. Inoltre, qualora questi sia una persona giuridica, l'applicazione dell'art. 83 GDPR non presuppone un'azione e neppure una conoscenza dell'organo di gestione di tale persona giuridica.
L'ultimo quesito riguardava la sanzionabilità di un titolare del trattamento per operazioni effettuate da un responsabile del trattamento. Il punto è sciolto dalla Corte mediante la lettura congiunta delle disposizioni che seguono. L'art. 4, n. 7 GDPR annoda la qualifica di «titolare del trattamento» alla concreta determinazione, singolarmente o insieme ad altri, delle finalità e dei mezzi del trattamento. Il Considerando 74 GDPR chiarisce che «è opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto». Infine, ai sensi dell'art. 4, n. 8 GDPR si definisce responsabile del trattamento «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento». Al quesito in analisi non può che darsi, dunque, risposta positiva, dichiarando che l'art. 83 GDPR deve interpretarsi nel senso che una sanzione amministrativa pecuniaria può essere inflitta a un titolare del trattamento in relazione a operazioni effettuate per suo conto da un responsabile del trattamento.
Tuttavia, tale responsabilità non può estendersi alle situazioni in cui il responsabile ha trattato dati personali per finalità proprie o in modo incompatibile con il quadro o le modalità del trattamento determinate dal titolare dello stesso ovvero in modo tale da non potersi ragionevolmente ritenere che quest'ultimo vi abbia acconsentito. Infatti, conformemente all'art. 28(10) GDPR, in un'ipotesi del genere tale soggetto deve qualificarsi come titolare di quello specifico trattamento.

VALENTINO RAVAGNANI

https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62021CJ0683

2023/4(24)EMI

24. La sentenza CGUE nel caso C-307/22 in materia di accesso, copia e trattamento di dati sanitari

La Corte di Giustizia dell'Unione europea (di seguito la **Corte** o **CGUE**), con sentenza del 26 ottobre 2023 nel caso C-307/22 (di seguito la **Sentenza**), si è espressa in merito al diritto del paziente di ricevere gratuitamente una copia della cartella medica da parte del medico.
La pronuncia in esame riguarda un paziente che, dopo aver ricevuto cure dentistiche e sospettando che ci fossero errori nel trattamento medico a lui riservato, richiedeva la consegna, a titolo gratuito, di una prima copia della propria cartella medica. Il medico rispondeva favorevolmente alla richiesta così presentata alla sola condizione che il paziente si facesse carico delle spese connesse alla fornitura della copia della cartella medica, come previsto dal diritto nazionale tedesco.
Per queste ragioni, il paziente proponeva ricorso presso il Tribunale di primo grado tedesco, richiedendo di ottenere, a titolo gratuito, una prima copia della sua cartella medica. Sia in primo grado sia in appello, veniva accolta la domanda del paziente sulla base dell'interpretazione della normativa nazionale applicabile alla luce dell'art. 12, par. 5, nonché dell'art. 15, par. 1 e 3, del regolamento (UE) 2016/679 (di seguito **GDPR** o il **Regolamento**).
Il medico, allora, ricorreva presso la Corte federale di giustizia tedesca, proponendo ricorso di revisione. La Corte federale, ritenendo determinante nel caso di specie l'interpretazione della disciplina contenuta nel GDPR, rimetteva la questione alla Corte di giustizia europea per una pronuncia pregiudiziale.
Infatti, in virtù del codice civile tedesco (BGB), l'art. 630g, par. 2 prevede che il paziente debba rimborsare al professionista sanitario i costi sostenuti per ottenere una copia della propria cartella medica. È previsto un regime tariffario il

cui fine principale è quello di tutelare gli interessi economici dei professionisti sanitari.
Tuttavia, in contrapposizione a tale disposizione ed alla luce del combinato disposto degli artt. 15, par. 3 e l'art. 12, par. 5, prima frase, del GDPR, potrebbe sostenersi che il titolare del trattamento, nel caso di specie il medico, sia tenuto a trasmettere al paziente una prima copia della sua cartella medica a titolo gratuito.
Inoltre, il giudice del rinvio rilevava che lo scopo perseguito dal paziente - verificare l'esistenza di errori terapeutici - fosse estraneo alla impostazione contenuta all'interno considerando 63 del GDPR, che prevede il diritto di accedere ai dati personali per essere consapevole del trattamento di tali dati e verificarne la liceità.
Per tali ragioni, Corte federale di giustizia tedesca pone tre differenti questioni pregiudiziali alla CGUE.
Con la prima questione, il giudice del rinvio chiede se l'art. 12, par. 5, e l'art. 15, par. 1 e 3, del GDPR debbano essere interpretati nel senso che l'obbligo di fornire all'interessato, a titolo gratuito, una prima copia dei suoi dati personali oggetto di trattamento grava sul titolare del trattamento, anche qualora tale richiesta sia motivata da uno scopo estraneo a quelli di cui al considerando 63, prima frase, di tale regolamento.
A tal riguardo, la CGUE stabilisce che gli articoli ora citati devono essere interpretati nel senso che l'obbligo di fornire all'interessato, a titolo gratuito, una prima copia dei suoi dati personali oggetto di trattamento grava sul titolare del trattamento anche qualora tale richiesta sia motivata da uno scopo estraneo a quelli di cui al considerando 63 del GDPR. I due articoli, difatti, non subordinano la fornitura a titolo gratuito di una prima copia dei dati personali alla presenza di motivi giustificativi, diretti a supportare le richieste degli interessati, né, tantomeno, il titolare del trattamento ha la facoltà di richiedere i motivi della domanda di accesso.
La seconda questione, invece, affronta il problema della possibile interpretazione dell'art. 23, par. 1, lett. i), del GDPR nel senso che esso autorizza una normativa nazionale - adottata prima dell'entrata in vigore del GDPR - che, al fine di tutelare gli interessi economici del titolare del trattamento, pone a carico dell'interessato le spese di una prima copia dei suoi dati personali oggetto del trattamento.
A tal proposito, la Corte osserva preliminarmente che il diritto riconosciuto all'interessato di ottenere una prima copia a titolo gratuito dei suoi dati personali oggetto di trattamento non è assoluto.
Nel caso in esame, il sistema tariffario previsto dal BGB a favore dei professionisti sanitari induce a scoraggiare i pazienti dalla richiesta di accesso contraddicendo il principio di gratuità della prima copia, così come espresso dalla disciplina europea. Esso, inoltre, si contrappone anche alla *ratio* dell'art. 15, par. 1, del GDPR e riduce enormemente il suo campo applicativo.
Dunque, in merito alla seconda questione la Corte afferma che l'art. 23, par. 1, lett. i), del GDPR deve essere interpretato nel senso che una normativa nazionale adottata prima dell'entrata in vigore di tale regolamento può rientrare nell'ambito di applicazione di detta disposizione. Come si legge nella sentenza, una simile facoltà non consente di adottare una normativa nazionale che, al fine di tutelare gli interessi economici del titolare del trattamento, ponga a carico dell'interessato le spese di una prima copia dei suoi dati personali oggetto di tale trattamento.
Infine, con la terza questione il giudice del rinvio chiede se l'articolo 15, par. 3, prima frase, del GDPR debba essere interpretato nel senso che, nell'ambito di un rapporto medico/paziente, il diritto di ottenere una copia dei dati personali oggetto di trattamento implica che sia consegnata all'interessato una copia integrale dei documenti contenuti nella sua cartella medica e che contengono i suoi dati personali o soltanto una copia dei dati in quanto tali.
La Corte, sul punto, stabilisce che esso deve essere interpretato nel senso che nell'ambito di un rapporto medico/paziente, il diritto di ottenere una copia dei dati personali oggetto di trattamento implica che sia consegnata all'interessato una riproduzione fedele e intelligibile dell'insieme dei dati. Tale diritto presuppone, quindi, quello di ottenere la copia integrale dei documenti contenuti nella sua cartella medica che contengano, tra l'altro, questi dati, anche nel caso in cui la fornitura della copia sia necessaria per consentire al paziente di verificarne l'esattezza e la completezza nonché per garantirne l'intelligibilità. Inoltre, per quanto riguarda i dati relativi alla salute dell'interessato, un simile diritto comprende sempre quello di ottenere una copia dei dati della sua cartella medica contenente informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati al paziente.
Alla luce delle ricostruzioni e motivazioni della CGUE, la pronuncia in esame ha il merito di fare chiarezza sulla portata applicativa del GDPR in relazione al diritto di ogni paziente di poter ricevere gratuitamente copia della propria cartella clinica, anche laddove, come nel caso di specie, dovesse sussistere una normativa nazionale precedente e contrastante.

ENZO MARIA INCUTTI

https://curia.europa.eu/juris/document/document.jsf?text=&docid=279125&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=3549717

2023/4(25)EG

25. Le sentenze dei Tribunali di Pordenone e Udine sulla medicina di iniziativa contro le sanzioni del Garante privacy

Con **Delibera n. 1737** del 20 novembre 2020 la Regione Friuli-Venezia Giulia (di seguito, la "**Regione**" o "**Friuli**") ha sviluppato un progetto di "*stratificazione statistica*" della popolazione, propedeutica all'individuazione dei soggetti in condizione di complessità e comorbilità da segnalare ai Medici di Medicina Generale (di seguito, "**MMG**") ai fini di permettere una migliore gestione della vaccinazione nel contesto epidemiologico da Covid-19. All'interno di tale schema gli MMG venivano chiamati a validare, attraverso il portale informatico regionale, una lista di utenti/assistiti in relazione alle loro condizioni di fragilità. Tali informazioni venivano estratte dal c.d. *datawarehouse* regionale e venivano elaborate da due società *in-house* del Friuli tramite un algoritmo di classificazione denominato "ACG" ("*Adjusted Clinical Group*"). Tale algoritmo aveva l'obiettivo di realizzare un profilo sanitario di rischio dell'interessato con riferimento alle specifiche patologie che potevano esporre gli assistiti più fragili a contrarre infezioni più gravi da SARS COV-2, al fine di mettere in atto interventi preventivi di presa in carico del paziente. L'intera iniziativa della Regione si poneva all'interno della Legge FVG 22/2019 volta a riconoscere in capo al Servizio sanitario regionale l'attivazione "*di modalità organizzative innovative di presa in carico, basate sulla proattività e sulla medicina di iniziativa in grado di integrare le forme di risposta ai bisogni delle persone in condizione di cronicità e fragilità, per garantire la continuità nell'accesso alla rete dei servizi e l'appropriatezza delle prestazioni sanitarie, sociosanitarie e sociali*".
Nel dicembre 2022, a seguito della segnalazione di un medico di base, il Garante per la protezione dei dati personali apriva un'istruttoria per ottenere delucidazioni in riferimento al trattamento dei dati svolto sia dalla Regione del Friuli-Venezia Giulia che dalle Aziende regionali che avevano ricevuto i dati.

I Provvedimenti del Garante

Con i Provvedimenti nn. 415, 416 e 417 del 15 dicembre 2022 (di seguito, i "**Provvedimenti**") il Garante per la privacy italiano ha sanzionato tre ASL friulane (ovvero, Azienda Sanitaria Universitaria Friuli - ASFO , Azienda Sanitaria universitaria Friuli Centrale - ASUFC e Azienda Sanitaria universitaria Giuliano Isontina -ASUGI) che, attraverso l'uso di algoritmi, avevano classificato gli assistiti in relazione al rischio di avere o meno complicanze in caso di infezione da Covid-19. Le attività delle ASL erano legate all'elaborazione dei dati dei pazienti presenti nelle banche dati aziendali al fine di realizzare, con riferimento a specifiche patologie (che, nel caso in esame, erano quelle che potevano esporre gli assisti più fragili a contrarre infezioni più gravi da Covid-19), un profilo sanitario di rischio dell'interessato, prodromico alla presa in carico di iniziative nei confronti del paziente stesso. Nell'analisi dello schema sotteso al procedimento di stratificazione del rischio dei pazienti messo in atto dalle ASL, l'Autorità Garante ha rilevato la sussistenza di elementi idonei a configurare la violazione, imputabile alle Aziende sanitarie, della normativa in materia di protezione dei dati personali sanitari. In particolare, è emerso che i dati degli assistiti erano stati trattati in assenza di una idonea base giuridica, senza fornire agli interessati tutte le informazioni necessarie (in particolare sulle modalità e finalità del trattamento) e senza aver effettuato preliminarmente la valutazione d'impatto prevista dall'art. 35 GDPR. In riferimento ai casi specifici il Garante Privacy ha inoltre ribadito che "*la profilazione dell'utente del servizio sanitario, sia questo regionale o nazionale, determinando un trattamento automatizzato di dati volto ad analizzare e prevedere l'evoluzione della situazione sanitaria del singolo assistito e l'eventuale correlazione con altri elementi di rischio clinico […] può essere effettuata solo nel rispetto di requisiti specifici e garanzie adeguate per i diritti e le libertà degli interessati*" mancanti nei casi di specie.
In forza di quanto sopra il Garante ha dichiarato illecito il trattamento dei dati personali effettuato dalle tre ASL friulane per la violazione degli artt. 5, par. 1, lett. a), 9, 14 e 35 del Regolamento e dell'art. 2-*sexies* del Codice Privacy e ha valutato che, nei casi specifici, le operazioni avevano riguardato i dati sanitari di un ingente numero di assistiti, ordinando ad ognuna delle tre Aziende di pagare la sanzione di 55.000 euro e di procedere alla cancellazione dei dati elaborati.
Con i Provvedimenti il Garante ha quindi sancito che le Aziende sanitarie, per il loro ambito di competenza, dovevano considerarsi responsabili

delle violazioni della privacy commesse nell'attuazione di progetti decisi dalla Regione, in quanto titolari dei dati contenuti nelle proprie banche dati.
I Provvedimenti sono stati impugnati davanti al Tribunale di Pordenone, Udine e Trieste, in ragione degli ambiti di competenza territoriale.

