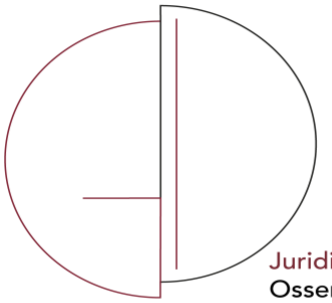

Juridical Observatory on Digital Innovation
Osservatorio Giuridico sulla Innovazione Digitale

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

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

SOMMARIO

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

ISSN 2239-8570

6. **2024/3(6)FS** Le disposizioni del 'Decreto salva infrazioni' (DL 131/2024) a completamento della liberalizzazione della gestione collettiva dei diritti d'autore - **Francesco Santonastaso**

7. **2024/3(7)RG** I primi tre decreti del Ministro della Salute previsti dalla legge sull'oblio oncologico e il vademecum del Garante privacy – **Raffaella Grisafi**

8. **2024/3(8)VR** La decisione del Garante privacy olandese del 16.5.2024 contro Clearview per illecito trattamento di dati biometrici con finalità di riconoscimento facciale. – **Valentino Ravagnani**

9. **2024/3(9)FG** L'annuncio del 26.9.2024 dal Garante privacy italiano di aver avviato un'indagine sull'accordo tra Open AI ed alcuni editori italiani di testate giornalistiche (GEDI, RCS) - **Francesco Grossi**

10. **2024/3(10)SO** L'annuncio del Garante privacy irlandese del 12.9.2024 di aver avviato un'indagine per verificare se Google ha svolto una DPIA per lo sviluppo del modello di IA 'PaLM2' – **Salvatore Orlando**

11. **2024/3(11)FP** I lavori dell'UNCITRAL nel settore del commercio digitale e l'approvazione del Model Law sulla contrattazione automatizzata (MLAC) del luglio 2024 – **Federico Pistelli**

12. **2024/3(12)GD** La storica sentenza emessa il 5.8.2024 negli USA contro Google sul monopolio nelle ricerche online e nella pubblicità degli annunci di testo (causa Stati Uniti d'America c. Google LLC, 2024 WL 3647498) – **Giorgia Diotallevi**

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

ISSN 2239-8570

2024/3(1)CC

1. La sentenza CGUE (seconda sezione) del 30.5.2024 nelle cause riunite C-662/22 e C-667/22 sul divieto ai sensi della direttiva 2000/31/CE per uno Stato membro di imporre obblighi ulteriori a un fornitore di servizi online stabilito in un altro Stato membro quali l'iscrizione in un registro, la comunicazione di informazioni e il versamento di un contributo economico (caso Airbnb Ireland UC e Amazon Services Europe Sàrl c. AGCOM).

La sentenza in oggetto si segnala poiché torna a chiarire la portata di un principio, quello del controllo nel Paese di origine, che storicamente rappresenta un presidio della certezza del diritto nello spazio dell'Unione Europea, in quanto strumento di contenimento dei rischi di frammentazione normativa e *over-regulation*; purtuttavia, potrebbe apparire come il simbolo di un residuo, fastidioso privilegio, riservato soprattutto a poche, potenti multinazionali straniere, le quali possono farsi scudo di esso per evitare l'applicazione di leggi nazionali più severe di quelle dello Stato scelto per stabilirsi. Esso, del resto, ha visto la luce (col fine di incentivare imprese con sede fuori dall'Ue a stabilire una filiale all'interno dell'Ue, evitando la possibile applicazione di una molteplicità di leggi nazionali) in un contesto molto diverso da quello attuale. Vale a dire negli anni '90 dello scorso secolo, allorché le scelte di politica legislativa in ambito europeo erano più che altro orientate a favorire la crescita e lo sviluppo di quelle che all'epoca erano *start up* dell'industria digitale, assicurando chiarezza e stabilità del quadro normativo. Oggi, il mercato interno è dominato da oligopolisti (per lo più statunitensi o cinesi) come Google, YouTube, Amazon o Tik Tok, i quali si sono potuti avvantaggiare del principio dell'*home state control* più (e a scapito) di potenziali concorrenti europei. Nel volgere dei decenni, la regola ha finito per dare ampio spazio al fenomeno del cd. *forum shopping*, spesso dissuadendo gli Stati europei dall'adozione di legislazioni più ambiziose anche per la paura di una fuga d'imprese digitali stabilite nel proprio territorio.

Non è un caso se la vicenda che ha originato le questioni devolute, in questa occasione, alla Corte di giustizia dell'Unione Europea ha visto protagoniste due multinazionali come Airbnb Ireland UC (**Airbnb**) e Amazon Services Europe Sàrl (**Amazon**), rispettivamente stabilite in Irlanda e Lussemburgo.

In breve, questi i fatti.

Alla luce di alcune modifiche del quadro normativo nazionale – derivanti, da un lato, dalla l. 30 dicembre 2020, n. 178 (art. 1, co. 515) e dall'altro, relativamente all'Autorità per le garanzie nelle comunicazioni (**AGCOM**) dalla delibera AGCOM n. 200/21 e dal provvedimento AGCOM n. 14/21, adottati in applicazione del regolamento (UE) 2019/1150 (**regolamento P2B**) – Airbnb e Amazon, in quanto fornitrici di servizi di intermediazione *online*, sono state assoggettate all'obbligo d'iscriversi in un registro tenuto dalla stessa Autorità; a comunicare una serie di informazioni

ISSN 2239-8570

nonché a versare un contributo economico. Avverso tale delibera e tale provvedimento Airbnb e Amazon hanno proposto ricorso al Tribunale amministrativo regionale per il Lazio (**TAR Lazio**), lamentando la violazione del principio della libera prestazione dei servizi, del regolamento (UE) 2019/1150 e di diverse direttive. Nell'ottobre 2022, il TAR Lazio ha proposto alla Corte di giustizia dell'Unione europea (**CGUE**) cinque domande di pronuncia pregiudiziale, vertenti sull'interpretazione: (*i*) del regolamento (UE) 2019/1150; (*ii*) della direttiva 2000/31/CE (**direttiva sul commercio elettronico**); (*iii*) della direttiva (UE) 2015/1535, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione; (*iv*) della direttiva 2006/123/CE, relativa ai servizi nel mercato interno, nonché dell'art. 56 del Trattato sul funzionamento dell'Unione europea (**TFUE**).

Il giudice del rinvio, in sostanza, ha chiesto se l'art. 56 TFUE, l'art. 16 della direttiva 2006/123/CE o l'art. 3 della direttiva 2000/31/CE debbano essere interpretati nel senso che ostano a misure adottate da uno Stato membro, allo scopo dichiarato di garantire l'adeguata ed efficace applicazione del regolamento (UE) 2019/1150, le quali, a pena di sanzioni, prevedano che i fornitori di servizi di intermediazione *online* stabiliti in un altro Stato membro siano obbligati, per poter prestare i loro servizi in Italia, a iscriversi in un registro tenuto da un'autorità di tale Stato, a comunicare a quest'ultima una serie di informazioni dettagliate sulla loro organizzazione e a versare alla stessa un contributo economico.

La CGUE, richiamando il precedente costituito dalla sentenza del 9 novembre 2023, *Google Ireland e a.*, C-376/22, ha ribadito come, sulla scorta del principio del mutuo riconoscimento, lo Stato membro di destinazione di servizi della società dell'informazione non può limitare la libera circolazione di tali servizi esigendo il rispetto di obblighi aggiuntivi, rientranti nell'ambito regolamentato. L'art. 3 della direttiva 2000/31/CE osta, salve le deroghe autorizzate alle condizioni previste al par. 4, a che uno Stato membro diverso da quello di stabilimento assoggetti il prestatore del servizio a prescrizioni nuove nell'ambito regolamentato. Nel caso di specie, hanno rilevato i giudici, è pacifico che le misure dell'AGCOM contestate abbiano imposto a fornitori di servizi di intermediazione *online* stabiliti in altri Stati membri l'adempimento di obblighi nuovi. Né è stato contestato che i servizi prestati rientrino tra i «servizi della società dell'informazione», di cui all'art. 2, lett. a), della direttiva 2000/31/CE. In contrasto con quanto sostenuto dal Governo italiano, i giudici hanno reputato che obblighi come quelli sanciti dalle misure contestate siano compresi nell'«ambito regolamentato», ai sensi dell'art. 2, lett. h), della direttiva 2000/31/CE, traendone che: «l'articolo 3 della direttiva 2000/31/CE osta a misure adottate da uno Stato membro in forza delle quali, a pena di sanzioni, i fornitori di servizi di intermediazione online, stabiliti in un altro Stato membro, sono obbligati, al fine di prestare i loro servizi nel primo Stato membro, a iscriversi in un registro tenuto da un'autorità di tale Stato membro, a comunicare a quest'ultima una serie di informazioni dettagliate sulla loro organizzazione, nonché a versare alla stessa un contributo economico».

ISSN 2239-8570

Sulla scorta di questo assunto, la CGUE ha ulteriormente puntualizzato che le misure contestate non soddisfano le condizioni di cui all'art. 3, par. 4, della direttiva 2000/31/CE: come risulta dal tenore letterale della disposizione, possono rientrare nell'ambito di applicazione di quest'ultima soltanto i provvedimenti «adottati per quanto concerne un determinato servizio della società dell'informazione». Già nella sentenza, 9 novembre 2023, *Google Ireland e a*. (C-376/22), la CGUE aveva invero chiarito che l'art. 3, par. 4, della direttiva 2000/31/CE dev'essere interpretato nel senso che provvedimenti generali e astratti, riguardanti una categoria di determinati servizi della società dell'informazione descritta in termini generali, e applicabili indistintamente a qualsiasi prestatore di tale categoria di servizi, non rientrano nella nozione di «provvedimenti adottati per quanto concerne un determinato servizio della società dell'informazione», ai sensi e agli effetti della citata disposizione. Anche nel caso di specie, alle misure contestate i giudici hanno riconosciuto portata generale e astratta, negando la qualificazione di «provvedimenti adottati per quanto concerne un determinato servizio della società dell'informazione» *ex* art. 3, par. 4, lett. a) della direttiva 2000/31/CE. Sotto un altro e rilevante aspetto, la CGUE ha posto in evidenza che i provvedimenti nazionali sono conformi a quest'ultima previsione se necessari al fine di garantire l'ordine pubblico, la tutela della sanità pubblica, la pubblica sicurezza o la tutela dei consumatori. Non sono tali quelli adottati, come nel caso *de quo*, allo scopo dichiarato di garantire l'applicazione del regolamento (UE) 2019/1150 dal momento che tale provvedimento mira a promuovere equità e trasparenza per gli utenti commerciali dei servizi di intermediazione *online*: non riguarda l'ordine pubblico, la sanità pubblica o la pubblica sicurezza.

Interessante è, infine, notare come la CGUE abbia rimarcato che la disposizione del par. 4 dell'art. 3 della direttiva 2000/31/CE deve interpretarsi restrittivamente «in quanto eccezione al principio del controllo nello Stato membro di origine» (in senso conforme le sentenze del 22 novembre 2012, *Probst*, C-119/12 e del 21 giugno 2022, *Ligue des droits humains*, C-817/19): «tale eccezione non può essere applicata a misure che possono, tutt'al più, presentare un nesso soltanto indiretto con uno degli obiettivi contemplati da tale disposizione [...] misure adottate da uno Stato membro in forza delle quali, a pena di sanzioni, i fornitori di servizi di intermediazione online, stabiliti in un altro Stato membro, sono obbligati, al fine di prestare i loro servizi nel primo Stato membro, a iscriversi in un registro tenuto da un'autorità di tale Stato membro, a comunicare a quest'ultima una serie di informazioni dettagliate sulla loro organizzazione, nonché a versare alla stessa un contributo economico, non soddisfano le condizioni previste all'articolo 3, paragrafo 4, lettera a), della direttiva 2000/31/CE».

La CGUE ha risposto, dunque, alla prima, terza e quarta domanda, affermando che l'art. 3, direttiva 2000/31/CE «osta a misure adottate da uno Stato membro, allo scopo dichiarato di garantire l'adeguata ed efficace applicazione del regolamento 2019/1150, ai sensi delle quali, a pena di sanzioni, i fornitori di servizi di intermediazione online stabiliti in un altro Stato membro sono obbligati, al fine di prestare i loro servizi nel primo

ISSN 2239-8570

Stato membro, a iscriversi in un registro tenuto da un'autorità di tale Stato membro, a comunicare a quest'ultima una serie di informazioni dettagliate sulla loro organizzazione e a versare alla stessa un contributo economico». Sono rimaste, invece, assorbite la seconda e la quinta questione, riguardanti gli obblighi di previa notifica previsti dalle direttive 2000/31/CE e (UE) 2015/1535, la cui inosservanza comporta l'inopponibilità ai privati delle misure.

Sia consentita, in chiosa, soltanto una succinta considerazione: la perdurante vigenza del principio del controllo del Paese d'origine non manca (e non ha mancato) di suscitare riflessioni critiche. Desta perplessità, in particolare, la facilità per i prestatori di servizi di scegliere lo Stato che "offre" una legislazione più conveniente, per poi indirizzare le proprie attività (anche o esclusivamente) al pubblico di un altro Stato. L'applicazione di questo principio, ove non accompagnata da correttivi, rischia di favorire una "corsa al ribasso", inducendo i fornitori di servizi a stabilirsi nello Stato che, nel rispetto delle regole minime armonizzate, "offre" la legislazione più vantaggiosa, aggirando così le regole interne. Il timore è amplificato dalla circostanza che, secondo la CGUE, il pubblico *target* del fornitore di servizi non è tra i criteri da prendere in considerazione per individuare lo Stato di stabilimento, potendo un prestatore esser considerato stabilito in uno Stato membro in base alla sede del suo centro di attività anche se quest'ultime sono in concreto dirette soltanto al pubblico localizzato in altri Paesi membri.

Se i fornitori di servizi *online* sono liberi di scegliere il Paese di stabilimento e con ciò la giurisdizione per sé, il rischio (concreto) è che le autorità dei Paesi con le legislazioni più liberali finiscano per non avere capacità e incentivi sufficienti per vigilare sul rispetto della normativa nazionale da parte d'imprese che, per la stessa natura dei servizi che offrono, operano su tutto il mercato europeo, ben oltre i confini nazionali. Occorre evitare che, di fatto, si creino sacche di immunità e il principio cd. *one-stop-shop* degeneri nella sua versione peggiore ossia si declini nei termini di *zero-stop-shop*.

CLAUDIA CONFORTINI

https://curia.europa.eu/juris/liste.jsf?language=it&num=C-662/22

2024/3(2)TB

2. La sentenza CGUE (prima sezione) del 26.9.2024 nella causa C-768/21 sulla non obbligatorietà per le autorità di controllo di imporre una sanzione a fronte dell'accertamento di una violazione del GDPR

Con sentenza emessa in data 26 settembre 2024 nella causa C-768/21, la Corte di Giustizia dell'Unione Europea (**CGUE**) ha statuito su una domanda pregiudiziale presentata dal Tribunale Amministrativo di Wiesbaden

ISSN 2239-8570

(Germania), riguardante l'interpretazione del combinato disposto di alcune norme del regolamento (UE) 2016/679 (**GDPR**) in relazione ai poteri sanzionatori delle autorità nazionali incaricate di vigilare sulla corretta applicazione del medesimo regolamento ai sensi degli art. 57(1)(a) e (f), art. 58(2) e art. 77(1) GDPR.