Tribunale di Pordenone, Sentenza del 13/10/2023
Con Sentenza del 13 ottobre 2023, emessa a definizione della causa n.228/2023, il Tribunale di Pordenone, tramite un'attenta analisi dei rapporti privacy nel mondo della sanità regionale, ha annullato il provvedimento n.415 del 15 dicembre 2022 del Garante, azzerando la sanzione di 55 mila euro comminata all'Azienda Sanitaria Universitaria Friuli Occidentale (di seguito, "**ASFO**").
Con il primo motivo di opposizione l'ASFO ha eccepito di non aver assunto nella vicenda la qualità di titolare del trattamento, in quanto mai detentrice del potere di determinare le finalità e i mezzi del trattamento (nella specie l'applicazione dell'algoritmo "ACG" alle banche dati presenti nel c.d. *datawarehouse* regionale) che, invece, erano interamente stabiliti a livello regionale. Secondo la difesa del Garante, invece, la circostanza che la Regione chiedesse all'Azienda Sanitaria, quale titolare del trattamento, di effettuare operazioni di trattamento su dati personali non esonerava l'Azienda dall'obbligo di valutare la legittimità della richiesta trasmessale e la sussistenza di un'idonea base giuridica, soprattutto alla luce della delicatezza del trattamento avente ad oggetto i dati sanitari di migliaia di soggetti tramite l'uso di algoritmi.
Con Sentenza del 13 ottobre 2023 il Tribunale di Pordenone accoglie il primo motivo di opposizione dell'ASFO da cui l'annullamento del provvedimento del Garante, fondato *in toto* sul presupposto del riconoscimento della qualità di titolare del trattamento in capo ad ASFO.
Il giudice sottolinea, infatti, che il titolare del trattamento deve essere ritenuto, in coerenza all'art. 4 par. 7 GDPR, "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali*".
Il Tribunale evidenzia altresì che è Titolare del trattamento colui che tratta i dati senza ricevere istruzioni da altri e il cui ruolo "*non dipende da designazioni formali bensì dall'effettiva attività svolta nello specifico trattamento dei dati*; *in altri termini, il titolare del trattamento non è chi gestisce i dati, ma chi in concreto decide il motivo e le modalità del trattamento*". Sul punto vengono richiamate anche le Linee Guida sul concetto di Titolare e Responsabile del trattamento dell'European Data Protection Board che indicano, come elemento chiave per la qualificazione del soggetto "*l'influenza del titolare in virtù dell'esercizio di un potere decisionale ("determina"), in forza di disposizioni di legge o di una concreta influenza fattuale*".
In forza di tale ricostruzione dei rapporti privacy, conclude il Tribunale, l'ASFO non può essere considerata titolare del trattamento di profilazione degli assistiti in classi di rischio sanitario non solo poiché il trattamento dei dati ha tratto origine dalla delibera n. 1737 del 20 novembre 2020 (che a propria volta faceva seguito ad una Intesa raggiunta tra la Regione Friuli Venezia Giulia e le organizzazioni sindacali dei medici di medicina generale), ma anche e soprattutto perché il ruolo dall'Azienda Sanitaria è stato meramente esecutivo di precise e vincolanti disposizioni ricevute dalla Regione. Secondo questo schema, dunque, i titolari del trattamento consistente nella "*nella profilazione degli assistiti del Servizio sanitario ragionale in base alle informazioni relative allo stato di salute individuale e nella relativa collocazione in classi di rischio sanitario*", sono gli enti che hanno individuato finalità e mezzi del trattamento, tra i quali non può essere ricompresa l'ASFO che non ha assunto un ruolo attivo o di rilievo.
In ogni caso – motiva ancora il giudice - il Garante non ha mai dato prova della circostanza che l'ASFO avesse avuto un ruolo tale da determinare finalità e mezzi del trattamento, presumendolo solo in ragione della riferibilità delle banche dati alle Aziende.

Tribunale di Udine, Sentenza del 21/09/2023
Il Tribunale di Udine con sentenza del 21 settembre 2023 a definizione della causa n.308/2023, si è espresso accogliendo integramente il ricorso presentato dall'Azienda Sanitaria universitaria Friuli Centrale (di seguito, "**ASUFC**") proposto contro il provvedimento del Garante per la Privacy n.416 del 15 dicembre 2022.
La sentenza in esame condivide l'orientamento del Tribunale di Pordenone arrivando alle medesime conclusioni aggiungendo, tuttavia, precisazioni di estremo rilievo. Nella sentenza in esame, il Tribunale di Udine, infatti, a differenza di quello di Pordenone, passa in rassegna tutte le violazioni che il Garante ha imputato all'Azienda Sanitaria, finendo con il dichiararne l'insussistenza.
In primo luogo, in merito alla natura del trattamento dei dati personali oggetto di sanzione da parte del Garante, il giudice afferma che:

i. la profilazione dei pazienti è stata effettuato dalla società *in house* su mandato regionale in

recepimento del "*Verbale di intesa tra la Regione Friuli Venezia Giulia e le Organizzazioni Sindacali dei Medici di Medicina Generale per la disciplina dei rapporti biennio 2020-2021 e delle attività connesse all'emergenza epidemiologica da Covid-19*";

ii. l'algoritmo consentiva la selezione e gestione delle informazioni sensibili dei soli pazienti che avevano già espresso il loro consenso alla divulgazione dei dati ai propri medici potendo essi ricavarli dal Fascicolo Sanitario Elettronico (di seguito, "**FSE**");

iii. gli MMG avrebbero potuto redigere anche manualmente e in completa autonomia gli elenchi dei pazienti maggiormente vulnerabili in caso di infezione da Covid-19, poiché consultabili sul c.d. Portale di continuità delle cure. La circostanza di usare un software per tale scopo derivava esclusivamente dalla volontà della Regione di fornire un supporto tecnico ai medici in un momento emergenziale;

l'insieme dei motivi di cui sopra permette al Tribunale di ricondurre l'estrazione dei dati dal *datawarehouse* regionale e l'elaborazione delle liste di pazienti alla nozione giuridica di "trattamento secondario" di dati sensibili già raccolti dall'Azienda Sanitaria, previo consenso dei pazienti, e già a disposizione degli stessi medici, ancorché non ancora organizzati "*in liste di più immediata percezione*". In definitiva – conclude il giudice – l'attività compiuta dalla società *in house*, su espresso mandato regionale, "*è consistita in una mera rielaborazione di dati già raccolti e a disposizione anche dei medici di base, compiuta con l'obiettivo precipuo di agevolare i medici di medicina generale del territorio nell'individuazione dei pazienti in condizioni di complessità e comorbilità, al fine di consentire loro una più tempestiva ed efficiente gestione, in termini di prevenzione, pianificazione e programmazione, della vaccinazione nel contesto pandemico*". Per di più, il Tribunale ritiene che il trattamento deliberato dalla Giunta Regionale, qualificabile come "trattamento secondario" è ammissibile, in ossequio all'art. 5 GDPR, in quanto non incompatibile con le finalità originarie di diagnosi e cura per le quali è stato introdotto il FSE e per le quali i dati dei pazienti erano originariamente stati raccolti presso l'Azienda Sanitaria ricorrente.

In riferimento all'imputabilità del trattamento all'Azienda Sanitaria ricorrente, nella sentenza viene sottolineato che è stata la Giunta regionale a stabilire non solo le finalità del trattamento, ma anche e soprattutto le specifiche modalità di esecuzione dello stesso, attribuendo compiti tecnici e specifici, privando totalmente l'ASUFC di qualsiasi margine di discrezionalità. Inoltre, a differenza di quanto rilevato dal Garante, il Tribunale aggiunge che l'Azienda Sanitaria non avrebbe comunque potuto opporsi all'esecuzione della delibera regionale che ha natura di "*atto regolamentare, formalmente amministrativo ma sostanzialmente normativo, dunque vincolante e cogente*". In conclusione, quindi, anche qualora si ritenesse illegittimo il trattamento dei dati personali di titolarità dell'Azienda Sanitaria, la sua condotta andrebbe comunque scriminata "*sussistendo il presupposto dell'adempimento ad un dovere giuridico imposto da una fonte regolamentare regionale, emanata sulla base di una copertura legislativa di rango primaria*".

In relazione all'asserita mancanza di un'idonea base giuridica sollevata dal Garante, il Tribunale evidenzia come il trattamento potrebbe legittimamente trovare la sua base giuridica nell'art.9 lett. i) GDPR relativo ai motivi di interesse pubblico riguardanti la "*protezione da gravi minacce per la salute a carattere transfrontaliero*". Sul punto viene richiamato, inoltre, il dettato del Considerando 54 GDPR che statuisce quanto segue: "*il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato[…]In tale contesto, la nozione di sanità pubblica dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio: tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità"*. Nel caso di specie – conclude il giudice – il trattamento oggetto della sanzione del Garante per la Privacy trova la sua base giuridica nell'interesse pubblico e, nello specifico, nei diversi provvedimenti legislativi emanati nell'ambito del contesto emergenziale pandemico. Inoltre, il Tribunale ricorda che l'art.2 *ter* del Codice Privacy prevede che la base giuridica del trattamento può anche consistere in un atto amministrativo generale: nel caso di specie il trattamento è stato deliberato dalla Giunta regionale in attuazione della normativa di fonte primaria.

Con riguardo alla violazione degli obblighi di informativa, il giudice richiama l'obbligo di segretezza professionale in capo ai medici di

medicina generale nell'espletamento delle loro attività di diagnosi e cura, da cui l'applicazione della derogatoria all'obbligo di preventiva informazione del trattamento, ai sensi dell'art. 14 par. 5 lett. d) GDPR.
Infine, del tutto infondata anche la censura rilevata dal Garante in relazione alla violazione dell'art.35 GDPR, riguardante la carenza della preventiva valutazione di impatto del trattamento dei dati personali. In primo luogo, viene sottolineato che, nel caso di specie, non appare integrato il requisito dell'impiego di "nuove tecnologie" nel trattamento dei dati prescritto dalla Giunta Regionale, in quanto – sostiene il giudice – l'uso dell'algoritmo costituisce, ormai, "*una tecnica largamente diffusa nelle operazioni di elaborazione dei dati, soprattutto in ambito medico-scientifico*". In secondo luogo, non si comprende "*quale pregiudizio per i diritti e le libertà dei pazienti possa derivare dalla predisposizione di elenchi di assistiti in condizioni di maggiore vulnerabilità, in base ad informazioni già presenti nei database delle Aziende Sanitarie e già noti ai medici di base, tenuto conto della finalità, già più volte ribadite, di tale trattamento (potenziamento e programmazione degli interventi di prevenzione e cura nell'ambito del contesto emergenziale pandemico)*". Da ultimo, viene rilevato che il trattamento in esame non risulta neppure ascrivibile alla fattispecie di cui all'art. 35 paragrafo 3) lettera a) GDPR, in quanto "*non si vede in che modo la disponibilità, da parte dei medici di medicina generale, delle informazioni sanitarie rielaborate in modo automatizzato, secondo gli obiettivi di programmazione e pianificazione della Regione, avrebbe potuto o potrebbe incidere sulla sfera giuridica dei pazienti*".
In forza dei motivi di cui sopra il giudice accoglie integralmente il ricorso dell'Azienda Sanitaria Friuli Centrale riconoscendo la piena legittimità del trattamento dei dati personali censurato dal Garante, in quanto avvenuto, secondo l'analisi tecnica e non meramente formale proposta nella sentenza, in piena conformità del diritto nazionale ed europeo in materia di privacy.

ELISA GROSSI

Tribunale di Pordenone, Sentenza del 13 ottobre 2023:
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9940829

Tribunale di Udine, Sentenza del 21 settembre 2023:
https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9957324

2023/4(26)VP

26. Il provvedimento sanzionatorio di AGCOM contro Google e Twitch per la pubblicizzazione di gioco d'azzardo e l'archiviazione di un analogo procedimento a carico di TikTok

Con le delibere nn. 317/23/CONS e 318/23/CONS, l'Autorità per le garanzie nelle comunicazioni (di seguito **AGCOM** o l'**Autorità**) ha emesso due sanzioni nei confronti di Google Ireland Limited e Twitch Interactive Germany GmbH (di seguito **Google**, **Twitch** o anche le **società**) per aver violato il divieto di pubblicità di giochi e scommesse con vincite in denaro, nonché di gioco d'azzardo, previsto dall'art. 9, comma 1 del decreto-legge n. 87 del 12 luglio 2018 convertito in legge 96 del 9 agosto 2018 *cd.* "Decreto Dignità" (di seguito **Decreto Dignità**), a mente del quale: "Ai fini del rafforzamento della tutela del consumatore e per un più efficace contrasto del disturbo da gioco d'azzardo […] è vietata qualsiasi forma di pubblicità, anche indiretta, relativa a giochi o scommesse con vincite di denaro nonché al gioco d'azzardo, comunque effettuata e su qualunque mezzo, incluse le manifestazioni sportive, culturali o artistiche, le trasmissioni televisive o radiofoniche, la stampa quotidiana e periodica, le pubblicazioni in genere, le affissioni e i canali informatici, digitali e telematici, compresi i social media. Dal 1° gennaio 2019 il divieto di cui al presente comma si applica anche alle sponsorizzazioni di eventi, attività, manifestazioni, programmi, prodotti o servizi e a tutte le altre forme di comunicazione di contenuto promozionale, comprese le citazioni visive e acustiche e la sovraimpressione del nome, marchio, simboli, attività o prodotti la cui pubblicità, ai sensi del presente articolo, è vietata. Sono esclusi dal divieto di cui al presente comma le lotterie nazionali a estrazione differita di cui all'articolo 21, comma 6, del decreto-legge 1º luglio 2009, n. 78, convertito, con modificazioni, dalla legge 3 agosto 2009, n. 102, le manifestazioni di sorte locali di cui all'articolo 13 del decreto del Presidente della Repubblica 26 ottobre 2001, n. 430, e i loghi sul gioco sicuro e responsabile dell'Agenzia delle dogane e dei monopoli".
Le decisioni dell'AGCOM (competente alla contestazione e all'irrogazione delle sanzioni in materia, ai sensi del co. 3 del medesimo art. 1 del

Decreto Dignità) muovono da due procedimenti avviati a seguito di numerose segnalazioni, le quali hanno evidenziato che entrambe le società hanno pubblicizzato attività di gioco e scommesse *online* su oltre 90 canali, contenenti oltre 23 mila video, attraverso le rispettive piattaforme di condivisione video: YouTube, di proprietà di Google, e Twitch.

Le società sono state ritenute responsabili in quanto *"titolari del mezzo di diffusione dei video pubblicati da soggetti terzi con i quali avevano specifici contratti di partnership commerciale."*

L'Autorità ha valutato la natura di *hosting provider* delle società, richiamando l'art. 6 del regolamento (UE) 2022/2065 c.d. *Digital Services Act* (di seguito **DSA**), il quale esonera dalla responsabilità i soli soggetti che non siano a conoscenza dei contenuti illegali o che, venendone a conoscenza, agiscano prontamente per rimuoverli.

Al fine di valutare l'applicabilità di tale norma ai canali sui quali si è registrata la violazione, l'Autorità ha fatto riferimento alla pratica di verifica delle informazioni e dei contenuti condivisi sulle piattaforme, sottolineando l'esistenza di due distinte categorie di canali: quella dei *content creator* non verificati e quelli dei *content creator* verificati, anche denominati *"partner"*.

Per la prima categoria, la conformità alla legge avviene attraverso l'accettazione dei termini e delle condizioni di utilizzo della piattaforma al momento della creazione del canale. Dunque, tra un utente comune che dopo aver creato dei contenuti li carica sulla piattaforma e quest'ultima esiste a monte un rapporto negoziale sorto mediante la stipula di un contratto per adesione, poiché è sufficiente l'accettazione delle clausole unilateralmente predisposte dal fornitore del servizio intermediario affinché il rapporto sinallagmatico si perfezioni.

Un meccanismo differente è quello invece previsto per la seconda categoria, ovvero quella dei *content creator* verificati.

Questi sono soggetti ai quali – dopo aver raggiunto una certa quantità di *engagement* ed aver soddisfatto altri criteri minimi - viene data la possibilità di richiedere di sottoscrivere un contratto per divenire, appunto, *partner* commerciale.

Trattasi dunque di un invito a proporre cui non consegue l'automatica instaurazione del rapporto contrattuale. *Il content creator*, infatti, predispone e invia al fornitore del servizio intermediario una proposta di sottoscrizione cui segue una seconda fase nell'ambito della quale, piattaforma ed utenti, giungono al già menzionato accordo di *partnership* commerciale.

Tra le due categorie si registrano dunque differenza significative.

Per la prima, si esclude la consapevolezza delle società riguardo ai contenuti del canale, mentre, per la seconda, la verifica preventiva esclude l'ignoranza della società riguardo alla tipologia di contenuti pubblicati. L'approvazione, infatti, implica una conoscenza dei contenuti dei canali verificati.

Con le delibere oggetto del presente commento, il tema della responsabilità dell'*hosting provider* assume una importante rilevanza poiché vengono per la prima volta applicate le norme contenute nel DSA al fine di sanzione il divieto di pubblicità di giochi e scommesse di cui all'art. 9 del Decreto Dignità.

Si evidenza, dunque, una crescente attenzione nei confronti delle piattaforme *online* con riferimento ai compiti di vigilanza e gestione dei contenuti pubblicati dai propri utenti in un settore ove appare innegabile l'esigenza di rafforzare la tutela del consumatore al fine di contrastare il disturbo da gioco d'azzardo.

Degna di menzione appare la circostanza che, con Delibera 316/23/CONS adottata in pari data (5.12.2023) (la **Delibera 316/2023**), l'Autorità abbia invece archiviato un analogo procedimento avviato contro la società TikTok Technology Limited, con sede in Irlanda, titolare della omonima famosa piattaforma (di seguito **TikTok** o la **società**), alla quale era stata contestata la pubblicizzazione di gioco d'azzardo su 30 canali TikTok. In questo caso, alla luce di quanto dichiarato da TikTok circa la mancanza di alcun tipo di rapporto commerciale con i 30 *content creator*, l'AGCOM ha ritenuto che non potesse essere imputata responsabilità in capo alla società in quanto la stessa non risultava aver avuto conoscenza circa l'illecito commesso presso la propria piattaforma di condivisione di video; e tanto - si legge nella Delibera 316/2023 - «*in ossequio a quanto previsto dalla elaborazione giurisprudenziale formatasi sulla direttiva e-commerce nonché alla luce del dettato dell'articolo 6, comma 1, lett. a) del Regolamento DSA*».

L'AGCOM ha aggiunto che «*nessuna responsabilità è possibile imputare alla società sempre alla luce dell'elaborazione giurisprudenziale nonché ai sensi dell'articolo 6, comma 1, lett. b) del predetto Regolamento DSA in quanto la società ha immediatamente rimosso tutti i video identificati nell'atto di contestazione inibendo altresì l'accesso ai relativi account da parte degli utenti italiani*».

Infine, sembra interessante segnalare una specifica difesa avanzata da TikTok e la relativa risposta dell'Autorità, con riguardo ad una recente sentenza della Corte di Giustizia dell'Unione europea (di

seguito **CGUE** o la **Corte**), segnatamente la sentenza sul caso C-376/22 (9 novembre 2023, *Google Ireland Limited, Tik Tok Technology Limited and Meta Platforms Ireland Limited v Kommunikationsbehörde Austria (Komm Austria))*.
TikTok ha utilizzato questa sentenza affermando che, attraverso di essa "*i giudici dell'Unione Europea hanno statuito che uno Stato membro non può assoggettare un fornitore di servizi della società dell'informazione stabilito in un altro Stato membro a misure normative generali e astratte che si discostino dalle misure dello Stato membro in cui l'operatore è stabilito. Dunque, la Corte di Giustizia dell'Unione Europea ha dichiarato inapplicabile a TikTok (come noto con sede in Irlanda) la legge austriaca sulle piattaforme di comunicazione*". Alla luce di tale pronuncia TikTok ha sostenuto davanti all'AGCM che "*il c.d. Decreto dignità (art. 9 D.L. 12 luglio 2018, n. 87) sia in contrasto con il diritto dell'Unione Europea direttamente applicabile (principio del Paese d'origine) e quindi da disapplicare da parte delle Autorità nazionali amministrative e giurisdizionali;* [e che] *comunque non sussista né possa sussistere alcuna attribuzione in capo ad AGCOM*".
L'AGCM ha replicato a questa difesa ritenendola non pertinente, in quanto – così ha motivato l'Autorità - essa «*riguarda la possibilità da parte di ciascuno Stato membro di derogare "caso per caso" al principio del Paese di origine per determinati casi e secondo le specifiche modalità previste dall'articolo 3, commi 4 e 5 della Direttiva sul commercio elettronico. In particolare, occorre osservare che l'articolo 9 del decreto dignità rientra proprio tra quei provvedimenti, previsti dall'articolo 14 della direttiva e-commerce prima e del regolamento DSA adesso ex art. 6, che, conformemente all'ordinamento giuridico di ciascun Stato membro, attribuiscono ad un'autorità giudiziaria o amministrativa la possibilità di esigere che il prestatore del servizio impedisca o ponga fine a una violazione*».

VINCENZO PITTELLI

Comunicato stampa AGCOM:
https://www.agcom.it/documents/10179/32522781/Comunicato+stampa+12-12-2023/c981bcb0-fcb9-4e30-926e-05e2191a2ae0?version=1.0

Delibera 317/23 (Google):
https://www.agcom.it/documents/10179/32598315/Delibera+317-23-CONS/8a12c65c-519b-48b2-8c5d-50d582d1d9aa?version=1.7

Delibera 318/23 (Twitch):
https://www.agcom.it/documents/10179/32598315/Delibera+318-23-CONS/62b6aba0-96e6-41ac-a0b8-1a410204be8f?version=1.1

Delibera 316/23 (TikTok):
https://www.agcom.it/documents/10179/32598315/Delibera+316-23-CONS/844f8177-3d1d-49e5-8dad-e5cdb5d01ce9?version=1.1

2023/4(27)IG

27. Le cause intentate da oltre 40 Stati degli USA contro Meta per pratiche online che creano dipendenza nei giovani

Una coalizione di 41 stati americani, con atto del 24 ottobre 2023, ha citato in giudizio Meta Platforms Inc., Instagram Llc, Meta Payments, Inc., Meta Platforms Technologies, Llc, (d'ora in avanti **Meta**), con l'accusa di aver violato le leggi sulla protezione dei consumatori, catturando slealmente l'attenzione dei minori di età e ingannando gli utenti sulla sicurezza delle sue piattaforme di social media (in particolare Instagram e Facebook), nonché la legislazione sulla privacy dei minori ai sensi del Children's Online Privacy Protection Act (**COPPA**).
L'azione legale è promossa dallo Stato del Colorado e della California ma è stata presentata congiuntamente ad altri Stati presso la Corte del distretto settentrionale della California.
L'indagine e la conseguente azione giudiziaria muovono dalla divulgazione di alcuni documenti interni da parte di un ex dipendente di Facebook, noti come "Facebook Files" e pubblicati dal Wall Street Journal nel 2021, dai quali emerge che Meta era al corrente dei danni che, in particolare, Instagram può causare agli adolescenti - soprattutto alle ragazze - in termini di salute mentale e di immagine corporea.
Nell'atto di citazione si legge come Meta abbia creato un modello di business incentrato sulla massimizzazione del profitto, orientato ad attirare, in modo crescente, l'attenzione dei giovani utenti sulle sue piattaforme di social media, generando profitti attraverso la vendita di pubblicità attentamente mirata a soddisfare le loro esigenze e interessi. A tal fine avrebbe "progettato e distribuito funzionalità di prodotto dannose e psicologicamente manipolative per indurre i minori ad un uso compulsivo e prolungato delle piattaforme, assicurando falsamente al pubblico che le sue funzionalità erano sicure e adatte ai giovani utenti". Ciò, nonostante le ricerche, l'analisi di esperti indipendenti e i dati pubblicamente disponibili

avessero dimostrato la stretta correlazione tra l'uso delle piattaforme di Meta da parte dei giovani e l'insorgenza (o l'aggravamento), negli stessi, di stati emotivi importanti come l'ansia, la depressione, l'insonnia, l'insoddisfazione del proprio corpo, la bassa autostima e molti altri effetti negativi. Sempre nell'atto di citazione si legge come dagli studi interni, commissionati da Meta, risultasse evidente la consapevolezza dell'azienda dei gravi danni associati al tempo trascorso dai giovani utenti sui social media. Tuttavia Meta si sarebbe impegnata a travisare, nascondere e minimizzare l'impatto di tali funzioni sulla salute mentale e fisica dei giovani utenti, promuovendo piuttosto le sue piattaforme come sicure per i minori di età, nonché espandendo l'uso di queste pratiche in nuove piattaforme e domini, quali per esempio il Metaverso di Meta per la realtà virtuale, la comunicazione di Meta come Whatsapp e Messenger e altri prodotti.
Infine i procuratori generali hanno accusato Meta di aver violato (e di continuare a violare) gli obblighi previsti dal Children's Online Privacy Protection Act (COPPA) raccogliendo illegalmente i dati personali dei suoi utenti minorenni (di età inferiore ai 13 anni) senza il permesso dei genitori.
L'insieme di questi atti costituiscono, secondo i procuratori generali, pratiche sleali e/o ingannevoli ai sensi degli statuti statali per la protezione dei consumatori, violano il COPPA, oltre che atti illegali ai sensi dei principi del diritto comune, per i quali ciascuno stato richiede specifici rimedi e sanzioni.