Il rinvio pregiudiziale era stato effettuato nell'ambito di un contenzioso tra un privato (**T.R.**) ed il Land dell'Assia (Germania) relativo all'omessa adozione di misure correttive da parte dell'autorità per la protezione dei dati di tale Land (la **DPA**) nei confronti di una cassa di risparmio locale (la **Cassa**).

Il caso trae origine dal fatto che la Cassa, dopo aver verificato che una propria dipendente aveva ripetutamente effettuato degli accessi illeciti ai dati personali di T.R., notificava tale circostanza come violazione dei dati personali (*data breach*) alla DPA, senza procedere invece alla comunicazione all'interessato.

T.R., venuto a conoscenza del fatto, presentava un reclamo alla medesima DPA lamentando la mancata comunicazione nei propri confronti, asseritamente in violazione dell'art. 34 GDPR. L'art. 34(1) GDPR dispone che «Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo».

La DPA, sentita la Cassa per iscritto e oralmente, statuiva che essa non avesse violato tale disposizione. La motivazione della DPA si fondava sul fatto che la decisione della Cassa di non effettuare la comunicazione all'interessato era stata assunta sulla base di un'analisi effettuata dal DPO, il quale aveva ritenuto che non vi fosse un rischio elevato per i diritti e le libertà di T.R.

Sotto questo profilo, l'analisi rilevava che erano state adottate misure disciplinari nei confronti della dipendente e che quest'ultima aveva confermato per iscritto di non aver copiato, conservato o trasmesso i dati personali a terzi, e che non lo avrebbe fatto in futuro.

T.R. impugnava allora la decisione avanti il Tribunale Amministrativo di Wiesbaden, il quale sospendeva il procedimento al fine di richiedere alla CGUE di chiarire se, in caso di violazione accertata di disposizioni relative alla protezione dei dati personali, il GDPR debba essere interpretato nel senso che un'autorità di controllo è tenuta ad adottare misure correttive ai sensi dell'art. 58(2) GDPR, come una sanzione amministrativa pecuniaria, oppure nel senso che tale autorità dispone di un potere discrezionale in materia, in forza del quale è legittimata ad omettere, se del caso, siffatte misure.

La CGUE, evidenziando i criteri di necessità e proporzionalità che ai sensi del GDPR devono informare l'esercizio dei poteri delle autorità di controllo, nonché il tenore letterale delle disposizioni rilevanti in materia di poteri sanzionatori, ha statuito che il GDPR lascia all'autorità di controllo un margine di discrezionalità quanto al modo in cui essa deve porre rimedio all'inadeguatezza constatata, prendendo in considerazione tutte le circostanze del caso concreto.

ISSN 2239-8570

Pertanto, secondo la CGUE, non si può dedurre dall'art. 58(3) GDPR, né dall'articolo 83 GDPR, che vi sia un obbligo per l'autorità di controllo di adottare, in tutti i casi in cui riscontri una violazione dei dati personali, una misura correttiva, in particolare una sanzione amministrativa pecuniaria.

In questo senso, non è infatti da escludersi che l'autorità di controllo possa omettere di adottare una misura correttiva quando – ad esempio – il titolare del trattamento che avesse già attuato, prima del trattamento, misure tecniche e organizzative adeguate ai sensi dell'art. 24 GDPR, abbia poi adottato, non appena venuto a conoscenza di una violazione, misure appropriate e necessarie a farla cessare ed evitarne la ripetizione.

La Corte ha quindi statuito che l'autorità di controllo non è tenuta ad adottare una misura correttiva qualora un siffatto intervento non sia appropriato, necessario o proporzionato al fine di porre rimedio all'inadeguatezza constatata e garantire il pieno rispetto del GDPR, rimettendo infine al giudice del rinvio la valutazione dei fatti del procedimento principale alla luce dell'interpretazione fornita.

TIMOTEO BUCCI

https://curia.europa.eu/juris/document/document.jsf;jsessionid=6ED530B4876D57561BCCC016F84B89A9?text=&docid=290402&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1&cid=3494592

2024/3(3)SB

3. La sentenza CGUE (quarta sezione) del 4.10.2024 nella causa C-446/21 sulla nozione dei dati particolari resi manifestamente pubblici e sul periodo massimo di trattamento dei dati personali degli utenti di una piattaforma di social network a fini di pubblicità mirata

Nella recente sentenza resa il 4 ottobre 2024 nella causa C-446/21, la Corte di giustizia dell'Unione europea (**CGUE**) è tornata a pronunciarsi sulla nozione del trattamento dei dati particolari ex art. 9 regolamento (UE) 2016/679 (**GDPR**) resi manifestamente pubblici e sul periodo massimo di trattamento dei dati da parte di una piattaforma online quale un social network come Facebook.

L'occasione è stata data dalla nuova causa avviata dal Sig. Maximilian Schrems contro Meta Platforms Ireland Ltd (**Meta**), già Facebook Ireland Ltd.

Nella vicenda che qui si esamina, le contestazioni mosse dal Sig. Schrems riguardavano, tra le altre cose, il trattamento da parte di Meta dei dati dello Schrems anche relativi al suo orientamento sessuale omosessuale senza che tali dati, aggregati ad altri dati personali dello stesso Schrems e raccolti da Meta direttamente o tramite terze parti, fossero stati sottoposti a limiti temporali e al principio di minimizzazione di cui all'art. 5, par. 1, lett. c), GDPR e in assenza di consenso al loro trattamento.

ISSN 2239-8570

Il punto cruciale era che il Sig. Schrems, utente di Facebook, sul proprio profilo non aveva mai discusso del proprio orientamento sessuale né aveva mai autorizzato Facebook a trattare i dati relativi alla propria vita sentimentale e, però, grazie ai cookie, ai social plugin e pixel inseriti nelle pagine dei siti di terze parti con le quali Meta aveva accordi, quest'ultima aveva comunque avuto accesso ai dati concernenti l'orientamento sessuale dello Schrems e aveva iniziato ad inviargli pubblicità mirata riferita anche al suo orientamento omosessuale. Secondo Meta, la base per il trattamento dei dati particolari del Sig. Schrems afferenti al suo orientamento sessuale consisteva nell'accettazione da parte del medesimo Sig. Schrems delle condizioni di utilizzo del social network che indicavano espressamente l'implementazione da parte di Meta di programmi con terze parti tramite i social plugin e appositi pixel contenuti sulle pagine dei siti terzi.

In più, durante una tavola rotonda tenutasi a Vienna il 12 febbraio 2019, liberamente accessibile dietro acquisto del relativo biglietto, trasmessa contemporaneamente in streaming ed il cui video era stato anche caricato su Youtube, il Sig. Schrems aveva pubblicamente detto di essere omosessuale. Il trattamento del dato relativo all'orientamento sessuale dello Schrems avrebbe, quindi, trovato la propria base giuridica nell'art. 9, par. 2, lett. e), GDPR, in quanto dato reso manifestamente pubblico dall'interessato.

Sul trattamento dei dati particolari in relazione alle condizioni di utilizzo di un social network, la Corte di Giustizia si era già pronunciata a Grande Sezione con la sentenza del 4 luglio 2023, C-252/21 (sulla quale v. in questa Rubrica la notizia n.7 nel numero 3/2023: 2023/3(7)CAT). In tale occasione, tra le altre cose, la CGUE aveva dichiarato che visitare un sito o usare un'applicazione attinente ad una delle categorie menzionate nell'art. 9, GDPR (ad es. consultare un sito di un partito politico o un sito aderente ad una confessione religiosa) non rende di per sé manifestamente pubblico alcun dato (ad es. aderenza ad un partito o ad una confessione religiosa) e che il dato particolare di una persona non diviene manifestamente pubblico nemmeno quando l'utente di un sito sfrutti tool di like o di condivisione o che, comunque, consentano l'identificazione dell'utente medesimo salvo che quest'ultimo non abbia esplicitamente espresso preliminarmente la propria scelta di rendere i dati pubblicamente accessibili a un numero illimitato di persone.

Nel caso Schrems in esame, dove vi era stata una pubblica dichiarazione ad una tavola rotonda circa il proprio orientamento sessuale anche se rientrante in un più ampio dibattito circa il modo in cui Meta trattava i dati personali e soprattutto quelli particolari degli utenti della piattaforma Facebook, la Corte ha da un lato ritenuto che, se tale dichiarazione fosse da considerarsi manifestamente pubblica ai sensi dell'art. 9(2)(e) GDPR fosse questione di fatto spettante al Giudice a quo, dall'altro lato però – e qui risiede l'importanza della sentenza - la stessa Corte ha rilevato che, anche qualora si renda manifestamente pubblico un dato relativo al proprio orientamento sessuale, ciò "*non autorizza… il trattamento di altri dati personali relativi all'orientamento sessuale di quella persona … ottenuti, eventualmente, al di fuori di tale piattaforma a partire da applicazioni e siti Internet di partners terzi, al fine dell'aggregazione e dell'analisi di detti*

ISSN 2239-8570

dati, per proporre a tale persona della pubblicità personalizzata" (così, punti 80 e 83 della sentenza).

Il fatto, quindi, che il gestore di un social network possa trattare un dato particolare perché divenuto manifestamente pubblico, non significa che altri dati particolari, quand'anche rientranti nella stessa categoria ed area del dato diventato manifestamente pubblico, possano essere considerati anch'essi pubblici, ma per il loro trattamento si richiede comunque l'espresso consenso o che, in mancanza di consenso espresso, il trattamento di tali altri dati possa trovare la propria base giuridica in una delle eccezioni previste dall'art. 9(2) GDPR.

Quanto alla questione dell'aggregamento dei dati, ivi inclusi quelli di natura particolare, e il limite temporale del loro trattamento, la Corte, sulla scorta del principio di minimizzazione di cui all'art. 5(1)(c), GDPR, ha escluso che "*tutti i dati personali che un responsabile del trattamento, come il gestore di una piattaforma di social network online, ha ottenuto dall'interessato o da terzi e che sono stati raccolti sia su tale piattaforma che al di fuori di essa, siano aggregati, analizzati ed elaborati a fini di pubblicità mirata, senza limitazione temporale e senza distinzione basata sulla natura di tali dati*" (così, punto 65 e dispositivo della sentenza) .

Il trattamento, infatti, deve essere limitato al periodo di tempo strettamente necessario alle finalità per le quali i dati sono stati raccolti e trattati, rimanendo preciso dovere del titolare dare la prova, ai sensi dell'art. 5(2) GDPR, che i dati vengono conservati per il tempo limitato al conseguimento delle finalità per le quali sono stati acquisiti. E se è vero che il periodo di conservazione non può essere predeterminato in astratto, dovendosi ogni volta verificare la natura dei dati in questione e le finalità del trattamento, secondo la Corte "*una conservazione, per un periodo illimitato, dei dati personali degli utenti di una piattaforma di social network a fini di pubblicità mirata deve essere considerata un'ingerenza sproporzionata nei diritti garantiti a tali utenti dal [GDPR]*" (così, punto 58 della sentenza). E parimenti sproporzionato deve essere considerato il trattamento indifferenziato di tutti i dati (indipendentemente dalla loro natura e, quindi, dal loro grado di sensibilità) degli utenti Facebook (in tal senso, punto 64 della sentenza).

Per questi motivi, in conclusione la CGUE ha così dichiarato:

1) L'art. 5(1)(c) GDPR dev'essere interpretato nel senso che:

il principio della «minimizzazione dei dati», da esso previsto, osta a che tutti i dati personali che un responsabile del trattamento, come il gestore di una piattaforma di social network online, ha ottenuto dall'interessato o da terzi e che sono stati raccolti sia su tale piattaforma che al di fuori di essa, siano aggregati, analizzati ed elaborati a fini di pubblicità mirata, senza limitazione temporale e senza distinzione basata sulla natura di tali dati.

2) L'articolo 9(2)(e) GDPR dev'essere interpretato nel senso che:

la circostanza che una persona si sia espressa sul proprio orientamento sessuale in occasione di una tavola rotonda aperta al pubblico non autorizza il gestore di una piattaforma di social network online a trattare altri dati relativi all'orientamento sessuale di detta persona, ottenuti, eventualmente, al di fuori di tale piattaforma a partire da applicazioni e da siti Internet di

ISSN 2239-8570

partners terzi, al fine dell'aggregazione e dell'analisi di detti dati, per proporre a tale persona della pubblicità personalizzata.

STEFANO BARTOLI

https://curia.europa.eu/juris/document/document.jsf;jsessionid=D52D73E4017A10D23654467ADE0F9BC9?text=&docid=290674&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=5074199

2024/3(4)FPe

4. Le novità del Testo unico sui servizi di media audiovisivi (TUSMA) alla luce delle modifiche apportate dal D. Lgs. 50/2024 ('decreto correttivo')

La legge 22 aprile 2021, n. 53, ha conferito al Governo la delega per l'attuazione della direttiva (UE) 2018/1808 (direttiva su servizi media audiovisivi) e il riordino delle disposizioni concernenti la fornitura di servizi di media audiovisivi, di cui al decreto legislativo 31 luglio 2005, n. 177, recante il Testo unico dei servizi di media audiovisivi e radiofonici. In attuazione di tale delega, il Governo ha adottato il decreto legislativo n. 208/2021, recante il nuovo testo unico per la fornitura di servizi di media audiovisivi (c.d. TUSMA, di seguito anche **Testo unico**) e abrogando il precedente.

A più di un anno dalla sua adozione, il Governo ha ritenuto necessario avvalersi della facoltà concessa dalla legge 24 dicembre 2012, n. 234, recante «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea», che all'articolo 31, comma 5, richiamato anche dall'articolo 1 della legge n. 53/2021, autorizza, entro 24 mesi dalla data di entrata in vigore del decreto legislativo n. 208/2021, nel rispetto dei principî e criteri direttivi fissati dalla legge di delegazione europea, ad adottare disposizioni integrative e correttive del predetto decreto legislativo. L'intervento correttivo ha lo scopo di correggere e aggiornare quelle che sono le novità introdotte in materia regolamentare, nel rispetto dei principî di delega di cui all'articolo 3 della predetta legge di delegazione europea. Tale *iter* si è concluso con l'adozione del decreto legislativo 25 marzo 2024, n. 50 (di seguito, anche "**decreto correttivo**"), dopo la notifica dello schema di provvedimento alla Commissione europea e il parere del Consiglio di Stato, Sezione Consultiva per gli Atti Normativi, reso nell'Adunanza di Sezione del 27 febbraio 2024.

Le modifiche adottate si propongono l'obiettivo di conferire maggiore chiarezza e omogeneità all'impianto normativo e al contenuto del Testo unico, al fine di meglio perseguire l'obiettivo del corretto funzionamento del mercato unico europeo per i servizi di media audiovisivi che la stessa legge delega si era prefissata.

Si è, in primo luogo, chiarito l'ambito di applicazione di diverse disposizioni di principio, estendendone la portata a tutti i fornitori di servizi

ISSN 2239-8570

media, sia audiovisivi sia radiofonici, indipendentemente dalla tecnologia di trasmissione, in coerenza con l'obiettivo del Testo unico di fornire un quadro completo di disciplina. In tale ottica, si è proceduto, ove possibile, in coerenza con i principi della direttiva – relativa, come noto, ai soli servizi di media audiovisivi – ad estendere anche alle piattaforme di condivisione di contenuti solo audio alcune disposizioni di contrasto alla diffusione di contenuti illegali e di tutela degli utenti, dettate dalla normativa europea solo per le piattaforme di diffusione di video.

Il decreto correttivo si compone, dunque, di quattro articoli: l'articolo 1, composto da 41 commi, in cui sono inserite le modifiche apportate al decreto legislativo n. 208/2021, che si intende integrare e correggere; l'articolo 2 che contiene le modifiche meramente formali apportate al medesimo Testo unico; l'articolo 3, recante disposizioni abrogative e l'articolo 4, contenente la clausola di invarianza finanziaria. Nell'ambito dell'articolo 1, sono sostituiti integralmente gli articoli del Testo unico 41 e 2, relativi alle piattaforme per la condivisione di video, e dal 51 al 57, recanti le disposizioni relative alla promozione delle opere europee e di produttori indipendenti; tali articoli sono sostanzialmente confermati nella precedente formulazione, salvo marginali modifiche integrative, ma sono stati integralmente ricompresi nel testo del decreto correttivo al fine di notificare tempestivamente la disciplina nei due settori di riferimento nella sua integralità.

Si procede, di seguito, a una, sia pur non esaustiva, disamina delle principali novità introdotte nel Testo unico dall'articolo 1 del decreto correttivo.

Il comma 1 modifica l'articolo 1 del Testo unico e, in particolare, la lettera a), nella quale si inserisce il richiamo ai servizi di condivisione di contenuti audiovisivi o anche solo audio al fine di ampliare, a tutela degli utenti, l'ambito di applicazione dei principî generali, relativi alla prestazione di servizi di media digitali (sic) audiovisivi e radiofonici e ai servizi di piattaforma contenuti nel Testo unico dei servizi di media audiovisivi. Inoltre, il contenuto dell'articolo 1, comma 2, del d. lgs. 208/2021 è accorpato al testo della lettera b), articolo 1, comma 1, del decreto stesso, al fine di una migliore razionalizzazione del dettato normativo.

Il comma 2 apporta diverse modifiche all'articolo 2, recante disposizioni relative all'applicazione della giurisdizione italiana ai servizi di media audiovisivi e radiofonici. Di particolare interesse, la maggior precisione con cui descrive l'ambito di applicazione soggettivo della norma, chiarendo che i destinatari della stessa, soggetti alla giurisdizione italiana, sono, oltre al fornitore, tutte le emittenti radiofoniche, indipendentemente dalla tecnologia di trasmissione, eliminandosi pertanto il riferimento ai soli concessionari radiofonici.

Il comma 3 modifica alcune definizioni dell'articolo 3 del Testo unico, per ragioni di carattere formale e sostanziale: in particolare, di grande interesse la modifica apportata al comma 1, lett. c), con cui si amplia il concetto di servizio di piattaforma per la condivisione dai soli contenuti video, ai contenuti sia audio che video o anche di solo audio. Ne deriva, dunque, che anche i servizi di piattaforma per la condivisione di audio, quali

ISSN 2239-8570

ad esempio i *podcast*, rientrano nell'ambito di applicazione del Testo unico. Tale modifica si connette alla introduzione del nuovo comma 10-*bis* del successivo articolo 42, che estende, per quanto compatibili, le disposizioni di tutela degli utenti dai contenuti illeciti trasmessi dalle piattaforme audiovisive anche alle piattaforme di condivisione di contenuti di solo audio. Coerentemente, vengono modificate anche le definizioni di "sponsorizzazione", di cui si amplia l'ambito oggettivo di applicazione facendo riferimento alla condivisione di contenuti audiovisivi e anche di solo audio; di "*telepromozione*", per cui si specifica che ogni forma di pubblicità consistente nell'attività di esibizione di prodotti o presentazione verbale e visiva di beni e servizi è realizzabile anche dal fornitore di servizi radiofonici o dall'emittente radiofonica; e, infine, di "*autopromozione*", allineando correttamente la previsione, sia per servizi di media audiovisivi sia radiofonici, alla pronuncia della Corte di giustizia dell'Unione europea, sezione terza, 30 gennaio 2024, C-255/21 –RTI, la quale ha chiarito che "*l'articolo 23, paragrafo 2, della direttiva 2010/13/UE del Parlamento Europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), deve essere interpretato nel senso che: la nozione di «annunci dell'emittente relativi ai propri programmi» non include gli annunci promozionali effettuati da un'emittente televisiva per una stazione radio appartenente al medesimo gruppo societario di tale emittente, salvo che, da un lato, i programmi oggetto di tali annunci promozionali siano «servizi di media audiovisivi », ai sensi dell'articolo 1, paragrafo 1, lettera a), di tale direttiva, il che implica che siano scindibili dall'attività principale di tale stazione radio e, dall'altro, detta emittente televisiva ne assuma la «responsabilità editoriale», ai sensi dell'articolo 1, paragrafo 1, lettera c), di detta direttiva*".

Il comma 4 modifica l'articolo 4 del Testo unico, recante i "*principi generali del sistema dei servizi di media audiovisivi e della radiofonia a garanzia degli utenti e in materia di servizi di media in ambito locale*". Infatti, il comma 1 è riformulato con l'inserimento di una suddivisione della disposizione per punti, al fine di agevolare la lettura delle casistiche riportate all'interno della norma e viene introdotto, ferma restando la libertà di espressione di ogni individuo inclusa la libertà di opinione, il "*contrasto alla tendenza contemporanea di distruggere o comunque ridimensionare gli elementi o simboli della storia e della tradizione della Nazione (cancel culture)*" (art. 4, comma 1, lett. h)).

I commi 3 e 4, invece, sono riformulati per garantire maggiore chiarezza e precisione al testo normativo inserendo, peraltro, anche il Ministero dell'università e della ricerca, il Ministero dell'istruzione e del merito e l'Autorità politica delegata all'innovazione tecnologica, quali organi che, oltre al Ministero della cultura, il Ministero delle imprese e del made in Italy, d'intesa con l'Autorità per le garanzie nelle comunicazioni (di seguito anche **AGCOM** o l'**Autorità**), deve sentire, al fine di promuovere lo sviluppo dell'alfabetizzazione mediatica e digitale. Inoltre, a tale riguardo si ricorda quanto previsto dall'articolo 1, comma 360, Legge 29 dicembre

ISSN 2239-8570

2022, n. 197, recante "*Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025*", che prevede l'istituzione di un fondo nello stato di previsione del Ministero delle imprese e del made in Italy, per sostenere e promuovere progetti di alfabetizzazione mediatica e digitale e progetti educativi a tutela dei minori, realizzati dai fornitori di servizi di media e dai fornitori di piattaforme di condivisione.

Il comma 5 modifica l'articolo 5 del Testo unico, recante i "*principi generali del sistema dei servizi di media audiovisivi e della radiofonia a salvaguardia del pluralismo e della concorrenza*", sopprimendo il principio di previsione di titoli distinti per lo svolgimento dell'attività di fornitura esercitate su frequenze terrestri nella parte in cui stabilisce che uno stesso soggetto o soggetti tra loro in rapporto di controllo o di collegamento non possono essere contemporaneamente titolari di autorizzazioni per fornitore di servizi media radiofonici digitali in ambito nazionale e in ambito locale. Già il Testo unico nel 2021 sopprimeva il divieto di titolarità congiunta dell'autorizzazione alla fornitura di media audiovisivi lineari su scala nazionale e su scala locale, su frequenze terrestri. Tale divieto potrebbe permanere in vita per la sola radiofonia digitale, ma per assicurare un corretto coordinamento di disciplina, considerando anche le modalità operative di tutta la radiofonia, nazionale o locale, che fa ricorso a tecnologie di trasmissione come il *web streaming*, prescindendo da qualsiasi distinzione di ordine territoriale, si è preferito evitare trattamenti discriminatori e adottare una disciplina uniforme. Viceversa, resta ferma la previsione di distinti titoli abilitativi per i servizi radiofonici digitali terrestri su scala nazionale e su scala locale. L'articolo 5, inoltre, amplia e specifica il novero dei soggetti nei cui confronti la normativa si riferisce. Nel dettaglio, in luogo delle emittenti o dei soli fornitori di servizi di media audiovisivi si fa riferimento sia alle emittenti radiofoniche, sia ai fornitori di servizi di media radiofonici che ai fornitori di servizi di media audiovisivi.

L'articolo 8 è modificato, e per l'effetto il Comitato di applicazione del codice di autoregolamentazione media e minori viene sostituito da un comitato interistituzionale con compiti di promozione e ricerca sui temi dell'alfabetizzazione mediatica e digitale, di esprimere pareri su codici di auto- e co-regolamentazione dei fornitori di servizi di media a tutela dei minori. Le conseguenti modifiche sono altresì trasposte nell'articolo 38, relativo alla tutela dei minori.

Oltre alle già menzionate novità delle previsioni relative alle piattaforme di audio e video o solo audio, di cui agli articoli 41 e 42, l'altra modifica di rilievo del decreto correttivo è quella apportata agli articoli da 51 a 58, come sopra già accennato, relativi al recepimento delle disposizioni della direttiva sui servizi di media audiovisivi relativi agli obblighi di programmazione e investimento in opere europee e di produttori indipendenti.

Il quadro normativo riportato nella precedente formulazione del Testo unico, stratificatosi nel tempo, prevedeva un complesso sistema di quote e sottoquote, recanti obblighi di programmazione e investimento, diversificati a seconda della natura del fornitore di servizi di media audiovisivi, se lineari o non lineari, che rendevano l'Italia uno dei sistemi più prescrittivi d'Europa

ISSN 2239-8570

in tale ambito. Conseguentemente, nel giugno del 2023, il Consiglio dell'AGCOM ha rilevato la necessità di segnalare al Governo l'opportunità di una revisione dell'impianto generale del sistema degli obblighi in materia di programmazione e investimento formulando "[…] *alcune osservazioni e proposte in ragione dell'esigenza di una revisione di alcuni aspetti della vigente disciplina di tutela e promozione della produzione audiovisiva europea e indipendente, di cui al d. lgs. 8 novembre 2021, n. 208, e del regime di credito di imposta per le imprese di produzione cinematografica e audiovisiva, di cui all'art. 15, della legge 14 novembre 2016, n. 220, con specifico riferimento alla produzione indipendente*". In particolare, per il tema che qui rileva, l'Autorità ha ritenuto di portare all'attenzione del legislatore la necessità di un generale ripensamento dell'impianto del sistema delle cd. Quote europee, teso a una maggiore semplificazione, flessibilità e trasparenza e al superamento del sistema di sottoquote, ritenuto eccessivamente prescrittivo, proponendo, quindi, le conseguenti modifiche al Testo unico. Tali suggerimenti sono stati parzialmente accolti nel decreto correttivo, in particolare con riferimento agli obblighi di investimento dei fornitori di servizi di media a richiesta, abbassata dal 20% inizialmente previsto dalla precedente formulazione del Testo unico al 16%. Tuttavia, la modifica apportata al comma 8 del medesimo articolo ha elevato la sottoquota in favore di opere di espressione originale italiana recenti portandola dal 50% al 70% della quota di investimento sopra menzionata, e stabilendo direttamente, e non delegandolo al regolamento ministeriale come precedentemente previsto, la ulteriore percentuale del 27% di investimento in opere cinematografiche di espressione originale italiana ovunque prodotte negli ultimi cinque anni da produttori indipendenti.

Tali obblighi di investimento si applicano anche ai fornitori di servizi di media *on-demand* stabiliti in altro Stato membro ma che siano responsabili di servizi destinati al pubblico italiano. Il legislatore italiano, infatti, si è avvalso della facoltà appositamente riconosciuta dall'articolo 13, paragrafo 2, della direttiva 2010/13/UE, come modificato dalla predetta direttiva (UE) 2018/1808 (direttiva su servizi media audiovisivi).

Infine, il decreto correttivo è intervenuto anche sull'articolo 57, relativo alle competenze riservate al regolamento dei Ministri delle imprese e del made in Italy e della cultura, non ancora adottato nel momento in cui si redige il presente contributo, a cui è demandato di stabilire, sulla base di principi di proporzionalità, adeguatezza, trasparenza ed efficacia, la definizione delle opere audiovisive, ovunque prodotte, di espressione originale italiana. Appare degno di nota come il decreto correttivo abbia provveduto a una semplificazione e snellimento anche delle previsioni del regolamento ministeriale, eliminando, inter alia, l'apertura a un'eventuale previsione di ulteriori sotto quote a favore di particolari tipologie di opere audiovisive prodotte da produttori indipendenti, ovvero le previsioni relative ai criteri per la limitazione temporale dei diritti di utilizzazione e sfruttamento delle opere e per le modalità di valorizzazione delle stesse sulle diverse piattaforme, in un'ottica di semplificazione del sistema e di un approccio maggiormente organico, a certezza del mercato e degli operatori.

ISSN 2239-8570

FRANCESCA PELLICANÒ
Funzionaria dell'Ufficio servizio pubblico televisivo radiofonico e multimediale dell'Agcom
Le opinioni riportate sono personali e non impegnano in alcun modo la posizione dell'Autorità per le garanzie nelle comunicazioni. Ogni errore od omissione è imputabile unicamente all'autrice

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024;50

2024/3(5)ES

5. Pubblicato il D.Lgs. 138/2024 del 4.9.2024 di recepimento della direttiva 2022/2555/UE ("NIS2") relativa a misure per un livello comune elevato di cibersicurezza nell'Unione europea.

Il 1 ottobre 2024 è stato pubblicato sulla Gazzetta Ufficiale il D. Lgs. 138 del 4 settembre 2024 (da ora anche il **Decreto**) di recepimento della direttiva 2022/2555/UE (da ora anche **Direttiva NIS 2**, acronimo inglese che sta per "Network and Information Security", o la **Direttiva**) relativa a misure per un livello comune elevato di cibersicurezza nell'Unione europea.

Il Decreto, infatti, mira a stabilire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo altresì a migliorare il livello comune di sicurezza nell'Unione europea e il funzionamento del mercato interno. In particolare, tra gli obiettivi del Decreto figurano: i) la definizione di una strategia nazionale per la cybersicurezza; ii) l'integrazione del quadro di gestione delle crisi informatiche con l'organizzazione nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza; iii) l'attribuzione di specifiche competenze all'Agenzia per la cybersicurezza nazionale; iv) l'individuazione dei destinatari della normativa in commento (art. 1).

Dopo aver fornito una serie di definizioni all'art. 2, l'art. 3 stabilisce che il Decreto si applica ai soggetti pubblici e privati che operano nei settori descritti negli allegati I (c.d. "settori altamente critici"), II (c.d. "settori critici"), III, IV al Decreto, nonché ai soggetti meglio individuati dai commi 2 e seguenti del medesimo articolo. Il comma 10, infine, prevede un criterio residuale per cui la disciplina in commento si applica, "*indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri: a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale; b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale; c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale; d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale*".

ISSN 2239-8570

Sono espressamente esclusi dall'ambito di applicazione del Decreto "*il Parlamento italiano, l'Autorità giudiziaria, la Banca d'Italia e l'Unita' di informazione finanziaria per l'Italia ... enti, organi e articolazioni della pubblica amministrazione che operano nei settori della pubblica sicurezza, della difesa nazionale, o dell'attività di contrasto ... di reati, nonché agli organismi di informazione per la sicurezza di cui alla legge 3 agosto 2007, n. 124, all'Agenzia per la cybersicurezza nazionale*" (art. 4).