ILARIA GARACI

https://oag.ca.gov/system/files/attachments/press-docs/Less-redacted%20complaint%20-%20released.pdf

2023/4(28)FP

28. Aggiornamenti di dicembre 2023-gennaio 2024 sul caso *Fortnite* in USA (le azioni di Epic Games vs Google e Apple per condotta anticoncorrenziale)

L'11 dicembre del 2023 la Corte federale di San Francisco ha emesso l'atteso verdetto che accerta l'abuso di posizione dominante da parte della controllata di Alphabet (Google) a causa delle condizioni applicate sul marketplace "Play Store" nei confronti della casa di sviluppo di videogames Epic Games. Il giudice James Donato dello stesso distretto della Corte del Northern California sarà ora incaricato di stabilire le misure rimediali che dovranno essere realizzate dall'azienda di Mountain View, la quale ha già preannunciato la propria intenzione di proporre appello.
La controversia ha interessato il prodotto di punta della Epic Games, il videogame Fortnite. La sua commercializzazione si basa su un modello di business tipico del mondo del gaming su dispositivi mobili, secondo cui lo sviluppatore mette a disposizione degli utenti il proprio prodotto in modalità «freemium» o «free-to-play». L'applicazione può essere scaricata e utilizzata gratuitamente, ma i giocatori hanno la possibilità di effettuare acquisti opzionali attraverso una valuta digitale, per migliorare o personalizzare la propria esperienza di gioco (nel caso di Fortnite, di costumi, armi e accessori), concludendo quelle che comunemente vengono definite come "micro-transazioni". È stato stimato che, nello scorso anno, circa il 94 % delle applicazioni presenti sui principali marketplaces per dispositivi mobili si basino su questo modello. Sebbene il mercato degli acquisti in-app non costituisca la fonte esclusiva dei proventi che Epic Games trae da Fortnite – fra gli altri, la sottoscrizione di un abbonamento per far parte di networks con altri giocatori, la vendita di spazi pubblicitari e di biglietti per l'accesso a determinati eventi – il sistema delle micro-transazioni rappresenta comunque la fetta più sostanziosa dei 5.8 miliardi di dollari annui di proventi dichiarati secondo la più recente rilevazione effettuata dalla stesa casa sviluppatrice (2021, Epic Games).
Oltre alla distribuzione effettuata attraverso una piattaforma proprietaria, la Epic Games ha concluso una serie di accordi di licenza (Developer Distribution Agreement, **DDA**) per consentire il download dell'applicazione Fortnite sui marketplaces gestiti da piattaforme di terze parti, permettendo di integrare il proprio prodotto all'interno dei diversi ecosistemi (Playstation, X-Box, PC, Android, Apple e così via) e incrementando, così facendo, in modo consistente la platea dei suoi potenziali utilizzatori. Si tratta di una operatività tipica dei sistemi di distribuzione di applicazioni per dispositivi digitali, poiché consente ai gestori dei principali marketplaces (Google Play Store, Apple Store) di offrire ai propri utenti app native di sviluppatori terzi. In estrema sintesi, questi accordi autorizzano il gestore del marketplace a riprodurre, eseguire, mostrare, analizzare e utilizzare i prodotti dello sviluppatore in modo non esclusivo, adattato al funzionamento della propria piattaforma, dei dispositivi e servizi che ne supportano l'utilizzo, con l'obiettivo di consentire

l'archiviazione della applicazione e l'accesso degli utenti agli stessi.

L'origine delle dispute legali fra Epic Games e i principali gestori di marketplace per app deriva dalle condizioni economiche imposte da queste ultime per la distribuzione delle applicazioni sviluppate da terzi. Con la stipulazione del DDA, il gestore si riserva tipicamente il diritto di applicare una commissione fissa o progressiva, in dipendenza del fatturato dell'applicazione, per i pagamenti legati alla sottoscrizione di abbonamenti e per gli acquisti in-app: Play Store e Apple Store prevedono, ad esempio, commissioni che si attestano fra il 15 e il 30 %. Al tentativo da parte di Epic Games di evitare il prelievo della commissione mediante un sistema di transazioni dirette fra l'utente e la casa di sviluppo, Apple e Google hanno reagito introducendo prima un blocco agli aggiornamenti di Fortnite e successivamente rimuovendo del tutto l'applicazione dal proprio store. Ritenendo la condotta dei due giganti del Tech lesiva della concorrenzialità del mercato delle applicazioni digitali su dispositivi mobili, Epic Games ha così intrapreso due distinte azioni nei confronti di Apple e Google (13 agosto 2020). Entrambe muovono, con tutta evidenza, da una finalità che va oltre gli scopi della controversia individuale, per assumere i connotati tipici di una strategic litigation – da qui, il nome "Project Liberty" utilizzato da Epic Games. L'obiettivo della casa di sviluppo è quello di rimettere in discussione gli equilibri fra le posizioni di potere su di un mercato che, nonostante le dimensioni assunte, è finora sfuggito in larga parte alla regolazione antitrust.

Il principale punto di discussione che accomuna i due processi è rappresentato dalla esatta delimitazione del mercato rilevante, come precondizione per comprendere la distribuzione degli equilibri di potere e suoi eventuali abusi. Questo aspetto costituisce difatti l'elemento nevralgico sul quale si incentra l'ambito di applicazione delle Sections 1-2 dello Sherman Act, la legge americana antitrust e del Cartwright Act californiano. Secondo la ricostruzione proposta da Epic Games, ciascuna piattaforma sulla quale si svolgono microtransazioni in-app dovrebbe considerarsi mercato rilevante in sé, stanti anche le differenze che corrono fra i sistemi Android e Apple. Viceversa, la ricostruzione proposta dalle due aziende del Tech allarga la prospettiva di osservazione del mercato al più ampio «digital video game market», a sua volta distinto nelle sottocategorie del *i*) mobile gaming; *ii*) PC gaming; *iii*) Console gaming; *iv*) Cloud-based game streaming.

Il verdetto raggiunto nella controversia con Google si discosta dalla soluzione precedentemente adottata dalla stessa Corte del Northern District of California, nella decisione sul caso Apple (10 settembre 2021), recentemente confermata dalla Corte Suprema degli Stati Uniti (17 gennaio 2024). In quest'occasione, la giudice Rogers aveva concluso che, nonostante potesse riconoscersi un certo margine di competitività e interoperabilità fra le diverse piattaforme, il mercato di riferimento cui guardare fosse quello delle transazioni su videogames per soli dispositivi mobili, con una quota di mercato appartenente ad Apple del 57,1 %. Nonostante alcune delle pratiche su questo mercato possano destare preoccupazioni per una distribuzione secondo la logica di duopolio, la Corte non ha ravvisato in quell'occasione gli estremi di alcuna condotta abusiva: i margini operazionali del gestore sono considerevolmente elevati, così come le barriere all'ingresso, ma è verosimile pensare che diminuiranno con l'incremento dell'interoperatività fra piattaforme e l'avvento di nuovi players nel settore del gaming. Secondo la Corte, il mantenimento di un elevato standard di sicurezza dell'ecosistema di Apple giustifica, inoltre, l'imposizione di condizioni più gravose per l'ingresso e il mantenimento dei prodotti offerti da case di sviluppo terze. La sentenza aveva dunque accertato un inadempimento contrattuale da parte della Epic Games e il conseguente obbligo di retrocedere la parte delle somme che sarebbero spettate al gestore a titolo di commissione.

Nell'analogo processo contro Google, si evince con chiarezza che a un diverso esito si è pervenuti in conseguenza della ben più marcata delimitazione del mercato di riferimento: l'«Android app distribution market» e l'«Andoid in-app billing services for digital good and services transaction market» (v., in calce, Form del verdetto raggiunto dalla Northern District of California sul caso Google Play Store). Trattandosi di una decisione assunta da una giuria invece che da un giudice togato, dal testo del verdetto non emergono le ragioni che hanno indotto a qualificare come monopolistiche le politiche di fatturazione intraprese da Google. Occorre inoltre considerare che fra i due casi vi è un'ulteriore differenza sul versante tecnico, consistente nella possibilità di *sideloading* sui sistemi Android. Come è noto, mentre i dispositivi mobili Apple permettono il download di applicazioni unicamente attraverso Apple Store, sui dispositivi Android è tecnicamente possibile avvalersi di markeplaces diversi da Play Store.

Il verdetto è stato accolto da Epic Games come «a Win for all Developers», un primo passo verso lo

smantellamento di un sistema di mercato soggetto al dominio monopolistico di due grandi players. Vi è, tuttavia, chi rileva che l'affidamento a una giuria – diversamente che nel caso Apple – abbia condotto ad una decisione influenzata più dal contegno di Google durante il processo (come la distruzione di alcuni documenti) che su evidenze probatorie solide di un abuso di posizione dominante; il che rende verosimile una riforma del provvedimento in sede di appello.

La prossima entrata in vigore del Digital Markets Act - regolamento (UE) 2022/1925 - (di seguito **DMA**) (7 marzo 2024) attenua – per lo meno in parte e per i soli utenti europei – gli esiti negativi della condanna nella controversia contro Apple, introducendo una più stringente regolazione per i gatekeepers. Anzitutto, il DMA apre al *sideloading* di app da altri app store di terze parti o altri siti web, superando la tradizionale restrizione imposta dall'azienda di Cupertino. In secondo luogo, il DMA riconosce la legittimità della pratica degli sviluppatori di indirizzare a pagamenti alternativi esterni agli stores. L'entrata in vigore del DMA coinciderà difatti con il ritorno dell'app Fortnite sull'Apple Store europeo.

FEDERICO PISTELLI

Google Play Developer Distribution Agreement
https://play.google.com/about/developer-distribution-agreement.html

Form del verdetto raggiunto dalla Northern District of California sul caso Google Play Store
https://storage.courtlistener.com/recap/gov.uscourts.cand.364325/gov.uscourts.cand.364325.606.0.pdf

Summary delle fasi del processo Epic Games, Inc. v. Apple Inc.
https://cand.uscourts.gov/cases-e-filing/cases-of-interest/epic-games-inc-v-apple-inc/

Ordinanza di rigetto dell'appello sul processo Epic Games, Inc. v. Apple Inc.
https://www.supremecourt.gov/orders/courtorders/011624zor_e1pf.pdf

2023/4(29)FS

29. La remissione alla CGUE da parte del TAR Lazio di questioni interpretative a proposito delle disposizioni della legge italiana sul diritto di autore e del regolamento AGCOM in materia di equo compenso agli editori di giornali online, in conseguenza del ricorso di Meta

Con sentenza n. 18790/2023 pubblicata il 12 dicembre 2023, il TAR Lazio (Sezione Quarta), adito su ricorso di Meta Platforms Ireland Limited (**Meta**), ha rimesso alla valutazione della Corte di Giustizia UE (innanzi **CGUE** o la **Corte**) la questione di compatibilità eurounitaria delle disposizioni previste dall'art. 43-*bis* della legge italiana sul diritto d'autore (legge 22 aprile 1941 n. 633, innanzi **l.a.**) e dal derivato regolamento dell'Autorità Garante delle Comunicazioni (AGCOM) in materia di individuazione dei criteri di riferimento per la determinazione dell'equo compenso per l'utilizzo online di pubblicazioni di carattere giornalistico, di cui alla Delibera AGCOM n. 3/23/CONS del 19 gennaio 2023, 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* [l.a.]", pubblicata sul sito internet dell'Autorità il 25 gennaio 2023 (di seguito, rispettivamente: il **Regolamento AGCOM**, e la **Delibera AGCOM 3/2023**).

Il rinvio pregiudiziale origina dal ricorso proposto da Meta per l'annullamento della Delibera AGCOM 3/2023 e degli allegati alla medesima delibera, incluso il Regolamento AGCOM. Nell'ambito dei diversi motivi di gravame articolati avverso l'atto impugnato, la multinazionale statunitense ha lamentato la contrarietà dell'art. 43-bis l.a. e delle derivate disposizioni regolamentarie di attuazione (non contestate per vizi propri) con la normativa eurounitaria e con la Costituzione italiana sotto vari profili, inclusa la violazione delle indicazioni Legge di delegazione europea 2019-2020 (legge 22 aprile 2021, n. 53: innanzi **legge delega**) per la parte relativa all'attuazione della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico digitale (innanzi **direttiva CDSM**). La ricorrente pone al centro della sua azione la doglianza che la legge delega, nel richiedere la previsione di forme di "adeguata tutela" per gli editori di giornali, non avrebbe tuttavia indicato la necessaria introduzione di un equo compenso a carico delle piattaforme, né, tantomeno, di un obbligo di negoziazione *inter partes*, con conseguente potere di determinazione in capo all'Autorità; né, da ultimo, di un divieto di oscuramento dei contenuti in pendenza della negoziazione.

Giova, a questo punto, operare una sintetica ricognizione delle disposizioni rilevanti ai fini della controversia sottoposta al TAR Lazio.

L'art. 15 della direttiva CDSM, la cui rubrica reca "*Protezione delle pubblicazioni di carattere giornalistico in caso di utilizzo online"*, ha introdotto anche per gli editori di giornali il riconoscimento dei diritti esclusivi di riproduzione e comunicazione al pubblico – già previsti dalla Direttiva 2001/29/CE sul diritto d'autore e i diritti connessi nella società dell'informazione (**direttiva InfoSoc**) – per l'utilizzo online delle loro pubblicazioni di carattere giornalistico da parte delle piattaforme. La norma intende colmare il c.d. "*value gap*" ossia l'iniqua distribuzione del valore generato dallo sfruttamento in ambiente digitale di un contenuto protetto tra il titolare del diritto (editore) e il prestatore di servizi che veicola questo contenuto online.

L'art. 9 della legge delega ha individuato i seguenti principi e criteri direttivi per il recepimento dell'art. 15 della Direttiva Copyright:

"(…)

h) prevedere, ai sensi dell'articolo 15 della direttiva (UE) 2019/790, che nel caso di utilizzo on-line delle pubblicazioni di carattere giornalistico da parte dei prestatori di servizi della società dell'informazione trovino adeguata tutela i diritti degli editori, tenendo in debita considerazione i diritti degli autori di tali pubblicazioni;

i) definire il concetto di «estratti molto brevi» in modo da non pregiudicare la libera circolazione delle informazioni;

l) definire la quota adeguata dei proventi percepiti dagli editori per l'utilizzo delle pubblicazioni di carattere giornalistico di cui all'articolo 15, paragrafo 5, della direttiva (UE) 2019/790, destinata agli autori, tenendo in particolare considerazione i diritti di questi ultimi; (…)".