Tra i destinatari del Decreto occorre distinguere i c.d. "soggetti essenziali" di cui all'allegato I, ossia quelli che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE; b) indipendentemente dalle loro dimensioni, i soggetti identificati come soggetti critici ai sensi del decreto legislativo che recepisce la direttiva (UE) 2022/2557; c) i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2 dell'allegato alla raccomandazione 2003/361/CE; d) indipendentemente dalle loro dimensioni, i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio; e) indipendentemente dalle loro dimensioni, le pubbliche amministrazioni centrali di cui all'allegato III, comma 1, lettera a) (art. 6, comma 1). Ai sensi dell'art. 6, comma 2, invece, sono considerati "soggetti importanti" tutti quelli a cui si applica il Decreto e che non sono classificati come essenziali. Entrambe tali categorie di soggetti sono tenute ad iscriversi in una piattaforma digitale "*resa disponibile dall'Autorità nazionale competente NIS*" e l'iscrizione è necessaria al fine di consentire a quest'ultima di svolgere le funzioni previste dal Decreto (art. 7).

L'art. 9, comma 1 è dedicato alla strategia nazionale di cybersicurezza che "*individua gli obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza*". In particolare, la strategia definisce gli obiettivi e le priorità inerenti ai settori di cui agli allegati I, II, III e IV; un quadro di governance per la realizzazione dei suddetti obiettivi e priorità e che chiarisca i ruoli e le responsabilità dei portatori di interessi coinvolti nell'attuazione della strategia. L'art. 9, comma 3, inoltre, specifica ulteriormente il contenuto della strategia nazionale. Quest'ultima deve essere aggiornata ogni volta che sia necessario e, comunque, almeno ogni 5 anni.

Il Decreto stabilisce che l'Agenzia per la cybersicurezza nazionale è individuata come l'Autorità nazionale competente NIS (da ora anche "**Autorità**") a cui sono assegnati i seguenti compiti:

1. sovrintendere all'implementazione e all'attuazione del Decreto, nonché predisporre i provvedimenti necessari a darvi attuazione;
2. svolgere le funzioni e le attività di regolamentazione di cui al Decreto, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti;
3. individuare i soggetti essenziali e i soggetti importanti;

ISSN 2239-8570

4. partecipare al gruppo di cooperazione NIS, nonché alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva NIS 2;

5. svolgere le attività ed esercitare i poteri in materia di monitoraggio e vigilanza.

L'Autorità è anche il "*punto unico di contatto NIS*" poiché svolge una funzione di collegamento tra le autorità nazionali, nonché con la Commissione europea e l'ENISA ("Agenzia dell'Unione europea per la cybersicurezza") (artt. 10 e 14). L'art. 11 individua delle "*Autorità di settore NIS*" che supportano l'Autorità nazionale competente NIS nell'attuazione del Decreto. Nondimeno, al fine di assicurare la corretta attuazione del Decreto è costituito il "*Tavolo per l'attuazione della disciplina NIS*" che sostanzialmente supporta l'Autorità nello svolgimento dei suoi compiti (art. 12, comma 5).

L'art. 13, comma 1 designa l'Agenzia per la cybersicurezza nazionale e il Ministero della difesa come autorità nazionali di gestione delle crisi informatiche e stabilisce, al comma 3, che entro 12 mesi dall'entrata in vigore del Decreto debba essere definito il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala. Il piano è aggiornato periodicamente e, comunque, ogni tre anni.

Sempre al fine di assicurare adeguati livelli di cybersicurezza, è istituito un gruppo nazionale di risposta agli incidenti di sicurezza informatica (c.d. "CSIRT Italia", dove CSIRT è un acronimo inglese che sta per "Computer Security Incident Response Team") "*preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i settori, i sottosettori e le tipologie di soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso*". I compiti del CSIRT sono meglio specificati agli artt. 15, comma 3 e 16 del Decreto.

Al fine di garantire un'adeguata cooperazione a livello europeo e internazionale tra le autorità di settore, il Decreto prevede che l'Autorità partecipi al gruppo di cooperazione NIS, l'Autorità' nazionale di gestione delle crisi informatiche a sua volta prenda parte alla "*Rete delle organizzazioni di collegamento per le crisi informatiche*" (c.d. "EU-CyCLONe") e il CSIRT Italia partecipi alla rete dei CSIRT (artt. 18 – 20). Nondimeno, l'Autorità trasmette all'Unione europea la strategia nazionale di cybersicurezza entro 3 mesi dalla sua adozione o dal suo aggiornamento e coopera con le autorità degli altri paesi membri dell'Unione europea (art. 39). Nell'ottica di favorire la condivisione di informazioni, è altresì previsto che i destinatari del Decreto possano concludere accordi di condivisione delle informazioni sulla sicurezza informatica (art. 17).

Il Decreto prevede degli specifici obblighi in materia di gestione del rischio per la sicurezza informatica. Tali obblighi devono essere proporzionati al grado di esposizione al rischio, alle dimensioni dei soggetti e alla probabilità di verificazione degli incidenti (art. 31) e l'Autorità può imporre obblighi ulteriori rispetto a quelli previsti dal Decreto (art. 32).

Nello specifico è previsto che gli organi di amministrazione dei soggetti "essenziali" e "importanti"

ISSN 2239-8570

approvino le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica che tali soggetti intendano adottare, sovrintendano all'implementazione degli obblighi di cui al Decreto e siano responsabili delle relative violazioni. I suddetti organi sono tenuti a seguire una formazione in materia di sicurezza informatica, così come devono assicurare ai loro dipendenti una formazione adeguata in materia (art. 23).

I soggetti "essenziali" e "importanti" devono adottare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nello svolgimento della loro attività o nella fornitura di servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari delle loro attività e servizi. Tali misure sono basate su un approccio multi – rischio e "*assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti … e … sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico*" (art. 24, comma 1). L'Autorità, inoltre, può imporre ai soggetti "essenziali" e "importanti" l'utilizzo di determinate categorie di prodotti o sevizi ICT al fine del contenimento del rischio cibernetico.

Laddove si verifichi un incidente che abbia un impatto significativo sullo svolgimento delle proprie attività o sulla fornitura dei loro servizi, i soggetti "essenziali" e "importanti" devono notificarlo senza indugio al CSIRT Italia. Ai sensi dell'art. 25, comma 4 un incidente si definisce significativo se "*a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali immateriali considerevoli*". In particolare, i menzionati soggetti sono tenuti a fornire:

"*a) senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;*

b) senza ingiustificato ritardo, e comunque entro 72 ore [nds, 24 ore per i prestatori di servizi essenziali] *da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto;*

c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b)" (art. 25).

Al fine di una gestione efficace dei rischi informatici, l'art. 26 consente anche notifiche volontarie, ossia nei casi in cui il Decreto non le imporrebbe.

Ancora, per contribuire alla sicurezza, alla stabilità e alla resilienza dei sistemi di nomi di dominio, i gestori di registri dei nomi di dominio e i

ISSN 2239-8570

fornitori di servizi di registrazione dei nomi di dominio devono istituire un'apposita banca dati in cui conservano i dati di registrazione (art. 29).

All'Autorità spetta il compito di monitorare l'osservanza dei suddetti obblighi se del caso richiedendo una rendicontazione, anche periodica, l'esecuzione di audit sulla sicurezza ed emanando raccomandazioni e avvertimenti relativi a presunte violazioni degli doveri di cui al Decreto (artt. 34 e 35). L'Autorità può sottoporre i destinatari del Decreto a verifiche, ispezioni, inviargli richieste di accesso ai dati, documenti e altre informazioni, intimare il rispetto di istruzioni vincolanti o altri obblighi meglio descritti dall'art. 36.

Laddove i destinatari del Decreto non rispettino le indicazione dell'Autorità, quest'ultima "*può sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale … di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale*", irrogare agli esponenti aziendali la sanzione della incapacità a svolgere funzioni dirigenziali nonché comminare delle sanzioni amministrative nei casi previsti dall'art. 38, comma 10.

Il Decreto, infine, prevede delle disposizioni transitorie e finali, entra in vigore il 16 ottobre 2024 e stabilisce che le sue previsioni si applicheranno progressivamente nel tempo.

EMANUELE STABILE

https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG

2024/3(6)FS

6. Le disposizioni del 'Decreto salva infrazioni' (D.L. 131/2024) a completamento della liberalizzazione della gestione collettiva dei diritti d'autore

Il decreto legge 16 settembre 2024, n. 131, c.d. '**Decreto salva infrazioni**', pubblicato nella GU n. 217 del 16 settembre 2024, interviene sulla disciplina della gestione collettiva dei diritti d'autore e completa il processo di liberalizzazione del settore imposto dalla direttiva (UE) 2014/26 (**direttiva Barnier**).

L'attuazione della direttiva Barnier in Italia è stata alquanto complicata, giacché il relativo decreto di recepimento (D.lgs. 35/2017) aveva attuato solo in parte le indicazioni del legislatore comunitario, mantenendo in vigore il monopolio SIAE nella intermediazione dei diritti d'autore previsto dal testo allora vigente dell'art. 180 della l. 633/1941 sul diritto d'autore (**L.A.**) (a differenza del regime di libera concorrenza che già dal 2012 caratterizza la gestione collettiva dei diritti connessi dei produttori discografici e degli artisti interpreti esecutori). La riserva a SIAE era poi venuta meno per effetto dell'art. 19, comma 1, del D.L. 148/2017 che aveva

ISSN 2239-8570

affiancato a SIAE gli altri organismi di gestione collettiva (**OGC**) di cui al D.Lgs. 35/2017, negando però accesso al mercato alle entità di gestione indipendenti (**EGI**), ossia l'altra categoria di *collecting societies* cui la direttiva riserva l'esercizio dell'attività di intermediazione.

In questo scenario normativo, le EGI - ossia gli organismi che (i) non sono detenuti né controllati, direttamente o indirettamente, integralmente o in parte, dai titolari dei diritti intermediati, e (ii) perseguono fini di lucro - potevano stipulare licenze e riscuotere le *royalties* sul territorio nazionale solo sulla base di un accordo di rappresentanza con SIAE o con un OGC stabilito in Italia.

A seguito delle numerose perplessità sollevate da dottrina, giurisprudenza e Autorità per le garanzie nelle comunicazioni (**AGCOM**) circa la scelta normativa di escludere le EGI dal mercato nazionale dell'intermediazione dei diritti d'autore, limitando così ai soli OGC la possibilità di competere con SIAE, la questione è approdata dinanzi alla Corte di giustizia dell'Unione europea (**CGUE**), che con sentenza del 21 marzo 2024 nella causa C-10/22 *Lea/Jamendo* (su cui v. in questa Rubrica notizia n. 5 del numero 1/2024: 2024/1(5)FG) ha stabilito che l'art. 180 L.A. è contrario all'art. 56 del Trattato sul funzionamento dell'Unione europea (**TFUE**), in combinato disposto con la direttiva Barnier, nella misura in cui esclude in modo generale e assoluto la possibilità per le EGI stabilite in altro Stato membro di prestare in Italia i propri servizi di gestione dei diritti d'autore.

Proprio la sentenza della CGUE ha suscitato l'intervento della Commissione e ha dato la stura alla procedura di infrazione (n. 4092/2017), cui intende porre rimedio l'art. 15 del D.L. 131/2024, dedicato specificamente (tra le altre) a questa procedura di infrazione. La norma interviene sia sulla formulazione dell'art. 180 L.A., aggiungendo al riferimento a SIAE e agli OGC anche quello alle EGI, sia sull'art. 19, comma 2, del D.L. 148/2017, che viene novellato ammettendo all'attività di intermediazione sul territorio nazionale anche le EGI stabilite nel territorio dell'Unione Europea, sia infine sul D. Lgs. 35/2017, il cui impianto viene adeguato nel senso di parificare – nei limiti consentiti dalla direttiva – le EGI agli OGC operanti in Italia.

Si intende così recuperare un quadro armonico tra la liberalizzazione dell'attività di gestione collettiva dei diritti d'autore e quella dei diritti connessi già operata con il D.L. 1/2012, favorendo inoltre l'affermarsi di nuovi mercati, l'innovazione tecnologica e l'offerta di servizi innovativi distinti in favore dei consumatori, che possono così beneficiare di una maggiore varietà di opere e di modalità di fruizione delle stesse. Quanto agli operatori del settore, ossia le *collecting societies*, la piena attuazione della direttiva Barnier assicura una più ampia libertà circa la scelta della forma organizzativa ritenuta più idonea allo svolgimento dell'attività di gestione collettiva.

FRANCESCO SANTONASTASO

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2024;131

ISSN 2239-8570

7. I primi tre decreti del Ministro della Salute previsti dalla legge sull'oblio oncologico e il vademecum del Garante privacy

Come riportato in questa Rubrica nella notizia n. 21 del numero 2/2024 (v. 2024/2(21)RG), il 2 gennaio 2024 è entrata in vigore la legge 7 dicembre 2023, n. 193 (**legge sull'oblio oncologico** o **l. 193/2023**) finalizzata alla prevenzione delle discriminazioni e alla tutela dei diritti delle persone che sono state affette e sono guarite da malattie oncologiche. L'intento è perseguito dal legislatore attraverso la codificazione di un c.d. diritto all'oblio oncologico inteso, secondo l'art.1, co.2 l. 193/2023, come «*diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire indagini in merito alla propria pregressa condizione patologica, nei casi di cui alla presente legge*».

Il reticolato normativo distribuito in cinque articoli copre una molteplicità di ambiti poiché, ferma la portata generale dell'art.1, si occupa all'art. 2 della contrattazione generalmente intesa, con disposizioni particolari dedicate all'accesso ai servizi bancari, finanziari, di investimento e assicurativi, all'art. 3 al campo delle adozioni e all'art. 4 alle procedure concorsuali e selettive, al lavoro e alla formazione professionale. L'ultimo articolo è dedicato alle disposizioni transitorie e finali. In esso si prevedono una serie di ulteriori interventi normativi necessari a disciplinare aspetti formali o specifici dei diversi campi di applicazione invero richiamati anche nelle norme precedenti.

Il risultato è stato la produzione di una serie di decreti ministeriali che si sono susseguiti all'entrata in vigore della legge sull'oblio oncologico, e che arricchiscono il quadro generale della normativa.

Il primo intervento si è avuto con il D.M. 22 marzo 2024 del Ministro della Salute pubblicato in G.U. n. 96 del 24/4/2024 (**D. Min. Salute 22.3.2024**).

Si tratta di un decreto emanato in base alla previsione di cui all'art. 5, comma 2 l. 1993/2023, che reca un elenco di patologie oncologiche per le quali si applicano termini inferiori rispetto a quelli previsti dagli artt. 2, co. 1, 3, co. 1, lett. a), e 4, co. 1, della l.193/ 2023, della medesima legge, ossia, in tutti i casi di cui alle predette disposizioni: il decorso di dieci anni dalla conclusione del trattamento attivo della patologia in assenza di episodi di recidiva, o di cinque anni nel caso in cui la patologia sia insorta prima del compimento del ventunesimo anno di età.

Il D. Min. Salute 22.3.2024 prevede un elenco di patologie per cui l'oblio oncologico matura in un minore lasso di tempo. La ragione è da rinvenirsi in valutazioni di natura scientifica che ammettono si possa considerare il soggetto clinicamente guarito in presenza di un periodo temporale ridotto.

Nell'allegato 1 del D. Min. Salute 22.3.2024 sono indicate dieci patologie diverse, dettagliate per stadio della malattia ed età del malato con periodi di tempo, ai fini dell'oblio, che vanno da un minimo di un anno (es.

ISSN 2239-8570

nel caso di tumori alla tiroide) ad un massimo di sette anni (tumori colon-retto).

Riepilogando dunque, perché siano applicabili gli obblighi e i divieti della l. 193/2023 è necessario che decorra un periodo pre-individuato dalla normativa e utile a far maturare il diritto all'oblio oncologico: detto lasso temporale a seconda della patologia oncologica sarà pari a dieci o cinque anni, come previsto nella l. 193/2023, ovvero sarà di una durata ancora inferiore in base alla tabella dell'allegato 1 del D. Min. Salute 22.3.2024.

Una volta maturato l'oblio oncologico, si rende necessaria la sua certificazione cosicché i destinatari della legge siano in grado di essere edotti dello stato di irrilevanza della storia oncologica e dunque provvedano a non considerarla nei diversi ambiti contemplati (es. in sede negoziale, durante un procedimento di adozione o in ambito lavorativo).

L'esigenza di una formalizzazione dei presupposti del diritto viene soddisfatta con un altro Decreto del Ministero della Salute, del 5 luglio 2024 (il **D. Min. Salute 5.7.2024**) il quale, come previsto dall'art. 5, co.1 l. 193/2023, disciplina le modalità e le forme, senza oneri per l'assistito, per la certificazione della sussistenza dei requisiti necessari ai fini dell'applicazione delle disposizioni della stessa.

Il D. Min. Salute 5.7.2024 è stato preceduto da una consultazione con le organizzazioni dei pazienti oncologici aderenti ad un avviso pubblico per la manifestazione di interesse pubblicato dallo stesso Ministero e sentito il Garante per la protezione dei dati personali (**Garante Privacy**).

Il fulcro del D. Min. Salute 5.7.2024 è contenuto negli artt. 1 e 2. Il primo descrive l'iter di presentazione e rilascio dell'istanza di certificazione per l'oblio oncologico stabilendo che l'ex paziente oncologico deve presentare un'istanza adoperando il modello predisposto dal Ministero della Salute (Allegato I del D. Min. Salute 5.7.2024) corredata di eventuale documentazione medica, con cui chiede sia attestato l'oblio oncologico attraverso l'apposito certificato previsto dalla l. 193/2023 (il **Certificato di Oblio oncologico**). Il secondo comma individua i soggetti deputati a rilasciare il Certificato di Oblio oncologico, ossia strutture sanitarie pubbliche o private accreditate, un medico dipendente del Servizio Sanitario Nazionale o un medico di medicina generale ovvero un pediatra.

Tutti questi soggetti, non solo dovranno ricevere l'istanza, ma dovranno adempiere ad un ulteriore onere: fornire le informazioni di cui all'art. 13 (rubricato *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*) e all'art. 14 (rubricato *Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*) del Regolamento 2016/679 (**GDPR**) relative ai dati personali trattati per il rilascio del Certificato di Oblio oncologico e i diritti riconosciuti al richiedente tale certificato in qualità di interessato al trattamento. L'allegato I al D. Min. Salute 5.7.2024 contiene, oltre al modello di istanza anche l'informativa da rendersi a questi fini *ex* artt. 13 e 14 GDPR.

Nel rilasciare il Certificato di Oblio oncologico, i sanitari o le strutture dovranno altresì utilizzare il modello predisposto dal Ministero (allegato II al D. Min. Salute 5.7.2024) nonché rispettare una tempistica stringente di 30 giorni dalla presentazione dell'istanza.

ISSN 2239-8570

Vi è un altro obbligo per i soggetti onerati dalla certificazione che ancora una volta richiama il GDPR e che per tale motivo richiederà particolare attenzione: il periodo di conservazione delle istanze di oblio oncologico che sanitari e strutture dovranno appunto custodire per dieci anni, termine scaduto il quale deve avvenire la loro cancellazione. Va sottolineato come la norma ribadisca detto obbligo in entrambi i commi individuando chiaramente come l'obbligo di cancellazione incomba sugli stessi soggetti che hanno ricevuto l'istanza e come esso trovi la sua fonte nella disciplina sulla tutela dei dati personali.

Ed infatti, il precitato modello di informativa sul trattamento dei dati personali allegato al D. Min. Salute 5.7.2024 contiene tra le altre anche l'informazione su questo periodo di conservazione.

Il terzo decreto attuativo della legge sull'oblio oncologico è quello adottato il 9 agosto 2024 dal Ministro della Salute di concerto con il Ministro della Giustizia (**D. Min. Salute 9.8.2024**), recante le Disposizioni in materia di oblio oncologico in relazione alle adozioni, pubblicato nella Gazzetta Ufficiale del 13 settembre 2024. Esso è stato adottato, ai sensi dell'art. 3 co. 2 l. 193/2023, per dare attuazione alle disposizioni di cui agli articoli. 22, comma 4, 29-bis, comma 4, lettera c), e 57, comma 3, lettera a), della legge n. 184 del 1983, così come modificati dalla l. 193/2023.

Anche in questo caso, il decreto è stato preceduto da interlocuzioni con il Garante Privacy e con la Commissione per le adozioni internazionali.

La struttura del D. Min. Salute 9.8.2024 riprende quella del D. Min. Salute 5.7.2024 e concentra il cuore delle previsioni negli artt. 1 e 2. In forza del primo articolo si prevede che i soggetti che presentano domanda di adozione, se hanno maturato i requisiti per l'oblio oncologico, forniscono all'azienda sanitaria incaricata dal Tribunale delle indagini di rito, il Certificato di oblio oncologico previsto dal D. Min. Salute 5.7.2024 poc'anzi analizzato, con la precisazione che se l'oblio matura dopo la fase delle indagini, il certificato è depositato direttamente presso il Tribunale.

Va ricordato come lo schema originario di questo decreto prevedeva che la produzione del Certificato di Oblio oncologico da parte dei soggetti titolari del diritto di oblio oncologico dovesse avvenire, unitamente al deposito del certificato di sana e robusta costituzione rilasciato dalla Azienda sanitaria competente.

Sul punto si era espresso il Garante Privacy il quale, con nota in data 12 giugno 2024 prot. U.0071584 aveva osservato come una tale previsione apparisse incoerente con le finalità della legge e in contrasto con il principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c) del GDPR, comportando l'ostensione dell'informazione relativa alla pregressa malattia oncologica, ancorché già soggetta ad oblio, in assenza di un apparente giustificato motivo.

A seguito dei su esposti rilievi, il Ministero, con comunicazione del 18 giugno 2024, ha presentato una versione aggiornata del decreto che recepisce le osservazioni formulate dall'Ufficio del Garante e che è stata poi definitivamente approvata con parere favorevole del Garante Privacy (provvedimento n. 368 del 20.6.2024).

ISSN 2239-8570

L'art. 2 del D. Min. Salute 9.8.2024 richiama gli obblighi di cui all'art. 2 del DM 5 luglio 2024 del Ministro della Sanità per cui il Tribunale dovrà conservare per 10 anni il certificato di oblio oncologico e procedere poi a sua cancellazione.

I tre Decreti qui illustrati non esauriscono gli interventi attuativi previsti dalla Legge 193. Non è stato infatti ancora pubblicato il decreto del Ministro del Lavoro e delle politiche sociali previsto all'art. 4 della Legge 193 per promuovere specifiche politiche in grado di assicurare uguaglianza di opportunità nell'inserimento e permanenza nel mondo del lavoro a soggetti dal passato oncologico e mancano il decreto del Consiglio interministeriale per il credito e il risparmio ed il provvedimento di IVASS previsti dal comma 7 dell'art. 2 per darvi piena attuazione.

Infine, il Garante Privacy (che, ai sensi dell'art. 5, co. 4 della l. 193/2023 "vigila sull'applicazione delle disposizioni" di cui alla medesima legge), ha pubblicato sul suo sito una "Scheda informativa", nella quale, tra altre informazioni di carattere generale, viene anche offerto un chiarimento sul significato della espressione "*conclusione del trattamento attivo*". Come ricordato, tale espressione è utilizzata nella l. 193/2023 nelle tre disposizioni sopra richiamate, come *dies a quo* ai fini del computo del decorso del termine rilevante. Nell'Allegato I al D. Min. Salute 22.3.2024 si fa letteralmente riferimento come dies a quo a un termine ridotto che decorre "*dalla fine del trattamento o dall'ultimo intervento chirurgico*". Nella predetta Scheda informativa, si legge che «*Per "conclusione del trattamento attivo" della patologia si intende, in mancanza di recidive, la data dell'ultimo trattamento farmacologico antitumorale, radioterapico o chirurgico*» (p. 6 della Scheda informativa). Tale precisazione è il risultato di una interlocuzione tra il Garante Privacy ed il Ministero della Salute, che si è avuta in occasione della gestazione del secondo decreto del Ministro della Salute, il D. Min. Salute 5.7.2024. In particolare, dal parere favorevole emesso dal Garante su questo decreto (con provvedimento n. 367 del 20 giugno 2024) si ricava che il Ministero della Salute - su richiesta del medesimo Garante Privacy – aveva comunicato che avrebbe modificato il testo dell'art. 1, co. 2 dell'emanando decreto al fine di includere una spiegazione della espressione "conclusione del trattamento attivo" dello stesso tenore di quella sopra riportata, che si trova nella Scheda informativa del Garante Privacy (si tratta dei riferimenti alla nota dell'Ufficio nota dell'Ufficio del Garante Privacy del 30.4.2024 prot. n. 52629, e alla nota del Ministero della Salute del 7.5.2024 prot. n. 6596). Si osserva, tuttavia, che nel testo finale del D. Min. Salute 5.7.2024, tale specificazione appare mancante.

RAFFAELLA GRISAFI

DM 22 Marzo 2024:
https://www.gazzettaufficiale.it/eli/id/2024/04/24/24A02057/SG
DM 5 Luglio 2024:
https://www.gazzettaufficiale.it/eli/id/2024/07/30/24A03953/SG

ISSN 2239-8570

DM 9 Agosto 2024:
https://www.gazzettaufficiale.it/eli/id/2024/09/13/24A04725/SG
Scheda Informativa Garante Privacy:
https://www.gpdp.it/documents/10160/0/Oblio+oncologico+-+vademecum+2024.pdf/9596adf0-207e-5402-8d7a-d8c4a706416d?version=1.0

2024/3(8)VR

8. La decisione del Garante privacy olandese del 16.5.2024 contro Clearview per illecito trattamento di dati biometrici con finalità di riconoscimento facciale.

Clearview AI Inc. (**Clearview**) è una società americana che offre servizi di riconoscimento facciale. Tra le altre attività, Clearview ha costruito una banca dati con miliardi di foto ed immagini di volti umani, anche di cittadini olandesi. L'Autorità garante per la protezione dei dati personali olandese (*Autoriteit Persoonsgegevens*, **AP**), con provvedimento del 16 maggio 2024 (il **Provvedimento**) ha comminato una sanzione pecuniaria di 30.500.000€ a Clearview in seguito ad accertate plurime violazioni del regolamento (UE) 2016/679 (**GDPR**) e ad essa ha accompagnato quattro ordini di cessazione delle violazioni ancora in corso con previsione di sanzioni pecuniarie per il caso della loro inottemperanza.

Come riassunto nella premessa del Provvedimento, Clearview è stata ritenuta responsabile di aver: *i*) trattato, nell'ambito del servizio *"Clearview for law-enforcement and public defenders"*, i dati personali di soggetti residenti nel territorio dei Paesi Bassi in assenza di idonea base giuridica, in violazione degli artt. 5(1)(a) e 6(1) GDPR; *ii)* trattato, in esecuzione del medesimo servizio, dati biometrici in violazione dell'art. 9 GDPR; *iii)* mancato di informare adeguatamente gli interessati, in contrasto con gli artt. 12(1), 14(1) e (2) GDPR; *iv)* mancato di rispondere a due richieste di accesso da parte di interessati, in violazione degli artt. 12(3) e 15 GDPR; *v)* mancato di agevolare gli interessati nell'esercizio del loro diritto di accesso, in contrasto con gli artt. 12(2) e 15 GDPR. Agli addebiti illustrati, l'AP aggiungeva quello della mancata designazione di un rappresentante nell'Unione europea ai sensi dell'art. 27 GDPR. Al riguardo tuttavia, l'AP si asteneva dal comminare una sanzione per tale violazione sulla base del rilievo che Clearview era stata già sanzionata dalle Autorità garanti italiane e greche per tale violazione (per il provvedimento dell'Autorità italiana del 10.2.2022, v. in questa Rubrica la notizia n. 8 del numero 1/2022: 2022/1(8)GDI).

L'AP ha verificato che Clearview fornisce servizi che sfruttano la tecnologia del riconoscimento facciale impiegando un algoritmo in grado di analizzare i volti rappresentati in una data immagine, memorizzarne la struttura e identificarli successivamente. Il cuore di tale algoritmo consiste in un "modello", costruito utilizzando il c.d. apprendimento automatico, che converte il volto raffigurato in un codice univoco (*"embedding"* o

ISSN 2239-8570

"vettore"). Il confronto tra vettori consente all'algoritmo di cogliere la raffigurazione del medesimo volto (*rectius*, del volto del singolo interessato) in diverse immagini.

Sfruttando la descritta tecnologia, Clearview ha costruito un database composto da oltre 30 miliardi di foto di volti umani, provenienti da fonti online pubblicamente accessibili, tra cui piattaforme di social media, siti web personali e professionali, articoli di cronaca, foto segnaletiche e database pubblici contenenti informazioni su persone condannate. Per ogni immagine mostrante uno o più volti, Clearview registra le seguenti informazioni: l'URL della pagina web della foto originale; la foto stessa; informazioni illustranti le caratteristiche della foto, come la data e l'ora in cui è stata scattata (i cc.dd. "metadati"); il vettore relativo ai volti raffigurati.

Tali dati vengono raccolti dai cosiddetti *"crawler"*, software che registrano automaticamente le informazioni su Internet. Più in dettaglio, come riportato dalla stessa Clearview nella sua *"Company Overview"*, la società opera un'attività di c.d. "*scraping* non mirato" e sistematico, procedendo alla raccolta di dati indipendentemente dal fatto che un cliente di Clearview effettui una richiesta di ricerca. La mole di informazioni raccolte nel database viene infine utilizzata per l'addestramento dell'algoritmo.

Il servizio *"Clearview for law-enforcement and public defenders"*, oggetto della decisione (di seguito, in breve "**il servizio**"), consiste nel rendere consultabile il database ad autorità governative e investigative clienti di Clearview. Gli utenti del servizio, calcolando in anticipo i vettori per ogni foto, sono così messi in grado di effettuare ricerche "per volto" partendo da un'immagine digitale di un determinato soggetto (la c.d. "immagine sonda"). Quest'ultima viene caricata sui server di Clearview, che procede a calcolarne il vettore mediante il modello addestrato. Confrontando tale specifico vettore con gli altri registrati, si possono recuperare le foto che ritraggono (anche) l'interessato, comprensive dei relativi URL e degli altri dati personali idonei a identificarlo.