A fronte della delega conferita dalla legge delega, è stato emanato il Decreto Legislativo 8 novembre 2021, n. 177 (sul D.lgs. 177/2021 v. in questa Rubrica la notizia n.1 del numero 1/2022: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf [2022/1(1)EB]). L'art. 1 del D.lgs. 177/2021 ("Modificazioni alla legge 22 aprile 1941, n. 633") alla lett. c) del comma 1, ha inserito all'interno della legge sul diritto d'autore l'art. 43-*bis*. Oltre a riconoscere agli editori di giornali i diritti esclusivi di riproduzione e comunicazione al pubblico di cui agli articoli 13 e 16 l.a. in caso di utilizzo online delle loro pubblicazioni di carattere giornalistico da parte dei prestatori di servizi della società dell'informazione (comma 1), l'art. 43-*bis* l.a. ha introdotto la previsione di un equo compenso a carico delle piattaforme, la cui determinazione, nel caso le trattative tra le parti falliscano, è rimessa ad un apposito Regolamento attuativo dell'AGCOM tenendo conto, tra l'altro, del numero di consultazioni online dell'articolo, degli anni di attività e della rilevanza sul mercato degli editori e del numero di giornalisti impiegati, nonché dei costi sostenuti per investimenti tecnologici e infrastrutturali da entrambe le parti, e dei benefici economici derivanti, ad entrambe le parti, dalla pubblicazione quanto a visibilità e ricavi pubblicitari (comma 8).

Ancora, per quanto qui rileva, l'art. 43-*bis* l.a. ha introdotto il divieto a carico delle piattaforme di limitare la visibilità dei contenuti degli editori nei risultati di ricerca durante le trattative (comma 9), nonché nuove competenze regolatorie di AGCOM, dando mandato all'Autorità di determinare in via autoritativa l'ammontare dell'equo compenso in caso di mancato accordo tra le parti (comma 10) e dotando la stessa di poteri ispettivi e sanzionatori in relazione agli obblighi di messa a disposizione dei dati da parte delle piattaforme (comma 12).

Sulla base del rinvio di cui ai commi 8 e seguenti dell'art. 43-*bis* l.a., è intervenuta la Delibera AGCOM 3/2023, il cui Allegato A reca il Regolamento AGCOM, con cui:

- sono stati individuati i criteri da utilizzare per determinare l'importo dell'equo compenso (art. 4 Regolamento AGCOM), che includono la definizione di una base di calcolo basata sui ricavi pubblicitari degli ISSP derivanti dall'utilizzo online delle pubblicazioni giornalistiche, al netto dei ricavi dell'editore derivanti dal traffico di reindirizzamento sul suo sito web;
- è stata determinata una aliquota fino al 70% da applicare alla base di calcolo (per determinare l'importo dell'equo compenso), sulla base di una serie di ulteriori criteri definiti dall'art. 4, co. 2 Regolamento AGCOM;
- sono stati dettagliati (art. 5 Regolamento AGCOM) gli obblighi di messa a disposizione dei dati, definiti i poteri ispettivi di AGCOM e prevista l'applicabilità di una sanzione amministrativa pecuniaria a carico del soggetto inadempiente fino all'1% del fatturato realizzato sul mercato nazionale nell'ultimo esercizio chiuso anteriormente alla notifica della contestazione;
- ha trovato disciplina (artt. 8-12 Regolamento AGCOM) la procedura per richiedere ad AGCOM di determinare l'importo dell'equo compenso e le regole del relativo procedimento, con possibilità di quest'ultima di determinarne unilateralmente l'ammontare.

Così ricostruito il quadro normativo di riferimento, il TAR ha anzitutto rilevato il carattere fortemente implementativo che caratterizza l'art. 43-*bis* l.a. rispetto alle indicazioni delineate dalla EUCD (ed anche rispetto ai contenuti della legge delega):

accanto al riconoscimento, per l'utilizzo online delle pubblicazioni di carattere giornalistico da parte delle piattaforme, di diritti esclusivi di riproduzione e comunicazione, la norma di recepimento ha introdotto la previsione di un equo compenso, la cui determinazione forma oggetto di negoziazione *inter partes* (ISSP ed editori).

Nondimeno, il mancato perfezionamento dell'accordo negoziale, alla scadenza di un termine pari a 30 giorni, facoltizza ciascuna delle parti a rivolgersi ad AGCOM, la quale entro i successivi 60 giorni: (i) indica, sulla base dei criteri stabiliti dal regolamento, quale delle proposte economiche formulate è conforme ai suddetti criteri; (ii) oppure, qualora non reputi conforme nessuna delle proposte, indica d'ufficio l'ammontare dell'equo compenso.

La normativa interna ha così introdotto, in un ambito che dovrebbe essere governato esclusivamente dalla libertà negoziale privata, la presenza di un soggetto terzo (non veicolata dall'unanime consenso delle parti stesse, ma evocabile anche da una soltanto di esse) con poteri:

- regolatori (quanto all'individuazione dei criteri di riferimento per la determinazione dell'equo compenso: cfr. art. 43-*bis*, co. 8 l.a.);
- decisori (quanto all'individuazione dell'ammontare dell'equo compenso relativamente alla singola fattispecie), ai quali, soltanto a seguito del perdurante mancato raggiungimento di un'intesa, sarà possibile adire il Tribunale delle imprese (art. 43-*bis*, co. 10 l.a.);
- dispositivi (sostanziati dall'obbligo, nei confronti delle parti ed esigibile anche da parte dell'Autorità, di mettere a disposizione "*i dati necessari a determinare la misura dell'equo compenso*" (art. 43-*bis*, co. 12 l.a.);
- sanzionatori (con applicabilità di una sanzione amministrativa pecuniaria fino all'1% del fatturato realizzato sul mercato nazionale nell'ultimo esercizio chiuso anteriormente alla notifica della contestazione).

Secondo il TAR, dunque, l'intervento autoritativo di AGCOM nel caso di mancato perfezionamento delle trattative tra editori e piattaforme, è suscettibile di compromettere – unitamente alla libertà negoziale delle parti – il principio di libertà nell'esplicazione del diritto di iniziativa economica, ai sensi degli articoli 16 e 52 TFUE.

Inoltre, ad avviso del Tribunale, il quadro normativo nazionale (primario, con riferimento all'art. 43-*bis* l.a.; così come di carattere attuativo, ad opera della Delibera AGCOM 3/2023) presenta dubbi di compatibilità rispetto alle indicazioni rinvenibili nella direttiva CDSM, giacché risulta accresciuto non soltanto di una fondamentale connotazione economica (il diritto all'equo compenso non disciplinato dall'art. 15 direttiva CDSM), ma anche di un corredo di obblighi (a carico degli ISSP) e di poteri di intervento, determinativi, ispettivi e sanzionatori (in favore dell'AGCOM), i quali non trovano riscontro e/o fondamento nella disciplina unionale.

Sotto questo profilo, il TAR non ha mancato di rilevare come simili perplessità siano state sollevate, nella fase di consultazione interistituzionale che ha preceduto l'emanazione del D.lgs. 177/ 2021, anche dall'Autorità Garante della Concorrenza e del Mercato (**AGCM**). Quest'ultima, infatti, con parere AS1788, reso in data 8 settembre 2021, ha osservato come la disposizione (poi) contenuta nell'art. 43-*bis* l.a. travalichi i limiti posti dal legislatore europeo e dalla delega parlamentare, introducendo fattispecie soggettive e oggettive non previste dalla disciplina europea e individuando meccanismi negoziali e autoritativi limitativi della libertà contrattuale degli operatori economici. La stessa AGCM ha, peraltro, rilevato che le modalità di recepimento in Italia dell'art. 15 direttiva CDSM non trovano riscontro nelle esperienze maturate in alcuni dei principali Stati membri che hanno già concluso l'iter di recepimento, indicando a tal proposito che mentre la legge tedesca, approvata il 20 maggio 2021 ed entrata in vigore il 1° agosto 2021, prevede il riconoscimento della tutela in commento mediante una trasposizione letterale del testo della direttiva, la legge francese (legge 24 luglio 2019, n. 2019-775) stabilisce che il diritto connesso può essere concesso in licenza dagli editori e affidato in gestione a uno o più organismi di gestione collettiva.

La difformità dei contenuti dell'art. 43-*bis* l.a. (e delle derivate disposizioni regolamentarie introdotte da AGCOM) rispetto alle previsioni di cui all'art. 15 direttiva CDSM, ha pertanto indotto il TAR a disporre rinvio pregiudiziale alla CGUE, ai sensi dell'art 267 TFUE, onde sottoporre ad essa la compatibilità delle disposizioni dettate dalla Delibera AGCOM 3/2023 con i principi:

- di autonomia contrattuale e di libertà di esercizio dell'iniziativa economica (artt. 16 e 52 della Carta dei Diritti Fondamentali dell'Unione Europea [innanzi **CDFUE**]);
- di libera prestazione dei servizi (art. 56 TFUE e art. 16 della direttiva 2006/123/CE "Direttiva Servizi");
- di libertà di concorrenza (artt. 10 e 119 TFUE);
- di proporzionalità (art. 52 della CDFUE).

In ordine a quest'ultimo aspetto, il TAR, richiamando le considerazioni espresse dalla CGUE nella sentenza resa in data 26 aprile 2022 sulla causa C-401/19, avente ad oggetto l'interpretazione dell'art. 17 della direttiva CDSM e, quindi, degli obblighi incombenti sui prestatori di servizi di condivisione di contenuti online al fine di tutela del diritto d'autore, ha osservato come la previsione di un equo compenso *comunque* dovuto da parte delle piattaforme agli editori, riveli carattere non proporzionato, non solo con riferimento alla tutela del diritto alla comunicazione e/o all'informazione, ma soprattutto a fronte della omogeneizzazione delle pubblicazioni giornalistiche (tutelate con la previsione di un equo compenso, in aggiunta ai diritti esclusivi), rispetto ai contenuti (parimenti diffusi in rete) protetti dal diritto d'autore; e, da ultimo, con riferimento ai significativi poteri di intervento – anche sulla libertà negoziale delle parti – riconosciuti dalla legislazione nazionale in favore dell'AGCOM.

Alla luce di tali rilievi, il TAR ha rimesso alla valutazione della CGUE le seguenti questioni pregiudiziali:

1) se l'art. 15 direttiva (UE) 2019/790 possa essere interpretato come ostativo all'introduzione di disposizioni nazionali – quali quelle previste dall'art. 43-bis della legge sul diritto di autore e quelle stabilite nella Delibera AGCOM 3/23/CONS – nella parte in cui:

1.a) vengono previsti obblighi di remunerazione (equo compenso), in aggiunta ai diritti esclusivi indicati dallo stesso art. 15 direttiva (UE) 2019/790, a carico degli ISSP ed in favore degli editori;

1.b) vengono stabiliti obblighi, a carico dei medesimi ISSP:

- di avviare trattative con gli editori,

- di fornire agli editori stessi ed alla Autorità regolatoria le informazioni necessarie ai fini della determinazione dell'equo compenso,

- nonché di non limitare la visibilità dei contenuti dell'editore nei risultati di ricerca in attesa del perfezionamento della negoziazione;

1.c) viene conferito all'Autorità regolatoria (AGCom):

- un potere di vigilanza e sanzionatorio,

- il potere di individuare i criteri di riferimento per la determinazione dell'equo compenso,

- il potere di determinare, nel caso di mancato accordo fra le parti, l'importo esatto dell'equo compenso;

2) se l'art. 15 direttiva (UE) 2019/790 sia ostativo a disposizioni nazionali, quali quelle indicate al precedente punto 1), che impongono ai fornitori di servizi della società dell'informazione (ISSP) un obbligo di divulgazione dei dati, assoggettato a vigilanza da parte della stessa Autorità regolatoria nazionale, la cui inosservanza incontra l'applicabilità di misure sanzionatorie amministrative;

3) se i rammentati principi di libertà di impresa di cui agli articoli 16 e 52 della Carta dei diritti fondamentali dell'Unione Europea, di libera concorrenza di cui all'art. 109 TFUE e di proporzionalità di cui all'art. 52 della Carta dei Diritti Fondamentali dell'Unione Europea, ostino a disposizioni nazionali, quali quelle precedentemente indicate, che:

3.a) introducono diritti di remunerazione in aggiunta ai diritti esclusivi di cui all'art. 15 direttiva (UE) 2019/790, la cui attuazione trova corredo nella già richiamata configurazione, a carico dei fornitori di servizi della società dell'informazione (ISSP), di un obbligo di avviare trattative con gli editori, di un obbligo di fornire agli editori e/o all'Autorità regolatoria nazionale le informazioni necessarie per determinare un equo compenso, nonché un obbligo di non limitare la visibilità dei contenuti dell'editore nei risultati di ricerca in attesa di tali trattative;

3.b) conferiscono a quest'ultima:

- un potere di vigilanza e sanzionatorio,

- il potere di individuare i criteri di riferimento per la determinazione dell'equo compenso,

- il potere di determinare, nel caso di mancato accordo fra le parti, l'importo esatto dell'equo compenso».

Da ultimo, alla luce della immediata esecutività delle disposizioni censurate da Meta, il TAR ha disposto la sospensione dell'efficacia della Delibera AGCOM 3/2023 oggetto di gravame, nelle more della definizione della questione pregiudiziale rimessa alla CGUE.

FRANCESCO SANTONASTASO

Delibera AGCOM 3/2023 3/2023:
https://www.agcom.it/documents/10179/29302270/Delibera+3-23-CONS/58624bf3-1ff2-4e09-9c49-8561db808984?version=1.2

Regolamento AGCOM (Allegato A alla Delibera AGCOM 3/2023 3/2023):
https://www.agcom.it/documents/10179/29302270/Allegato+25-1-2023/58525b07-198f-46de-93c8-bd7e3a7a162e?version=1.0

2023/4(30)DDA

30. Il primo provvedimento in USA nel caso Stable Diffusion sulla richiesta di protezione del copyright contro i sistemi di IA generativa: *fair use* o non *fair use*?