Nel Provvedimento, l'AP, dopo aver ricordato il Considerando 51 del GDPR a tenore del quale il trattamento di fotografie non dovrebbe essere sistematicamente considerato un trattamento di categorie particolari di dati personali, in quanto *« esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica»*, ha spiegato di ritenere che le operazioni di trattamento effettuate da Clearview rientrino nell'ambito di applicazione materiale del GDPR, per una serie di ragioni.

Innanzitutto, perché le foto raccolte da Clearview, le loro fonti e i relativi metadati sono qualificabili come dati personali ai sensi dell'art. 4, n. 1 GDPR, dal momento che i soggetti rappresentati sono persone fisiche riconoscibili e sia i metadati che l'URL possono concorrere a fornirne un'identificazione univoca. Inoltre, perché i vettori coniati dall'algoritmo devono qualificarsi come dati biometrici ai sensi dell'art. 4, n. 14 GDPR e dunque come dati particolari ai sensi dell'art. 9(1) GDPR. Al riguardo, com'è noto, la qualificazione come dato biometrico richiede un trattamento

ISSN 2239-8570

mediante uno specifico mezzo tecnico che consente l'identificazione o l'autenticazione univoca di una persona fisica, non essendo sufficiente la mera riconoscibilità delle persone fisiche effigiate. Ebbene, secondo l'AP, proprio l'illustrata conversione algoritmica delle foto raccolte in vettori soddisfa il predetto requisito.

Di poi, perché la finalità di identificazione univoca dei soggetti è insita nella natura stessa del servizio, per come sopra descritto (confronto fra i vettori dell'immagine sonda e quelli delle altre foto presenti nel database).

Quanto all'ambito territoriale di applicazione del GDPR, nel Provvedimento si ricorda che ai sensi dall'art. 3(2)(b) GDPR il Regolamento è applicabile anche a trattamenti effettuati da titolari non stabiliti nell'Unione su dati personali di interessati che si trovano nell'Unione quando il trattamento riguardi il monitoraggio di comportamenti di interessati, che abbiano luogo all'interno dell'Unione. Per quanto attiene strettamente a tale ultimo profilo, nel Provvedimento si ricorda il Considerando 24 del GDPR: «*Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*».

Relativamente all'applicazione del GDPR, nel Provvedimento si ricordava che con lettera del 17 marzo 2023, Clearview informava l'AP del fatto che, nonostante in passato la società avesse fornito agli interessati residenti nell'Unione informazioni sulla loro apparizione o meno tra i risultati di ricerca, tale pratica veniva successivamente interrotta in quanto Clearview riteneva che l'art. 15 GDPR non fosse applicabile ai suoi servizi.

Quanto all'accertamento dei fatti rilevanti, per contro, ribadito che Clearview, nello svolgimento dei propri servizi, eseguiva trattamenti di dati personali – inclusi quelli appartenenti a categorie particolari – l'AP accertava che il trattamento aveva riguardato anche dati di interessati olandesi, oltre che di cittadini di altri Stati membri dell'Unione. Tale circostanza risultava dimostrata dal fatto che in data 11 aprile 2023 Clearview rispondeva a una richiesta di accesso avanzata da un cittadino olandese allegando tre immagini che lo raffiguravano, a riprova dall'avvenuto *scraping* di siti web olandesi. L'accertamento dell'avvenuto trattamento di dati personali di cittadini europei risultava inoltre da decisioni adottate da diverse autorità nazionali di controllo (tedesca, italiana, britannica, francese, austriaca). In particolare, nel Provvedimento si ricordava il provvedimento del 10 febbraio 2022 del Garante privacy italiano (su cui v. in questa Rubrica la notizia n. 8 del numero 1/2022: 2022/1(8)GDI), dove veniva *inter alia* accertato anche come i cambiamenti nell'aspetto degli interessati non impedivano il loro riconoscimento, reso possibile attraverso una funzione tecnica che consente di collegare i nuovi dati a quelli vecchi, e che Clearview disponeva in tal modo di un archivio di informazioni costantemente aggiornato nel corso del tempo.

ISSN 2239-8570

Non solo. L'attività di ricerca e abbinamento di immagini consentiva ai clienti della società di estrarre informazioni ulteriori sui soggetti effigiati, quali lo stato di parentela, lo status di genitore, l'ubicazione o il luogo di residenza, l'uso di social media, le abitudini (ad esempio, se l'individuo in questione fuma o beve), la professione e le attività retribuite svolte (compreso il loro carattere lecito o meno). Con ciò, gli utenti di Clearview erano in grado di accedere ai diversi profili identitari dei soggetti rappresentati, ricostruendone la "storia" in chiave diacronica. È evidente l'interesse che tale servizio poteva destare per le autorità pubbliche, clienti di Clearview, e, massimamente, per le forze dell'ordine.

Per tali ragioni, l'AP concludeva che i trattamenti in esame dovessero rientrare nell'ambito territoriale di applicazione del GDPR.

Al quesito se Clearview potesse qualificarsi come titolare del trattamento ai sensi dell'art. 4, n. 7 GDPR veniva data risposta affermativa: sulla base di quanto descritto, infatti, l'AP accertava che Clearview determinava autonomamente scopo e modalità di funzionamento della propria piattaforma, cioè a dire il procedimento di estrazione dei dati, la compilazione del database, l'addestramento dell'algoritmo di riconoscimento facciale, la tecnologia specifica per il *matching* tra le foto caricate dall'utenza e quelle raccolte.

Quanto alla liceità del trattamento, delle basi giuridiche di cui all'art. 6 GDPR risultava astrattamente applicabile solo quella di cui alla lett. *f*), ossia la base del legittimo interesse. L'AP procedeva dunque a vagliare i tre presupposti cumulativi dell'anzidetta condizione di liceità del trattamento, ossia: il legittimo interesse del titolare del trattamento o di terzi; la necessità del trattamento per soddisfare tale legittimo interesse; la recessività, rispetto a quest'ultimo, degli interessi o dei diritti e libertà fondamentali dell'interessato rispetto.

Nel merito, occorreva, in primo luogo, verificare il perseguimento di un interesse ritenuto meritevole di protezione dall'ordinamento ed effettivamente tutelato dall'ordinamento. L'AP argomentava che tale interesse deve essere conforme alla legge, e ricordava la giurisprudenza della CGUE a tenore della quale esso deve essere anche sufficientemente specifico, attuale e concreto.

In sede di istruttoria, Clearview rifiutava di rispondere alle richieste formulatele in proposito dall'AP, ritenendosi non vincolata al GDPR. Gli accertamenti si incentravano, pertanto, sulle *privacy policy* pubblicate, che tuttavia si incentravano sulla base giuridica per il trattamento dei dati personali degli utenti del servizio (ossia i clienti di Clearview) o su adempimenti posti in essere per ottemperare ad altri requisiti di legge e si limitavano ad avvisare che la raccolta si appuntava su foto pubblicamente disponibili online.

Nel valutare la sussistenza del requisito in analisi, l'AP rilevava che il modello commerciale di Clearview consiste nel fornire l'accesso alla piattaforma a pagamento. Pertanto, emergeva un interesse eminentemente privato, espressivo di libertà di impresa, confliggente col diritto fondamentale alla protezione dei dati personali. Secondo l'AP, essendo il trattamento dei dati personali effettuato da Clearview (idoneo a violare i

ISSN 2239-8570

diritti fondamentali degli interessati) esattamente l'oggetto dell'attività commerciale svolta da Clearview con terzi (e non un aspetto secondario o incidentale) Clearview non può invocare la base del legittimo interesse ai sensi dell'art. 6(1)(f) GDPR. Ciò in quanto, così si trova argomentato nel Provvedimento, la libertà d'impresa non può estendersi fino al punto di comprendere attività la cui realizzazione quasi completamente coincide con la violazione di diritti fondamentali di terzi.

Quanto all'interesse degli utenti, clienti di Clearview (autorità governative e organi di polizia/investigativi), riassumibile nell'esercizio delle attività di contrasto della criminalità, risultava ostativa l'espressa disposizione normativa di esclusione dell'applicabilità dell'art. 6(1)(f) GDPR *«al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti»*. Né tantomeno l'interesse generale alla repressione della criminalità poteva dirsi sufficiente, secondo l'AP, ad integrare l'echeggiata condizione.

Ciò solo avrebbe esaurito il punto. Nondimeno, l'AP chiosava anche sulle condizioni di necessità e bilanciamento.

In proposito veniva ricordata la giurisprudenza della CGUE, per la quale il test di necessità impone che il trattamento sia strettamente funzionale a soddisfare il legittimo interesse e non siano disponibili a tal fine mezzi meno invasivi; e che tale seconda condizione deve essere esaminata alla luce del principio di minimizzazione di cui all'art. 5 GDPR. Tanto premesso, l'AP argomentava che neppure tale requisito risultava rispettato da Clearview, per almeno due ragioni. Anzitutto, perché della mole di dati estratti tramite lo *scraping* non mirato un gran parte risultava destinata a non essere concretamente impiegata per le ricerche degli utenti. Di poi, perché l'ampia formulazione del periodo di conservazione dei dati contenuta nella *privacy policy* di Clearview le consentiva di tenere questi ultimi a propria disposizione per lungo tempo.

Quanto al bilanciamento della libertà d'impresa con i diritti e le libertà fondamentali degli interessati, l'AP ricordava che esso deve basarsi sulle peculiarità del caso concreto, e che, sulla base della giurisprudenza della CGUE, devono osservarsi i seguenti parametri: la gravità del pregiudizio ai diritti e alle libertà dell'interessato; la natura dei dati personali raccolti; i metodi specifici di trattamento, con enfasi sul numero dei soggetti aventi accesso a tali dati; le ragionevoli aspettative dell'interessato, ascrivibili al rapporto intrattenuto col titolare del trattamento, a che i suoi dati non vengano ulteriormente trattati (arg. *ex* Considerando 47 GDPR); le eventuali garanzie offerte dal titolare del trattamento.

Alla stregua di questi parametri, l'AP affermava che, nel caso di specie, un ragionevole bilanciamento mancava.

Veniva in particolare ritenuto rilevante la circostanza che, come detto, l'impiego da parte di Clearview della tecnologia di riconoscimento facciale si qualifica come trattamento di dati biometrici in vista dell'identificazione univoca di un individuo *ex* artt. 4, n. 14 e 9(1) GDPR. Inoltre, l'AP sottolineava che si tratta di operazioni su larga scala, per di più coinvolgenti anche minori, meritevoli di *«una specifica protezione (...) in quanto (...) meno consapevoli dei rischi»* (Considerando 38 GDPR). Inoltre, l'AP

ISSN 2239-8570

rilevava il difetto di opportune misure di cancellazione automatica delle foto presenti nel database una volta che esse cessavano di essere pubblicate su Internet (ad esempio perché l'interessato aveva modificato le impostazioni sulla privacy del proprio account di social media o la foto veniva rimossa da un sito web accessibile al pubblico). Ancora, l'AP rilevava che nessuna aspettativa circa il trattamento da parte di Clearview poteva dirsi ipotizzabile nel caso di specie, posto che tra gli interessati e Clearview non si dava alcun preesistente rapporto giuridico. Infine, nel Provvedimento si negava la possibilità di ritenere assolti gli obblighi di trasparenza imposti dal GDPR (v. *infra*).

La conseguenza, secondo AP è che gli interessi e i diritti fondamentali degli interessati sono stati gravemente violati, in assenza di ragionevoli aspettative e in assenza di salvaguardie per gli interessati minimamente sufficienti. L'AP concludeva dunque affermando che le posizioni soggettive degli interessati, in difetto di un legittimo interesse idoneo a fondare il trattamento ai sensi degli artt. 5 e 6 GDPR, dovessero prevalere sull'interesse meramente privatistico all'esercizio di attività di impresa da parte di Clearview.

Per quanto attiene specificamente ai requisiti di liceità del trattamento di dati biometrici, in considerazione dei significativi rischi che esso è idoneo a produrre, nel Provvedimento si ricordava come l'art. 9 GDPR imprime al par. 1 un divieto, superabile nei casi eccezionali di cui al par. 2, e che, in questo contesto, rilevano, in particolare, i casi di cui alle lett. *a*) ed *e*), ossia, rispettivamente: il consenso esplicito dell'interessato; l'avere il trattamento a oggetto dati personali resi manifestamente pubblici dall'interessato. L'AP ricordava anche che tali eccezioni, come chiarito dalla giurisprudenza della CGUE, devono essere interpretate in senso restrittivo.

Anche alla luce di ciò, dalle dichiarazioni sulla privacy esaminate, l'AP riteneva non potersi evincere alcun motivo di eccezione. Più precisamente, solo l'ipotesi di cui alla lett. *e*) era astrattamente applicabile al caso di specie. Tuttavia, essa richiedeva una esplicita e chiara dichiarazione affermativa dell'interessato a rendere accessibili al pubblico i propri dati personali. Al riguardo, la mera circostanza che questi si trovassero online non poteva dirsi sufficiente a rappresentare un intento di questo tipo.

Nessun motivo legittimo di eccezione ai sensi dell'art. 9(2) GDPR era dunque invocabile da Clearview, di talché le operazioni da questa poste in essere dovevano ritenersi in contrasto col divieto di cui al par. 1.

L'AP proseguiva l'analisi soffermandosi sui doveri di trasparenza.

Com'è noto, l'art. 5(1)(a) GDPR pone la trasparenza tra i principi fondamentali applicabili al trattamento di dati personali. Nei Considerando 60 e 39 GDPR si chiarisce che l'interessato deve essere informato dell'esistenza del trattamento, delle sue finalità e dei rischi, delle regole, delle garanzie, dei diritti di cui è titolare e delle modalità di esercizio degli stessi. L'art. 12(1) GDPR, dal canto suo, stabilisce che il responsabile del trattamento adotta misure adeguate affinché gli interessati ricevano, per iscritto o con altri mezzi, le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio chiaro e semplice. Infine, le disposizioni di cui all'art. 14(1) e (2)

ISSN 2239-8570

GDPR fissano i requisiti sostanziali concreti che i titolari del trattamento devono rispettare per informare gli interessati quando le informazioni non sono state ottenute direttamente dall'interessato. Tali disposizioni sono particolarmente rilevanti, in quanto Clearview non riceveva i dati personali direttamente dagli interessati ma li estraeva da altre fonti (pubbliche), come le piattaforme dei social media.

In sede istruttoria, l'AP esaminava quattro diverse versioni della *privacy policy* di Clearview, aggiornate alle modifiche del: 13 gennaio 2019, 29 gennaio 2020, 20 marzo 2021, 29 dicembre 2022.

In esse, Clearview forniva una descrizione sommaria delle finalità del trattamento, senza fare riferimento a specifici motivi o legittimi interessi rilevanti ai sensi degli artt. 6 e 9 GDPR. Solo si accennava alla fornitura di servizi prestati ai propri clienti, quali autorità governative, servizi investigativi o altri servizi di sicurezza pubblici/privati, per collaborare alle indagini su possibili violazioni di leggi. Quanto ai tempi di conservazione delle informazioni, come sopra accennato, si impiegava la formula assolutamente generica *«per tutto il tempo in cui è possibile adempiere alle finalità»*. Sull'eventuale cessione a terzi dei dati derivanti dai modelli delle immagini raccolti, veniva precisato che questa era limitata a fornitori di servizi, altri fornitori e altri soggetti, senza tuttavia menzionare destinatari specifici o relative categorie. Inoltre, le informative del 2021 e del 2022 non indicavano i diritti degli interessati e le modalità di esercizio degli stessi, neppure la facoltà di reclamo. Solo per i cittadini della California, della Virginia e dell'Illinois, si rinviava a pagine web separate con moduli specifici per presentare, ad esempio, richieste di accesso, rettifica e/o cancellazione.