Il 30 ottobre 2023, la United States District Court, Northern District of California emetteva un'ordinanza procedimentale c.d. "*Order on Motion to Dismiss and Strike*" (Case No. 23-cv-00201-WHO) nella *class action* promossa da Sarah Anderson, Kelly McKernan, Karla Ortiz ed altri artisti contro Stability AI Ltd e Stability AI Inc. (un software "libreria" di intelligenza artificiale che fornisce servizi di generazione di immagini) e altri (DeviantArt Inc. e Midjourney Inc).
Gli attori sostenevano che i convenuti avessero copiato milioni di immagini protette dal copyright al fine dell'addestramento dei sistemi di Intelligenza Artificiale (IA) Generativa, senza aver ottenuto l'autorizzazione preventiva da parte dei titolari dei diritti.
La condanna richiesta dagli attori nei confronti dei convenuti si sostanzia nella responsabilità per violazione diretta del diritto d'autore (17 U.S.C. § 106); per violazione indiretta del diritto d'autore (17 U.S.C. § 106); per violazione del Digital Millenium Copyright Act (17 U.S.C. §§ 1201-1205); per violazione del diritto all'immagine (California Civil Code § 3344) e per concorrenza sleale (California Business & Profession Code). Solo nei confronti di DeviantArt è stata proposta un'azione di risarcimento per violazione contrattuale dei termini e condizioni del sito web che proibirebbero l'utilizzo di contenuti a fini commerciali.

ll provvedimento in commento, pur avendo natura endoprocedimentale, perchè volto a cristalizzare il processo, delineando il perimetro delle domande che saranno oggetto della decisione finale del giudice, è di spunto per alcune prime riflessioni sulla questione se l'attività di addestramento, c.d. *training*, da parte dei sistemi di intelligenza artificiale generativa, avente ad oggetto opere e materiali protetti, sia da considerarsi in violazione del copyright oppure un'attività legittima in quanto rientrante nella dottrina statunitense del "fair use" (US Copyright Act, Sect. 107). Come noto, nel sistema di *common law*, il *fair use* ha la stessa funzione dell'istituto delle eccezioni e limitazioni adottato dai sistemi di civil law, ossia quello di trovare un bilanciamento tra l'interesse dei titolari alla protezione dei diritti e quello della collettività all'accesso alla cultura.
Secondo la dottrina del *fair use* statunitense, per decidere se un'attività sia o meno lecita, il giudice deve valutare quattro circostanze: 1) l'oggetto e la natura dell'uso, ovvero se questo ha natura commerciale oppure didattica e senza scopo di lucro; 2) la natura dell'opera protetta; 3) la quantità e la rilevanza della parte utilizzata rispetto al complesso dell'opera protetta; e, infine, 4) le conseguenze di tale utilizzo sul mercato potenziale o sul valore dell'opera protetta. Inoltre, il preambolo alla Section 107 dell'U.S. Copyright Act, fornisce un elenco non tassativo di finalità per le quali è consentito l'utilizzo di materiale protetto senza dover chiedere la preventiva autorizzazione, ossia nel caso di uso ai fini di critica, commento, informazione, insegnamento e ricerca. È ampia la discrezionalità del giudice nella decisione se ravvisare un caso di *fair use;* come è intuibile dall'uso dell'espressione "*such as*" per indicare le finalità che consentono il *fair use* e del "*shall include*" che precede l'elenco dei quattro fattori. Il giudice è tenuto a valutare complessivamente i suddetti quattro fattori al fine di delineare o meno un uso consentito.
Stability AI è accusata di aver scaricato o in altro modo acquisito da internet copie di milioni di immagini protette dal copyright, senza autorizzazione, per l'addestramento e la creazione di Stable Diffusion, attraverso i servizi di LAION (Large Scale Artificial Intelligence Open Network). Stable Diffusion è un modello di apprendimento profondo, da testo a immagine, rilasciato nel 2022 ed utilizzato principalmente per generare immagini specifiche, secondo la descrizione testuale indicata nella richiesta dell'utente del sistema. Stability AI ha prodotto DreamStudio, anch'esso rilasciato nell'agosto 2022, che funziona come "interfaccia utente" che accede a "una versione addestrata di Stable Diffusion". L'uso di DreamStudio viene fatturato in pacchetti di crediti che possono essere utilizzati per creare immagini.
Il secondo convenuto è DeviantArt Inc., società fondata nel 2000 e conosciuta principalmente come una "comunità online" dove gli artisti digitali pubblicano e condividono le loro opere. DeviantArt ha rilasciato "DreamUp" nel novembre 2022, un prodotto commerciale che si basa su Stable Diffusion per produrre immagini e che è disponibile solo per i clienti abbonati a DeviantArt. Gli attori lamentano che almeno un set di dati LAION (incorporato in Stable Diffusion per l'addestramento delle immagini) è stato utilizzato attraverso lo *scraping* di numerosi siti web, tra cui DeviantArt. Di conseguenza, gli stessi sostengono che Stability ha illegittimamente copiato da DeviantArt milioni di immagini di addestramento create da artisti abbonati a DeviantArt.
Il terzo convenuto, Midjourney Inc., ha creato e distribuisce l'omonimo prodotto commerciale,

lanciato in forma beta nel luglio 2022. Midjourney è in grado di produrre immagini in risposta alle richieste di testo, con lo stesso funzionamento di DreamStudio e DreamUp. Gli attori sostengono che Midjourney utilizza le stesse immagini che sono state oggetto di addestramento di Stable Diffusion. Midjourney è offerto agli utenti online di Discord (piattaforma statunitense di VoIP, messaggistica istantanea e distribuzione digitale), nonché attraverso un'applicazione, a fronte di un servizio a pagamento. L'amministratore delegato di Midjourney ha dichiarato che quest'ultimo utilizza grandi insiemi di dati aperti, il che implica che abbia utilizzato per l'addestramento anche i dataset di LAION. Nell'agosto del 2022, Midjourney ha rilasciato una versione beta utilizzando Stable Diffusion.

Le doglianze degli attori sostengono che sistemi di IA, come Stable Diffusion, DeviantArt e Midjourney sono stati "addestrati" con le opere d'arte da loro create per generare immagini, nella fase di output, "nello stile" di determinati artisti. Gli utenti che utilizzano tali sistemi, inseriscono nei programmi delle richieste c.d. "*prompt*" di testo, per richiedere alla macchina di generare immagini nello "stile" di un artista noto. Le nuove immagini sono generate attraverso un procedimento matematico che si basa interamente sulle immagini di addestramento e, pertanto, devono considerarsi "derivate" da queste ultime.

La Corte sottolinea come gli attori abbiano anche ammesso che "in generale, nessuna delle immagini di output di Stable Diffusion fornite in risposta a un particolare prompt di testo corrisponda a un'immagine specifica nei dati di addestramento".

Difatti, i modelli di deep learning non archiviano una copia dei loro dati per l'addestramento, ma ne codificano una versione con punti dati simili ma più vicini tra loro. In un secondo momento questa rappresentazione viene decodificata per generare dati nuovi e originali con caratteristiche analoghe.

La prova della responsabilità dei convenuti per le singole fattispecie di violazioni delle quali si richiede la condanna non è agevole da un punto di vista tecnico-giuridico. Difatti, il Tribunale concedeva agli attori la possibilità di emendare l'atto introduttivo del giudizio per chiarire le loro teorie difensive circa il modo in cui ciascun convenuto abbia violato i diritti d'autore degli attori, rimosso o alterato le informazioni sulla gestione dei diritti d'autore o abbia violato i diritti di immagine, fornendo all'uopo le prove a sostegno.

In tema di tutelabilità delle opere protette dal diritto d'autore, la discussione si è incentrata sull'opposizione da parte dei convenuti alla tutela delle opere degli attori che non siano state registrate secondo il sistema dell'U.S. Copyright Office. Altra questione attiene, invece, all'onere a carico degli attori dell'identificazione specifica delle opere (registrate) oggetto di violazione. La semplice indicazione di una pagina web (https://haveibeentrained.com), ove ricercare le opere oggetto di addestramento non è considerata utile e sufficiente a soddisfare l'onere di identificazione, in quanto non consente una pronta identificazione delle specifiche opere registrate ed utilizzate per l'addestramento, ma si basa sul risultato offerto dalla ricerca con il nome del singolo artista. È necessario dimostrare, dall'esame delle immagini di output fornite dalla ricerca, che le opere oggetto di addestramento, coinvolte nell'attività di *scraping* da parte di LAION, siano riconducibili ad un determinato artista. Secondo il Tribunale unicamente la domanda di responsabilità per violazione diretta del diritto d'autore nei confronti di Stability risulta sufficientemente provata dagli attori e, pertanto, la richiesta di rigetto dei convenuti non veniva accolta.

Più tortuosa appare la via per definire gli ambiti di responsabilità di DevianArt sul presupposto che Stable Diffusion contiene copie compresse delle immagini utilizzate per l'addestramento e che tali immagini sono state poi utilizzate da DevianArt attraverso Dream Up. In tale senso, il Tribunale richiedeva agli attori di specificare le loro domande fornendo una definizione di "copie compresse" delle immagini di training, per dimostrare come Stable Diffusion operi con riguardo alle immagini suddette. Partendo dal presupposto che le immagini compresse di training, attraverso algoritmi e istruzioni di metodi matematici e statistici, sono state ricompilate in tutto o in parte per creare le immagini di output, è onere degli attori chiarire tale assunto e fornirne prova. Non è chiaro al Tribunale, inoltre, se DeviantArt e Midjourney contengano unicamente algoritmi e istruzioni che possono essere utilizzati per la generazione di immagini che includono solo alcune parti delle immagini utilizzate per il training o se le stesse società convenute possano essere considerate responsabili di violazione diretta del copyright per avere concesso ai propri clienti di utilizzare la libreria di immagini di Stable Diffusion. Inoltre, per poter lamentare la responsabilità per violazione diretta del diritto d'autore, gli attori devono chiarire in che modo DreamUp generi immagini di output che possono considerarsi opere derivate dalle immagini di training e dimostrare che tali immagini di output siano sostanzialmente simili alle opere protette.

L'analisi del provvedimento giurisprudenziale è rilevante anche per la valutazione della tutela delle informazioni sul regime dei diritti che identificano

l'opera nella sua veste digitale (DMCA, 17 U.S.C. §§ 1201-1205). Le informazioni sul regime dei diritti includono il titolo dell'opera e ogni altra informazione identificativa della stessa, incluse le informazioni che, nelle forme d'uso, sono inserite nei crediti in merito alla paternità del diritto morale dell'opera stessa. La legislazione statunitense è stata una delle prime a prevedere una disciplina a tutela delle informazioni sul regime dei diritti delle opere sfruttate in ambiente digitale e vieta ogni forma di rimozione o alterazione dolosa delle stesse; nonché la distribuzione o importazione per la distribuzione di opere di cui si conosca che le informazioni suddette siano state rimosse o alterate senza l'autorizzazione del titolare dei diritti. Le informazioni sul regime dei diritti rispondono all'esigenza di attribuzione della paternità dell'opera in ambiente digitale, quale espressione del diritto morale d'autore. L'attribuzione può essere fornita in diversi modi, sia citando l'autore, sia fornendo un link di collegamento alla fonte dell'opera. Seppure nella tradizione della legislazione statunitense sul copyright, il diritto morale non riceve un'alta protezione, la Section 1202 dell'U.S. Copyright Act ha riconosciuto ai titolari dei diritti (e non solamente all'autore) la possibilità di richiedere una tutela giudiziale in caso di rimozione o alterazione delle informazioni sul regime dei diritti da parte di terzi. Anche in questo contesto, gli attori non sono stati ancora in grado di fornire le prove della violazione riguardante le informazioni sul regime dei diritti delle immagini oggetto di scraping, di addestramento e utilizzate per la successiva generazione dell'immagine di output da parte dei rispettivi convenuti. L'elemento psicologico del dolo, previsto dalla disciplina, deve essere provato da parte degli esponenti. Inoltre, vi è un'ulteriore lacuna dovuta alla mancanza di specifica indicazione da parte degli attori di quali fossero state le informazioni sul regime dei diritti indicate nelle opere disponibili on line, né sono stati portati all'attenzione fatti che dimostrino in modo plausibile che quando le immagini sono state oggetto di scraping e incluse nei dataset di apprendimento, le informazioni sul regime dei diritti siano state rimosse; né fatti che dimostrino in modo plausibile che ciascun convenuto fosse a conoscenza che le informazioni stesse fossero oggetto di scraping e che tale condotta avrebbe "indotto, consentito, facilitato o occultato una violazione". Qualora quest'ultima violazione fosse accertata, si porrebbero dei problemi di violazione del diritto morale d'autore nell'utilizzo delle opere da parte dei sistemi di IA generativi.

Allo stato, difatti, i sistemi di IA generativa non riconoscono l'attribuzione dei contenuti utilizzati per l'addestramento volto alla generazione dell'output, e non sembrano aver rispettato il diritto di attribuzione che la legislazione sul copyright impone agli utilizzatori delle opere, sempre sul presupposto che i titolari dei diritti abbiano fornito tali informazioni. La tecnologia dovrebbe garantire che, anche nel contesto delle emergenti modalità di sfruttamento delle opere dell'ingegno, il diritto morale alla paternità (così come il diritto morale all'integrità dell'opera) sia rispettato, fornendo l'attribuzione alle opere che sono state utilizzate per l'addestramento nell'output generato dal sistema di IA. La procedura di attribuzione non è di agevole risoluzione in quanto non è facile stabilire quali determinate opere siano state utilizzate per generare uno specifico output e ciò necessariamente implica trasparenza sui dati di input.

Le modalità di utilizzo delle opere da parte dei sistemi di intelligenza artificiale generativa dovranno essere comprese a fondo dal punto di vista tecnologico, per poter efficacemente esercitare i mezzi di tutela previsti dall'ordinamento, affinché i giudici possano applicare la normativa esistente alla fattispecie specifica. Qualora l'attività di addestramento di opere protette senza la concessione della relativa autorizzazione da parte dei titolari dei diritti sarà considerata o meno rientrante nella dottrina del fair use, tale decisione avrà rilievo anche per la tutelabilità delle informazioni sul regime dei diritti.

Per poter, quindi, procedere all'esame del merito del caso di specie, fatta eccezione solo per la domanda volta ad accertare la violazione diretta del copyright da parte di Stability AI, il Tribunale ha accolto le richieste di rigetto presentate dai convenuti, con la riserva per gli attori di poter integrare le loro difese.

DEBORAH DE ANGELIS

https://storage.courtlistener.com/recap/gov.uscourts.cand.407208/gov.uscourts.cand.407208.1.0.pdf

2023/4(31)EB

31. La causa intentata dal NYT contro Open AI e Microsoft per la IA generativa

Il 27 dicembre 2023 The New York Times Company ("**The Times**") editore del giornale New York Times ("**NYT**") ha citato in giudizio Microsoft Corporation ("**Microsoft**") e una serie di società del gruppo di OpenAI Inc. (collettivamente "**OpenAI**"), di fronte alla Southern District Court of New York, chiedendo il risarcimento dei danni (da

quantificarsi) per violazione di copyright e atti di concorrenza sleale, oltre che l'inibitoria dalla continuazione della violazione e la distruzione di tutti i modelli GPT (e di ogni altro modello linguistico di grandi dimensioni "**LLM**") che abusivamente contengano opere dell'ingegno di titolarità della storica testata giornalistica.

La causa promette già di diventare un *leading case*. L'oggetto del contendere concerne infatti la legittimità da parte di strumenti di intelligenza artificiale generativa ("**GenAI**") – che nel caso di OpenAI si basano su LLM – di addestramento tramite l'utilizzo di materiale protetto da copyright, tra cui articoli del NYT. La ricorrente lamenta la particolare importanza data ai contenuti del NYT tra le numerose fonti utilizzate per costruire gli LLM della convenuta, rivelando una preferenza che riconosce il valore di queste opere. Inoltre – ed ecco spiegata la citazione anche di Microsoft – la ricorrente lamenta pratiche di concorrenza sleale perpetrate attraverso Bing Chat (recentemente ribattezzato 'Copilot') e ChatGPT, con cui i convenuti cercherebbero di sfruttare i massicci investimenti di The Times nel suo giornalismo, utilizzandoli per creare prodotti sostitutivi senza autorizzazione o pagamento di un equo compenso.

Andando al merito della questione, The Times sostiene che il *tool* generativo di OpenAI genererebbe un output capace di replicare, riassumere fedelmente e imitare lo stile espressivo dei contenuti protetti di titolarità del giornale, allegando a supporto numerose prove.

Inoltre, The Times ha denunziato il verificarsi di quelle che vengono definite "allucinazioni" ossia il fenomeno per cui, secondo la definizione datane dallo stesso ChatGPT: "una macchina, come ad esempio un *chatbot*, genera esperienze sensoriali apparentemente realistiche che non corrispondono a nessun input reale". Per cui i modelli GPT invece di astenersi dal rispondere, asseritamente forniscono con sicurezza informazioni che non sono del tutto accurate e, nel peggiore dei casi, dimostrabilmente (ma non riconoscibilmente) false. La conseguenza è che i revisori umani troveranno molto difficile distinguere le "allucinazioni" dall'output veritiero. Ciò è in grado di generare un danno reputazionale alla testata giornalistica laddove le viene attribuita la fonte di queste dichiarazioni false. A ciò si aggiunga un potenziale danno per la società tutta, nella misura in cui, sotto il marchio di una autorevole testata giornalistica, siano diffuse *fake news*, compromettendo quindi il diritto all'informazione.

L'ulteriore pratica denunciata attiene all'utilizzo che ChatGPT farebbe dell'indice di ricerca Bing di Microsoft: il *chatbox* copierebbe e categorizzerebbe i contenuti del Times pubblicati online, per generare risposte che contengono estratti e riassunti di articoli del giornale, significativamente più lunghi e dettagliati rispetto a quelli restituiti dai motori di ricerca tradizionali. Il rischio è che in tal modo si finirebbe per fornire contenuti senza il permesso o l'autorizzazione dei titolari dei diritti, non solo compromettendo il rapporto con i lettori, ma privando il giornale di entrate significative derivanti da abbonamenti, licenze, pubblicità e affiliazioni, in quanto i consumatori non sarebbero più incentivati a pagare per ottenere informazione.

A sostegno di ciò il NYT ha enfatizzato quanto questa violazione di copyright sia stata estremamente redditizia per gli imputati: la distribuzione da parte di Microsoft di LLM addestrati dal Times in tutta la sua linea di prodotti avrebbe asseritamente contribuito ad aumentare la sua capitalizzazione di mercato di un trilione di dollari solo nell'ultimo anno ed inoltre, il rilascio da parte di OpenAI di ChatGPT ha portato la sua valutazione fino a 90 miliardi di dollari.

Per supportare le proprie argomentazioni, il New York Times ha fatto specifico riferimento ai set di dati utilizzati nello sviluppo della versione GPT-2, per la quale OpenAI aveva divulgato alcune informazioni. Tra queste informazioni si evidenziava l'inclusione del set di dati denominato "WebText", composto da 45 milioni di collegamenti pubblicati dagli utenti del social network Reddit. Il "WebText" era stato creato come una selezione speciale di contenuti online caratterizzati da un elevato livello qualitativo, e al suo interno il dominio "NYTimes.com" era notevolmente presente, occupando il quinto posto con 333.160 voci. Nella versione GPT-3 era stato utilizzato un "WebText2", anch'esso creato con collegamenti provenienti da Reddit, e in questo corpus il New York Times rappresentava la prima fonte proprietaria e la terza in assoluto dopo Wikipedia e il database dei brevetti statunitensi. Sulla base di tali informazioni, il New York Times deduceva che nella più recente versione GPT-4, i suoi contenuti protetti avrebbero dovuto essere presenti ed utilizzati in modo ancora più massivo.

A ulteriore conferma della presunta violazione, il New York Times ha prodotto dei documenti rappresentati la situazione in cui, utilizzando specifici input relativi ad importanti inchieste giornalistiche del Times, ChatGPT generava contenuti identici agli articoli stessi del Times bypassando di fatto le misure tecniche di protezione applicate al sito web dal titolare dei diritti (es. *paywall*).

Questa riproduzione non si limitava ai contenuti storici, ma, grazie all'interazione con il motore di

ricerca Bing, era in grado di recuperare anche gli articoli di attualità più recenti pubblicati dal Times. In altre parole, mentre in passato i motori di ricerca erano in grado di mostrare solo *snippets*, spingendo l'utente ad accedere al sito del giornale per ottenere informazioni più dettagliate, nel contesto attuale il motore di ricerca poteva fornire una sintesi estesa all'utente, eliminando la necessità di accedere al sito originale.

OpenAI, dal canto suo, ha tentato di ricondurre la sua attività all'esenzione del "*fair use*" statunitense, invocando la natura "trasformativa" dell'utilizzo fatto delle opere protette. *Incidenter tantum*, si ricorda come l'eccezione del fair use è contenuta alla Section 107 del Copyright Act, costituita da un meccanismo che possiamo dire simile, per metodologia normativa, al three-step-test europeo, seppur il contenuto dei criteri decisionali previsti alla Section 107 siano diversi (anche se sostanzialmente compatibili).

Nello specifico, ai fini della determinazione se l'uso di un'opera in un caso particolare costituisca un "fair use", i fattori da prendere in considerazione includono:

(1) lo scopo e la natura dell'uso, compreso se tale utilizzo ha carattere commerciale o è finalizzato a scopi educativi senza fini di lucro;

(2) la natura dell'opera protetta da copyright;

(3) la quantità e la sostanzialità della porzione utilizzata rispetto all'opera protetta da copyright nel suo complesso;

(4) l'effetto dell'uso sul mercato potenziale o sul valore dell'opera protetta da copyright. Il fatto che un'opera non sia stata pubblicata non costituirà di per sé un impedimento a una valutazione di "fair use" se tale valutazione viene effettuata tenendo conto di tutti i fattori sopra menzionati.

In virtù di quanto sopra, il NYT ha comprensibilmente replicato, contestando l'uso trasformativo invocato, chiedendo il risarcimento dei danni sofferti.

L'azione del giornale non è un caso isolato, difatti altri autori si sono attivati per tutelare la propria posizione: il 19 settembre 2023 è stata infatti presentata una denuncia da parte di 17 autori appartenenti alla Authors Guild (la più prestigiosa organizzazione professionale che rappresenta gli scrittori americani), fra i quali George R. R. Martin, John Grisham e Jonathan Franzen, chiedendo di vietare l'uso di libri protetti da copyright per la creazione di modelli linguistici senza licenza, oltre a un risarcimento dei danni. Si ricordano inoltre anche le richieste sindacali avanzate a partire dal maggio del 2023 dall'associazione degli sceneggiatori americani (Writers Guild of America), che nel tentativo di tutelare gli autori di Hollywood dall'invasione dell'AI. Alla loro protesta si è unito successivamente anche il sindacato degli attori americani (la Screen Actors Guild-American Federation of Television and Radio Artists). Gli obiettivi dei due sindacati erano diversi: gli sceneggiatori volevano assicurarsi che l'AI non potesse essere addestrata sul loro lavoro o manipolarlo senza il loro consenso; gli attori volevano invece introdurre dei limiti all'uso della AI per ricreare le loro performance.

Di contro, altri operatori del mercato hanno assecondato l'AI generativa, come ad esempio Axel Springer, l'editore tedesco e politico, il quale ha annunciato il 13 dicembre 2023 una partnership globale con OpenAI consentendo che ChatGPT fornisca agli utenti degli estratti di notizie pubblicate sulle testate del gruppo di sua proprietà. O ancora, Associated Press, una delle più prestigiose agenzie di stampa statunitensi ha concesso a OpenAI l'accesso a parte del proprio archivio testuale. Come corrispettivo l'agenzia ha ottenuto l'accesso alla tecnologia di OpenAI. Le due aziende hanno dichiarato che stanno esaminando potenziali casi d'uso per l'AI generativa in prodotti e servizi giornalistici, avendo come scopo quello di un uso responsabile dei sistemi di intelligenza artificiale.

L'azione intentata dal New York Times resta comunque considerevole, in ragione della quantità di opere coinvolte. Inoltre, la portata giuridica delle questioni poste è destinata a segnare una tappa importante in tema di AI generativa; queste investono infatti la legittimità dell'uso per il training di sistemi di intelligenza artificiale di ampie basi di dati contenenti opere dell'ingegno. Inoltre, quello che deciderà la corte statunitense è di fondamentale importanza anche in Europa, dove il dibattito è molto accesso in ragione della recente introduzione della c.d. eccezione di text and data mining (artt. 3 e 4 della direttiva (UE) 2019/790) e ancor di più in ragione della prossima approvazione del testo definitivo dell'AI Act, in cui si rintraccia un riferimento esplicito alla necessità per i modelli e i sistemi di IA di rispettare il regime del text and data mining di cui alla citata direttiva (UE) 2019/790. L'azione del NYT è quindi certamente significativa se si considerano i diritti in gioco, tra cui i principali: diritto all'informazione, diritto all'immagine, diritto d'autore, accesso democratico ai contenuti.

EMANUELA BURGIO

https://www.documentcloud.org/documents/24238498-nyt_complaint_dec2023

2023/4(32)FG

32. La prima sentenza cinese che riconosce a certe condizioni all'utente del software il diritto d'autore sugli ouput ottenuti da un sistema di IA generativa (caso Li Yunkai *v*. Liu Yuanchun)

Il 27 novembre 2023, la Beijing Internet Court ha emanato una sentenza riconoscendo, ai sensi della normativa cinese sul diritto d'autore la tutelabilità delle immagini generate da sistemi di intelligenza artificiale generativa, in favore di un essere umano utente del software (caso Li Yunkai *v*. Liu Yuanchun).

La Corte è giunta a tale conclusione sulla base della constatazione che lo sforzo intellettuale effettuato dagli utenti del software, come la scelta deliberata delle immagini, la selezione delle istruzioni per guidare l'output creativo (cd. prompt), la disposizione dell'ordine delle parole chiave utilizzate nei prompt e la scelta dei parametri tecnici del software, sia sufficiente a riflettere l'espressione e l'originalità dell'autore umano.

Mr. Li Yunkai ha convenuto in giudizio Ms Liu Yuchuan, una blogger, per violazione dei propri diritti d'autore su un'immagine generata tramite Stable Diffusion, un sistema di IA generativa text-to-image.

In particolare, parte attrice aveva utilizzato Stable Diffusion per realizzare una serie di immagini [denominate "La brezza primaverile porta tenerezza - Immagine generata da un sistema di intelligenza artificiale" (春风送来了温柔)] e aveva pubblicato queste immagini sul social network cinese "Little Red Book" usando uno pseudonimo.

Il 2 marzo 2023, la convenuta ha pubblicato un articolo intitolato "Amore a marzo, durante la fioritura del pesco" (三月的爱情,在桃花里) sulla piattaforma Baijiahao utilizzando senza autorizzazione una delle immagini che parte attrice aveva generato utilizzando Stable Diffusion.

Mr. Li ha ritenuto che la convenuta abbia copiato l'immagine rimuovendo sia il suo ID utente sia il watermark dalla copia originale e l'abbia riprodotta nel suo articolo online in violazione del suo diritto di paternità e del diritto di comunicazione al pubblico e, per tale ragione, ha chiesto in giudizio la pubblicazione di scuse pubbliche sulla piattaforma Baijiahao da parte della convenuta e il pagamento di 5.000 RMB (circa 640 EUR) come risarcimento danni.