Pertanto, secondo l'AP nessuna delle predette versioni della *privacy policy* – anche senza considerare una serie di rilievi svolti nel Provvedimento su alcune contraddittorietà tra le diverse versioni – rispettava gli obblighi di trasparenza derivanti dagli artt. 12(1) e 14 GDPR, violando così l'art. 5 GDPR.

Il rilievo cruciale stava nel fatto che non veniva reso chiaro agli interessati la facoltà di Clearview di trattare le loro foto (compresi i metadati) a fini di riconoscimento facciale.

Nello specifico, la violazione stava nella mancata adozione di misure adeguate a rendere i soggetti: delle basi giuridiche del trattamento; dei periodi di conservazione; delle (categorie di) destinatari dei dati; dei dettagli dei trasferimenti verso paesi terzi; dei diritti esercitabili; della possibilità di presentare reclamo; della fonte specifica di provenienza dei singoli dati. In proposito, la mera pubblicazione di un'informativa sul sito web di Clearview non veniva considerato sufficiente dall'AP per adempiere agli obblighi di cui all'art. 14 GDPR.

Sul diritto all'accesso da parte degli interessati, l'art. 12(2) GDPR stabilisce che il titolare del trattamento deve facilitare l'esercizio dei diritti di cui agli articoli dal 15 al 22 GDPR (v. altresì Considerando 59 GDPR). Il par. 3 dell'art. 12 GDPR prescrive altresì l'obbligo di informazione sull'andamento dell'esame della richiesta, da assolversi senza indebito ritardo e in ogni caso entro un mese dal ricevimento della richiesta

ISSN 2239-8570

(prorogabile di altri due mesi se necessario, tenendo conto della complessità e del numero delle richieste). Ai sensi dell'art. 15(1) GDPR, infine, l'interessato ha diritto a sapere se sia o meno in corso un trattamento di dati personali che lo riguarda e, in tal caso, a ottenere l'accesso a tali dati.

Come si è detto, la versione del 2022 della *privacy policy* di Clearview ometteva riferimenti ai diritti summenzionati. Non solo. Nella sua risposta del 17 marzo 2023, la società informava l'AP di aver cessato di rispondere alle richieste di accesso, ritenendosi non soggetta al GDPR.

Per tali ragioni, l'AP affermava la violazione da parte di Clearview degli artt. 12(3) e 15 GDPR.

Infine, nel presupposto, ritenuto assolto nel caso di specie, come sopra ricordato, dell'applicazione dell'art. 3(2) GDPR, l'AP rilevava la violazione dell'art. 27 GDPR, ossia della disposizione che impone che sia designato per iscritto un rappresentante nel territorio dell'Unione (come definito all'art. 4, n. 17 GDPR), a meno che il trattamento: *a*) sia occasionale e non includa un trattamento su larga scala di categorie particolari di dati di cui all'art. 9(1) GDPR, o di dati personali relativi a condanne penali e a reati *ex* art. 10 GDPR e sia improbabile un rischio per i diritti e le libertà delle persone fisiche; *b*) sia effettuato da autorità pubbliche o organismi pubblici. Più precisamente, ai sensi dell'art. 27(3) GDPR, il rappresentante deve essere stabilito in uno degli Stati membri in cui si trovano gli interessati i cui dati personali sono trattati in relazione all'offerta di beni o servizi o il cui comportamento è monitorato.

Al riguardo, l'AP accertava che Clearview operava il monitoraggio del comportamento degli interessati nell'Unione non designando un rappresentante nel territorio della stessa. La società motivava tale omissione sostenendo di non avere clienti nei Paesi Bassi e nell'Unione e di non essere coinvolta nel monitoraggio dei comportamenti di soggetti all'interno del territorio dell'Unione.

Tuttavia, si è detto che l'AP concludeva per l'applicabilità del GDPR ai trattamenti posti in essere da Clearview, proprio ai sensi dell'art. 3(2)(b) GDPR e in particolare in relazione alla conclusione che il trattamento di Clearview comporti un monitoraggio dei comportamenti degli interessati, che hanno luogo all'interno dell'Unione.

Pertanto, non potendo applicarsi l'eccezione di cui alla lett. *b*) dell'art. 27(2) a cagione della natura privata della società, veniva statuita anche la violazione dell'art. 27 GDPR.

VALENTINO RAVAGNANI

file:///C:/Users/Orlandos/Downloads/Decision%20fines%20and%20orders%20subject%20to%20a%20penalty%20Clearview.pdf

https://www.autoriteitpersoonsgegevens.nl/en/documents/decision-fine-clearview-ai

ISSN 2239-8570

2024/3(9)FG

9. L'annuncio del 26.9.2024 dal Garante privacy italiano di aver avviato un'indagine sull'accordo tra Open AI ed alcuni editori italiani di testate giornalistiche (GEDI, RCS)

Con comunicato stampa del 26.9.2024, il Garante per la protezione dei dati personali (il **Garante** o l'**Autorità**) ha dichiarato di aver puntato la sua attenzione sugli accordi tra OpenAI (l'azienda che realizza ChatGPT) e due dei principali gruppi editoriali italiani, RCS MediaGroup (**RCS**) e GEDI Gruppo Editoriale (**GEDI**). L'obiettivo dell'Autorità è verificare se tali intese rispettino la normativa vigente in materia di protezione e circolazione dei dati personali, in particolare nel contesto della condivisione e sfruttamento dei contenuti editoriali per l'addestramento di modelli di intelligenza artificiale, come quelli sviluppati da OpenAI.

Al centro di questa questione vi è la conformità al Regolamento (UE) 2016/679 (**GDPR** o il **Regolamento**), e, in particolare, delle disposizioni dell'art. 6 GDPR per le quali qualsiasi trattamento di dati personali deve essere giustificato da una base giuridica conforme, tra cui il consenso o il legittimo interesse. Il Garante potrebbe concentrarsi sul rispetto di tali disposizioni da parte di OpenAI e degli editori coinvolti, verificando se nei contenuti editoriali utilizzati per addestrare i modelli di IA siano presenti dati personali e come questi siano trattati, ed ulteriormente accertando se il trattamento sia rispettoso delle disposizioni in materia di trasparenza e minimizzazione previste dal Regolamento.

Gli accordi tra OpenAI, RCS e GEDI sembrano infatti prevedere la concessione in licenza di contenuti editoriali, volti a migliorare la capacità dei modelli di intelligenza artificiale, come ChatGPT, di fornire risposte accurate e dettagliate. Tuttavia, rimangono aperte le sopra accennate questioni rilevanti per la privacy. In questo contesto, GEDI e RCS potrebbero ricoprire il ruolo di titolari del trattamento, mentre OpenAI potrebbe agire come responsabile del trattamento o anch'esso titolare, con conseguenti differenze sugli obblighi contrattuali e di sicurezza dei dati.

Un aspetto particolarmente rilevante in questo scenario riguarda il web scraping, ovvero la raccolta automatizzata di dati online. Questo processo è spesso utilizzato per arricchire i modelli di IA generativa con grandi volumi di dati. Tuttavia, se questi dati includono informazioni personali identificabili, la pratica deve rispettare il GDPR. Del web scraping si è già occupato il Garante, in una recente Nota informativa del 20.5.2024 (su cui v. in questa Rubrica la notizia n. 31 del numero 2/2024: 2024/2(31)SB) sotto il profilo delle possibili azioni di contrasto al fenomeno.

L'iniziativa del Garante, che, come tipicamente nel caso di avvio di istruttorie, verosimilmente comporterà la richiesta di informazioni dettagliate agli editori coinvolti e ad OpenAI, si colloca dentro questo scenario, in cui si vanno delineando le misure tecniche necessarie affinché gli editori, in qualità di titolari del trattamento, possano contrastare il web scraping o renderlo conforme ai requisiti di cui al Regolamento.

ISSN 2239-8570

Sempre in questo contesto, si segnala la questione sollevata di recente dall'autorità di controllo irlandese (v. *infra* notizia n. 10, in questo numero di questa Rubrica) sulla necessità ai sensi dell'art. 35 GDPR di esperire una valutazione d'impatto sul trattamento dei dati (*Data Protection Impact Assessment* o **DPIA**) per valutare il rischio per i diritti e le libertà degli interessati derivante dal trattamento dei dati a fini di addestramento dei modelli IA.

FRANCESCO GROSSI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10057722

2024/3(10)SO

10. L'annuncio del Garante privacy irlandese del 12.9.2024 di aver avviato un'indagine per verificare se Google ha svolto una DPIA per lo sviluppo del modello di IA 'PaLM2'

La *Data Protection Commission* irlandese (**DPC** o **Garante privacy irlandese**) ha annunciato con comunicato stampa del 12 settembre 2024 di aver avviato un'indagine su Google Ireland Limited (**Google**) ai sensi della Sezione 110 del Data Protection Act 2018.

L'indagine è volta ad accertare se Google ha assolto a tutti gli obblighi che avrebbe dovuto assolvere ai sensi dell'art. 35 del regolamento (UE) 2016/679 (**GDPR** o il **Regolamento**) relativamente allo sviluppo del suo modello di IA per finalità generali *Pathways Language Model 2* (**PaLM 2**).

Il Garante Privacy irlandese assume che per lo sviluppo di PaLM2 Google abbia trattato dati personali di persone fisiche che si trovano nell'Unione europea o nello Spazio Economico Europeo, e ritiene che tale circostanza renda obbligatorio per Google effettuare una valutazione d'impatto sulla protezione dei dati (**DPIA**, acronimo da *Data Protection Impact Assessment*), ai sensi dell'art. 35 GDPR.

L'art. 35(1) GDPR prevede che una DPIA è obbligatoria quando un tipo di trattamento, che prevede in particolare l'uso di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento.

Nel comunicato stampa, il Garante Privacy irlandese ha precisato che l'indagine è volta ad accertare se Google abbia effettuato una DPIA prima di aver dato inizio alle operazioni di sviluppo di PaLM 2, e, in caso affermativo, se abbia osservato tutti gli obblighi che il Regolamento prevede debbano osservarsi per compiere tempestivamente, correttamente ed esaustivamente tale valutazione.

La DPC ha ricordato che il rispetto delle prescrizioni del GDPR in materia di DPIA è di cruciale importanza per assicurare che i diritti e le libertà fondamentali delle persone fisiche siano adeguatamente presi in considerazione e protetti nel contesto di processi di trattamento di dati

ISSN 2239-8570

personali che comportano un rischio elevato di pregiudizio degli stessi diritti e libertà, e che tra le finalità della DPIA vi è quella di assicurare che il trattamento sia necessario e proporzionato e che salvaguardie appropriate siano adottate alla luce dei rischi evidenziati grazie alla valutazione.

Infine il Garante privacy irlandese ha dichiarato nel comunicato che l'indagine avviata nei confronti di Google per PaLM 2 fa parte di un più ampio impegno che la medesima autorità ha assunto, lavorando in modo congiunto con le altre autorità di controllo dell'Unione europea e dello Spazio Economico Europeo, per regolare il trattamento dei dati personali di interessati dell'Unione europea e dello Spazio Economico Europeo per finalità di sviluppo di modelli e di sistemi di intelligenza artificiale.

SALVATORE ORLANDO

https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-launches-inquiry-google-ai-model

2024/3(11)FP

11. I lavori dell'UNCITRAL nel settore del commercio digitale e l'approvazione del Model Law sulla contrattazione automatizzata (MLAC) del luglio 2024.

Nel corso della cinquantasettesima sessione (15 luglio 2024), la Commissione delle Nazioni Unite per il diritto commerciale internazionale (UNCITRAL) ha approvato il modello di legge MLAC sulla contrattazione automatizzata *(Model Law on Automated Contracting*). Lo sviluppo del MLAC è stato affidato allo Working Group IV dell'UNCITRAL al fine di garantire la maggior continuità possibile con le precedenti iniziative dedicate al commercio elettronico. L'UNCITRAL è la commissione delle Nazioni Unite per il diritto commerciale internazionale (*United Nations Commission on International Trade Law*). Essa ha il mandato di promuovere l'armonizzazione progressiva e la modernizzazione del diritto del commercio internazionale, e persegue questo obiettivo attraverso la preparazione e la promozione dell'uso e dell'adozione di strumenti legislativi e non legislativi in vari settori del diritto commerciale. Uno di questi settori è il commercio elettronico – o "commercio digitale" – per il quale l'UNCITRAL ha preparato una serie di modelli di legge (*Model Law*), di cui l'ultimo è il MLAC, e una Convenzione, precisamente:

MLEC UNCITRAL Model Law on Electronic Commerce (1996)

MLES UNCITRAL Model Law on Electronic Signatures (2001)

ECC United Nations Convention on the Use of Electronic Communications in International Contracts (2005)

MLETR UNCITRAL Model Law on Electronic Transferable Records (2017)

ISSN 2239-8570

MLIT UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (2022)

MLAC UNCITRAL Model Law on Automated Contracting (2024)

In vista del prossimo incontro (18-22 Novembre 2024), lo Working Group IV discuterà inoltre il secondo draft delle regole sui Data Provision Contracts, che potrebbero in futuro essere incorporate in un Model Law o in Model Contract Clauses. L'iniziativa ha lo scopo di fornire certezza giuridica relativamente alla circolazione contrattuale dei dati, dalle modalità di trasferimento fino alla identificazione dei rimedi.

Questi testi ambiscono ad abilitare e facilitare l'uso di mezzi elettronici per intraprendere attività commerciali, sono stati utilizzati in oltre cento Stati in tutto il mondo. I testi sul commercio elettronico dell'UNCITRAL riguardano prevalentemente le comunicazioni tra le parti contrattuali commerciali tramite "messaggi di dati" (i.e. mediante mezzi elettronici, magnetici, ottici o simili). I testi precedenti, come il Modello di legge UNCITRAL sul Commercio Elettronico del 1996 (MLEC), sono stati preparati con particolare riferimento alle comunicazioni elettroniche tramite l'interscambio elettronico di dati attraverso sistemi informativi (EDI: *electronic data interchange*), mentre testi più recenti, come la Convenzione delle Nazioni Unite del 2005 sull'uso delle comunicazioni elettroniche nei contratti internazionali (*United Nations Convention on the Use of Electronic Communications in International Contracts:* ECC), sono stati elaborati con l'intento di regolare le comunicazioni elettroniche effettuate utilizzando tecnologie Internet.

I testi più recenti dell'UNCITRAL sul commercio elettronico, in particolare il Modello di legge del 2017 sui titoli di credito elettronici (*Model Law on Electronic Transferable Records*: MLETR) e il Modello di legge del 2022 sull'identificazione elettronica transfrontaliera (*Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*: MLIT), hanno iniziato a riconoscere gli oggetti di scambio digitali e a facilitare l'uso di sistemi distribuiti. Altre questioni che richiedono uno sforzo di armonizzazione sono state presentate in un congresso organizzato nel 2017 per celebrare il cinquantesimo anniversario dell'UNCITRAL e per esplorare le nuove direzioni del commercio internazionale. Nel 2018, successivamente alla presentazione in seno all'UNCITRAL di una proposta per monitorare gli sviluppi relativi agli aspetti legali dei contratti intelligenti e dell'intelligenza artificiale (A/CN.9/960), è stato deciso che il lavoro esplorativo dell'UNCITRAL dovesse procedere sulla base di una comprensione più ampia delle questioni legali relative all'economia digitale, comprendente altri argomenti come l'uso delle tecnologie a registro distribuito, la gestione della supply chain e i flussi di dati transfrontalieri.