La Beijing Internet Court si è pronunciata in merito ai seguenti quesiti: (1) se l'immagine generata dal sistema di IA in questione costituisca un'opera tutelabile secondo la normativa sul diritto d'autore cinese ("Copyright Law of the People's Republic of China"); (2) in caso di risposta affermativa, se parte attrice sia il titolare dei diritti d'autore sull'immagine generata dal sistema di IA; e infine (3) se la convenuta debba essere ritenuta responsabile per la violazione del diritto d'autore per avere utilizzato senza autorizzazione l'immagine in questione.

Sulla prima questione, la Beijing Internet Court ha stabilito che l'immagine utilizzata dalla convenuta e generata dal sistema di IA ("La brezza primaverile porta tenerezza") costituisca una creazione artistica tutelata dal diritto d'autore.

Per giungere a tale conclusione, la Beijing Internet Court ha effettuato la sua analisi considerando: (1) se l'opera rientra nei campi della letteratura, dell'arte e della scienza; (2) se possiede il requisito dell'originalità; (3) se ha una forma specifica di espressione; e infine (4) se è una creazione intellettuale (da parte di esseri umani).

Per quanto riguarda il primo e il terzo criterio, la Corte ha ritenuto che, poiché l'immagine in questione è simile a fotografie e dipinti, essa soddisfa questi due criteri.

In merito al criterio delle "creazioni intellettuali", la Corte ha confermato che un'opera tutelabile deve riflettere il contributo intellettuale degli esseri umani (come già affermato il 25 aprile 2019 nel caso "Beijing Film Law Firm contro Beijing Baidu Netcom Science & Technology Co Ltd"); nel caso di specie, parte attrice ha fornito contributi intellettuali durante il processo di generazione dell'immagine in questione, compresi la scelta del fornitore di servizi IA (i.e. Stable Diffusion) tra molti altri fornitori di servizi IA generativi per ottenere lo stile di immagine preferito, l'inserimento di circa 150 "prompts" (come ad esempio "viso angolare simmetrico, capelli intrecciati di colore castano-rossiccio, sguardo verso la fotocamera, ora dorata e illuminazione dinamica") per determinare l'output dell'immagine generata e l'impostazione di vari parametri tecnici per produrre, selezionare e riorganizzare le immagini che parte attrice preferiva. Pertanto, la Beijing Internet Court ha ritenuto che l'immagine in questione rifletta il contributo intellettuale di parte attrice, soddisfacendo così il criterio in questione.

Per quanto riguarda, infine, il criterio dell'originalità, la Corte ha stabilito che un'opera tutelabile deve essere creata dall'autore e riflettere la sua personalità. La Corte ha precisato che per determinare se l'uso del sistema di IA per generare immagini rifletta la personalità dell'autore, è necessario decidere caso per caso. Con riferimento al presente caso risultava che parte attrice, pur non avendo disegnato fisicamente l'opera (usando le sue

mani), aveva tuttavia progettato gli stili dei personaggi e organizzato la composizione finale dell'immagine, sperimentando diversi prompt e vari parametri tecnici. Era risultato in particolare che Mr. Li, dopo aver ottenuto la prima immagine, avesse fornito ulteriori istruzioni e quindi modificato i parametri tecnici del software fino ad ottenere l'immagine finale oggetto della controversia. I giudici hanno quindi concluso che l'intero processo di adattamento e riorganizzazione degli output riflettesse le scelte estetiche di parte attrice e il suo giudizio personale. Pertanto, secondo la Beijing Internet Court l'immagine in questione non è semplicemente una "creazione intellettuale meccanica", ma possiede un carattere originale.
La Corte sembra distinguere tra un output diretto (cd. "AI-Generated Work"), in cui l'autore umano semplicemente prende e utilizza l'output senza alcun coinvolgimento creativo, e un output in cui l'autore umano continua a sperimentare e ad aggiungere vari input e parametri tecnici fino a ottenere il risultato finale soddisfacente. In quest'ultimo caso, l'opera in questione è un'opera creata con l'assistenza di un sistema di IA, in cui parte attrice esercita scelte estetiche e un giudizio personale nella rappresentazione finale dell'opera: cd. "AI-Assisted Work".
La Corte si è pronunciata sulla titolarità dei diritti d'autore escludendo la possibilità che un sistema di IA stesso possa essere considerato un autore di un'opera protetta perché non è un essere umano.
La Corte ha ritenuto che neanche gli sviluppatori/fornitori del servizio potrebbero essere considerati gli autori in questo caso, poiché tali fornitori/ fornitori non avevano né l'intenzione di creare la specifica immagine né avevano effettivamente partecipato al processo di creazione dell'immagine in questione. Inoltre, in base alla "CreativeML Open RATL++-M License" di Stable Diffusion pubblicata su GitHub.com, gli sviluppatori rinunciano ai loro diritti, se presenti, nell'output affermando che non rivendicano diritti sul contenuto dell'output. Pertanto, poiché l'immagine in questione è stata generata come risultato dell'input intellettuale di parte attrice e riflette la sua personalità, è la stessa parte attrice, Mr. Li, l'autore dell'immagine.
Infine, la Corte ha ritenuto il convenuto responsabile per la violazione dei diritti d'autore di Mr. Li, per aver rimosso sia l'ID utente dell'attore sia il watermark di Little Red Book dall'immagine e per aver ripubblicato la stessa senza autorizzazione.
Sulla base di queste tre considerazioni, la Beijing Internet Court ha confermato la protezione dell'opera d'arte generata dal sistema di IA condannando il convenuto al risarcimento del danno di 500 RMB (circa 65 Euro) e al rimborso delle spese legali di 50 RMB (circa 7 Euro).
La sentenza del Beijing Internet Court potrà essere impugnata, tuttavia il convenuto ha comunicato di non aver intenzione di procedere in tal senso.
Sebbene isolata, la pronuncia in oggetto, potrebbe essere la prima di molte sentenze dello stesso tipo; i tribunali cinesi potrebbero infatti considerare le opere create tramite sistemi di IA come contenuti protetti purché vi sia un intervento umano che rifletta l'apporto personale e l'originalità dell'autore umano.

FRANCESCO GROSSI

https://mp.weixin.qq.com/s/Wu3-GuFvMJvJKJobqqq7vQ

2023/4(33)FG

33. L'ultima sentenza della Corte Suprema del Regno Unito in materia di brevetti e IA nel caso Thaler DABUS

La Corte Suprema del Regno Unito ha emanato il 20 dicembre 2023 (UKSC 49) la sentenza nel caso "*Thaler v. Comptroller General of Patents, Designs and Trade Marks*, 2023 UKSC 49". Respingendo all'unanimità il ricorso, ha ribadito come la normativa sui brevetti del Regno Unito (UK Patents Act) non consenta a un sistema di intelligenza artificiale di essere nominato inventore di un brevetto. La sentenza della Corte Suprema ha confermato quindi, non solo la decisione dello UK Intellectual Property Office (UKIPO), ma anche i provvedimenti della High Court e della Court of Appeal, di fronte alle quali erano state proposte impugnazioni (v. in questa Rubrica le precedenti notizie: notizia n.6 nel numero 4/2021: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf [2021/4(6)FG]; e notizia n. 21 nel numero 1/2023: http://www.personaemercato.it/wp-content/uploads/2023/05/Osservatorio.pdf [2023/1(21)FG]).
Nell'ambito della campagna internazionale di depositi di brevetto e ricorsi ("Artificial Inventor Project") avviata dal Dr. Stephen Thaler a partire dal 2018, per sostenere la tesi che un sistema di intelligenza artificiale debba poter essere designato come inventore in una domanda di brevetto: il dottor Thaler ha depositato nel Regno Unito due domande di brevetto che individuano "DABUS" (Device for the Autonomous Bootstrapping of Unified Sentience) come inventore e il Dr. Thaler

come proprietario del brevetto; il Dr. Thaler riterebbero di essere legittimato a presentare le domande di brevetto in qualità di proprietario del software. Le decisioni adottate in successione dall'Intellectual Property Office inglese, dalla High Court e dalla Court of Appel, sono state identiche nei contenuti, affermando che un sistema di intelligenza artificiale non possa qualificarsi come "inventore" ai sensi dell'art. 7 e 13 della legislazione inglese sui brevetti del 1977, in quanto non è una persona fisica.

In seguito alla decisione della Corte d'Appello del settembre 2021, il Dr. Thaler ha impugnato il provvedimento presentando ricorso di fronte alla Corte Suprema. È interessante evidenziare come lo UKIPO nell'ottobre 2021 abbia pubblicato una consultazione sui sistemi di intelligenza artificiale e i brevetti in cui chiedeva opinioni sui seguenti aspetti:

1) Se la definizione di inventore dovesse essere ampliata per includere gli esseri umani responsabili di un sistema di intelligenza artificiale che concepisce invenzioni; o
2) Se la legge dovesse andare oltre e consentire di identificare un sistema di intelligenza artificiale come inventore.

La consultazione si è conclusa nel gennaio 2022 e lo UKIPO ha pubblicato a giugno 2022 la sua risposta alla consultazione concludendo che non vi sono prove che la legge sui brevetti del Regno Unito sia attualmente inadeguata a proteggere le invenzioni realizzate utilizzando sistemi di intelligenza artificiale e, quindi, decidendo di non apportare modifiche alla legge nel breve termine, ha lasciato che la Corte Suprema fosse la sola a decidere se un sistema di intelligenza artificiale possa essere o meno un inventore nelle domanda di brevetto nel Regno Unito.

La Corte Suprema ha respinto all'unanimità il ricorso, precisando che lo UKIPO avesse correttamente ritenuto che le domande di brevetto dovessero considerarsi ritirate ai sensi dell'art. 10 (3) delle Patent Rules 2007 perché il Dr. Thaler non aveva ottemperato alle prescrizioni dell'art. 13(2) del Patents Act 1977 non avendo identificato una persona come inventore nelle informazioni fornite né indicato un titolo derivativo valido.

La Corte Suprema ha affrontato tre questioni fondamentali:

1. Quale sia la portata e il significato del termine "inventore" nella legge del 1977 e se si estenda a un sistema di IA come DABUS.

Sul punto, la Corte ha ritenuto che, anche ai sensi degli articoli 7 e 13 della legge sui brevetti, non sia possibile estendere il termine "inventore" a un software come DABUS e, quindi, un "inventore" debba essere necessariamente una persona fisica come precisato anche nella causa *Rhone-Poulenc Rorer International Holdings Inc v. Yeda Research and Development Co Ltd [2007] UKHL 43*. In tale occasione Lord Hoffmann aveva chiarito che l'inventore di un brevetto è la persona fisica che ha posto in essere l'attività inventiva; inoltre, la sezione 7(2) e la sezione 7(3) forniscono un codice esaustivo per decidere chi ha diritto alla concessione di un brevetto.

2. Se il Dr. Thaler fosse comunque il proprietario delle invenzioni di DABUS e avesse il diritto di chiedere e ottenere un brevetto in relazione a tali invenzioni?

Sulla seconda questione, la Corte Suprema si è pronunciata in senso negativo, in quanto il proprietario del software non è contenuto nell'elenco esaustivo delle persone che hanno diritto alla proprietà delle invenzioni quando non sono essi stessi gli inventori (es., il datore di lavoro), così come definito nelle disposizioni dell'articolo 7, paragrafo 2, lettera b) o dell'articolo 7, paragrafo 2, lettera c). Inoltre, anche la richiesta del Dr. Thaler di applicare la dottrina dell'accessione (secondo la quale, il nuovo bene prodotto dal bene esistente diviene anch'esso di proprietà del proprietario del bene esistente) è stata respinta dalla Corte sulla base della considerazione che un'invenzione non è un bene materiale e, quindi, non può passare al proprietario della macchina che lo ha creato. Secondo la Corte Suprema non esiste alcun principio che consenta al Dr. Thaler di derivare da DABUS alcun diritto sulle domande di brevetto depositate.

3. Se lo UKIPO avesse correttamente ritenuto ritirate le domande di brevetto.

Nelle circostanze sopra richiamate, lo UKIPO aveva il diritto di ritenere che il Dr. Thaler non avesse nessuno dei requisiti di cui all'articolo 13, paragrafo 2 della legge sui brevetti, in quanto né aveva indicato una persona che riteneva essere l'inventore né la proprietà di DABUS era sufficiente per accettare la sua richiesta di avere diritto alla concessione dei brevetti richiesti.

La decisione della Corte Suprema (in linea anche con le altre decisioni adottate nella maggior parte delle altre giurisdizioni nelle quali il Dr. Thaler ha presentato delle richieste simili), ha confermato le attese in quanto la necessità che l'inventore indicato nella domanda di brevetto non possa essere una macchina (o un'intelligenza artificiale) e debba essere una persona fisica, risulta chiaramente dalla legge inglese: la conseguenza, quindi, è che sulla base della legge attuale le invenzioni che sono create dall'intelligenza artificiale senza alcun

inventore umano non possono essere oggetto di brevetto nel Regno Unito

La Corte Suprema ha adottato, nel prendere la sua decisione, un approccio testuale della normativa, non prendendo in esame la questione più ampia (di competenza del legislatore e non dei tribunali) di quale potrebbe essere nel futuro la corretta protezione per le opere generate dai sistemi di intelligenza artificiale. Lord Kitchin nella parte finale della sentenza, ha precisato di essere d'accordo con quanto affermato a questo riguardo da Elisabeth Laing LJ al paragrafo 103 della sentenza della Corte d'Appello:

"Whether or not thinking machines were capable of devising inventions in 1977, it is clear to me that that Parliament did not have them in mind when enacting this scheme. If patents are to be granted in respect of inventions made by machines, the 1977 Act will have to be amended".

FRANCESCO GROSSI

https://www.supremecourt.uk/cases/docs/uksc-2021-0201-judgment.pdf