In questo contesto, l'UNCITRAL ha elaborato nel 2023 un importante documento ricognitivo e classificatorio dedicato alla tassonomia delle questioni giuridiche legate all'economia digitale (Taxonomy of legal issues related to the digital economy), da servire per le proposte e per i lavori preparatori dell'UNCITRAL su nuovi testi legislativi e non legislativi sul commercio digitale.

ISSN 2239-8570

In preparazione della MLAC, lo Working Group IV è stato investito del mandato di rivedere, in una prima fase, le precedenti disposizioni UNCITRAL, al fine di verificare quali di esse possano essere adattate al contesto dell'economia digitale. Questo approccio è funzionale a sviluppare, in una seconda fase, nuove disposizioni per affrontare le ulteriori questioni derivanti dall'uso dell'automazione e dell'intelligenza artificiale nella contrattazione. L'obiettivo più generale della MLAC sulla contrattazione automatizzata è di fornire chiarezza e certezza giuridica alle imprese che si avvalgano di sistemi automatizzati per la formazione e l'esecuzione dei propri contratti e ai destinatari degli effetti giuridici corrispondenti.

Gli artt. 1-2 MLAC esordiscono richiamando alcune definizioni essenziali e specificando l'ambito di loro applicazione, a partire dall'uso di sistemi automatizzati nella contrattazione. Secondo la definizione datane nell'art. 1, par. 1 MLAC, la formazione e l'esecuzione del contratto avvengono tipicamente attraverso lo scambio di «data messages» contenenti input determinati di comunicazione – come, ad esempio, di proposta e accettazione, ovvero di evasione ordini ed effettuazione di pagamenti – all'interno dei quali sono poi memorizzate le clausole negoziali. Si tratta di sistemi in grado di coprire l'intero ciclo di vita del contratto, dalla negoziazione, alla formazione (art. 2, par. 1, lett. a MLAC) fino alla sua esecuzione e alla risoluzione di eventuali controversie (art. 2, par. 1, lett. b MLAC), senza che sia necessario il ricorso ad alcun intervento umano (art. 1, par. 2 MLAC). I sistemi automatizzati vengono distinti in deterministici, quando producono risultati prevedibili in base a determinati input, e sistemi non deterministici, come quelli che fanno uso dell'intelligenza artificiale (art. 1, par. 2 MLAC). L'ambito di applicazione è dunque particolarmente ampio, poiché copre sistemi con grado variabile di sofisticatezza, da quelli che si limitano a generare un medesimo output a partire da uno stesso input («ruled-based systems»), fino a quelli nei quali l'intervento della tecnologia dell'intelligenza artificiale introduce uno spettro più o meno ampio di incognite nella produzione dei risultati. I lavori preparatori della MLAC riconoscono comunque che, allo stato dell'arte, i sistemi automatizzati di contrattazione vengano usati soprattutto nel contesto di transazioni a basso costo e con un numero inferiore di variabili.

L'art. 3 definisce le regole sull'interpretazione della MLAC, sottolineandone il collegamento con i precedenti strumenti di armonizzazione nel settore del commercio elettronico. In primo luogo, sottolinea che lo scopo di promuovere l'uniformazione a livello internazionale nell'applicazione di queste regole e l'osservanza del principio di buona fede debbano costituire i criteri principi nell'interpretazione del MLAC. In secondo luogo, nelle materie non specificamente regolate, si dovrà continuare a far applicazione dei principi sviluppati nei precedenti testi sul commercio elettronico.

L'art. 4 introduce il concetto di neutralità tecnologica, stabilendo che il MLAC non imponga l'uso di alcuna tecnologia o sistema specifico per la contrattazione automatizzata. L'obiettivo è quello di garantire alle imprese la libertà di scegliere le tecnologie che meglio si adattino alle loro attività, senza che ciò possa determinare, di per sé, una violazione dei requisiti di

ISSN 2239-8570

legge. La neutralità tecnologica rappresenta inoltre il criterio per garantire la flessibilità del quadro giuridico e la sua attività ai progressi della scienza, che renderebbero altrimenti obsoleta la cornice normativa con l'emergere di nuove forme di sistemi automatizzati.

Gli artt. 5 e 6 MLAC concernono il riconoscimento di effetti giuridici ai contratti conclusi attraverso un sistema automatizzato. L'art. 5 MLAC sancisce che i contratti formati o eseguiti in conformità di questo sistema siano idonei a produrre effetti giuridici vincolanti per le parti contraenti. Detto in altri termini, la sola circostanza per cui le parti del contratto abbiamo impiegato sistemi automatizzati per la formazione o l'esecuzione dell'accordo non può venir dedotta come argomento a sostegno della pretesa invalidità o inefficacia. Inoltre, non solo agli inputs originari, ma anche a quelli ricevuti dopo la formazione del contratto (ad esempio, gli aggiornamenti dinamici delle informazioni) le parti possono riconoscere effetti giuridici (art. 6 MLAC). Il principio garantisce insomma che le interazioni fra il contratto e l'ambiente nel quale opera – come nel caso della fluttuazione dei prezzi – non ne compromettano l'esecuzione. Questo approccio si è ben radicato ha caratterizzato i lavori dell'UNCITRAL fin dalla Model Law sul Commercio Elettronico e ha di mira l'obiettivo di garantire che i processi automatizzati godano dello stesso status giuridico dei metodi contrattuali tradizionali.

L'art. 7 MLAC riguarda l'attribuzione delle azioni eseguite dai sistemi automatizzati. L'art. 7, par 2 MLAC riconosce che ciascun input generato o inviato da un sistema automatizzato e, di conseguenza, i risultati che ne discendono, debba essere attribuito alla persona per conto della quale il sistema opera. Nell'ipotesi in cui il sistema automatizzato sia gestito da più parti, i lavori preparatori precisano che il criterio di attribuzione delle azioni a ciascuna parte segua le regole operative del sistema di riferimento. Ciò può comportare la necessità di risalire allo script che regola l'attività di uno smart contract, al fine di comprendere quali siano i fattori che vi danno avvio. La norma ha però una valenza più generale, nel chiarire che i sistemi automatizzati sono strumenti; dunque, non possiedono una autonoma personalità giuridica. In linea con le precedenti disposizioni UNCITRAL e la Raccomandazione UNESCO sull'etica dell'IA i loro risultati devono pertanto essere attribuiti alle persone fisiche o giuridiche che li hanno creati o che li governano. L'art. 7, par. 4 MLAC specifica, tuttavia, che dal principio di attribuzione non debba necessariamente discendere una regola di allocazione della responsabilità, che chiede invece di verificare l'identità del soggetto che sopporti le conseguenze giuridiche derivanti da un certo output. In altre parole, l'art. 7 MLAC non pregiudica l'applicazione di norme di diritto sostanziale che disciplinino le conseguenze giuridiche del principio di attribuzione.

L'art. 8 affronta poi le questioni dell'intenzione, della conoscenza e della consapevolezza in relazione alla conclusione di contratti che coinvolgano l'uso di un sistema automatizzato, nonché delle conseguenze di azioni inattese. Quando la legge richiede la prova di questi stati d'animo nella formazione e nell'esecuzione del contratto, il MLAC stabilisce che tali requisiti sono soddisfatti attraverso l'esame della progettazione e del

ISSN 2239-8570

funzionamento tecnico del sistema automatizzato. La progettazione del sistema, comprese le regole e i parametri operativi, diventa così una prova fondamentale per dimostrare l'intenzione o la conoscenza, anche in assenza di un coinvolgimento umano diretto. Ciò ha lo scopo di garantire che i sistemi automatizzati siano trattati equamente nelle controversie legali, in particolare quando sorgono questioni relative a errori o frodi. La norma si occupa altresì di disciplinare le conseguenze relative al verificarsi di errori nella trasmissione di messaggi di dati generati dai sistemi automatizzati, stabilendo i presupposti per la tutela delle parti che abbiano fatto affidamento sui risultati da essi prodotti. L'affidamento non è tutelato quando la generazione e l'invio di un messaggio di dati da un sistema automatizzato sia frutto di un'azione che non poteva essere ragionevolmente prevista, a condizione che la parte affidataria sapesse o non potesse ignorare che il risultato fosse frutto di un'azione inattesa (art. 8, par. 1, lett. a-b MLAC). La MLAC si discosta dunque dall'iniziale proposta di far riferimento all'«error», evitando così ambiguità con la corrispondente nozione giuridica, utilizzando invece il concetto di «unexpected action». Nei lavori preparatori si precisa inoltre che le azioni inattese nella generazione e invio di messaggi di dati possono dipendere da falle nella progettazione del sistema o delle sue regole operative che, ad esempio, hanno permesso l'interferenza di terzi nel funzionamento del sistema automatizzato. La logica di questa regola è quella di rendere più trasparenti le caratteristiche e i limiti operativi dei sistemi automatizzati da parte delle imprese che ne fanno uso, incentivando così il rispetto di standard elevati professionalità e tracciabilità. L'art. 9 precisa però che la MLAC non pregiudichi l'applicazione di leggi sostanziali che disciplinino obblighi di disclosure sul design, operatività e utilizzo di sistemi automatizzati.

Nei lavori preparatori, lo Working Group ha esaminato anche le modalità per consolidare i vari testi UNCITRAL sul commercio elettronico e sulla contrattazione automatizzata in un quadro legislativo unificato. Il gruppo ha fornito una tabella di marcia per l'aggiornamento delle leggi e delle disposizioni esistenti nel MLEC, nel CEC e nei testi correlati, al fine di riflettere meglio l'uso della tecnologia moderna nella contrattazione. Lo Working Group suggerisce che questi testi consolidati potrebbero affrontare meglio le sfide poste dalle tecnologie digital ledger, dalla blockchain e da altre tecnologie emergenti. La raccomandazione formulata dal gruppo di lavoro è quella di sviluppare un nuovo testo legislativo consolidato per integrare le disposizioni relative alle firme elettroniche, ai messaggi di dati e ai sistemi automatizzati, garantendo alle imprese a livello globale un quadro giuridico chiaro e unificato per le transazioni digitali.

FEDERICO PISTELLI

https://uncitral.un.org/sites/uncitral.un.org/files/mlac_en.pdf

2024/3(12)GD

ISSN 2239-8570

12. La storica sentenza emessa il 5.8.2024 negli USA contro Google sul monopolio nelle ricerche online e nella pubblicità degli annunci di testo (causa *Stati Uniti d'America c. Google LLC*, 2024 WL 3647498).

Con una sentenza destinata a lasciare il segno (*Stati Uniti d'America c. Google LLC*, 2024 WL 3647498), il 5 agosto 2024, la Corte distrettuale degli Stati Uniti per il Distretto di Columbia ha stabilito che Google ha violato la Sezione 2 dello Sherman Act utilizzando illegalmente accordi di distribuzione esclusiva per mantenere il suo monopolio nel mercato dei servizi di ricerca online e della pubblicità degli annunci di testo (citando testualmente la sentenza "*Google has violated Section 2 of the Sherman Act by maintaining its monopoly in two product markets in the United States—general search services and general text advertising-through its exclusive distribution agreements"*).

Lo Sherman Act (del 1890) è la più antica legge antitrust degli Stati Uniti d'America e rappresenta il primo intervento del governo statunitense per limitare i monopoli e i cartelli. La Sezione 2 dello Sherman Act dispone che: *"Chiunque monopolizzerà, o tenterà di monopolizzare, o si combinerà o cospirerà con qualsiasi altra persona o persone per monopolizzare qualsiasi parte del commercio tra i vari Stati o con le nazioni straniere, sarà considerata colpevole di un crimine e, in caso di condanna, sarà punita con un'ammenda non superiore a 100.000.000 di dollari se si tratta di una società, o, se si tratta di qualsiasi altra persona fisica, a 1.000.000 di dollari, o con la reclusione non superiore a 10 anni, o con entrambe le pene, a discrezione della corte"*.

Le indagini, condotte dalla Federal Trade Commission e dal Dipartimento di Giustizia, sono iniziate nel 2020, durante l'amministrazione Trump, e si sono intensificate sotto il presidente Biden.

Nello specifico, con la sentenza in questione la Corte ha rilevato che:

- i servizi di ricerca generale e di pubblicità di annunci di testo sono dei mercati rilevanti da punto di vista del prodotto
- Google detiene il monopolio nei predetti mercati
- i contratti di distribuzione stipulati da Google sono accordi di esclusiva con effetti anticoncorrenziali
- Google non ha offerto valide giustificazioni affinché gli accordi di esclusiva stipulati potessero essere considerati pro-concorrenziali
- Google ha utilizzato il suo potere di monopolio per applicare tariffe sovra concorrenziali per gli annunci di testo.

Dalla sentenza di circa 280 pagine emessa dal giudice Amit P. Mehta si evince che Google spende miliardi di dollari all'anno per essere il motore di ricerca automatico su browser come Safari di Apple e Firefox di Mozilla. Ad esempio, secondo le risultanze istruttorie Google avrebbe pagato ad Apple un importo stimato in circa 20 miliardi di dollari per essere il motore di ricerca predefinito nel 2022 (punto 299 della sentenza).

Con la sentenza si è aperta la seconda fase del processo, attinente alla definizione della sanzione da irrogare a Google. Durante questa seconda

ISSN 2239-8570

fase le parti (*i.e.*, il Dipartimento di Giustizia e Google) potranno depositare le loro proposte di sentenza definitiva e gli elenchi dei testimoni, rispettivamente, il 20 novembre e il 20 dicembre 2024. Il giudice Mehta ha fissato le udienze per le richieste di risarcimento ad aprile 2025 e ha affermato che intende emettere una decisione entro agosto 2025.

Nel frattempo, Google ha dichiarato che impugnerà la sentenza in commento, preannunciando di voler andare fino in fondo. Vi è, quindi, la possibilità che il caso finisca alla Corte Suprema e che i tempi per la definizione della controversia siano più lunghi di quelli prospettati dal giudice federale Mehta.

La sentenza in commento è di particolare rilievo in quanto, se confermata, potrebbe costituire un "precedente" ed influenzare il mercato dei giganti del digitale. Infatti, questa decisione è solo la prima di una serie di altre sentenze attese nei confronti di Apple, Amazon, Meta e la stessa Google, contro cui il Dipartimento di Giustizia degli Stati Uniti d'America ha instaurato negli ultimi anni diversi giudizi, contestando il rispetto della normativa antitrust.

L'ultimo importante verdetto di una corte statunitense in un caso antitrust risale al 1998, reso all'esito del giudizio promosso dal Dipartimento di Giustizia degli Stati Uniti d'America contro Microsoft, su cui si è basato il giudice Mehta nel processo contro Google. In quell'occasione anche Microsoft era stata accusata di violare la sezione 2 dello Sherman Act, in quanto, quale monopolista nel mercato dei browser, impostava come predefinito *Internet Explorer* sul sistema operativo Windows (installato sulla quasi totalità di computer utilizzati all'epoca), a scapito dei concorrenti di allora come Netscape, Navigator e Opera. Durante il processo era stato dimostrato che, se un utente avesse provato a disinstallare Explorer, si sarebbe rallentato l'intero sistema operativo. *Explorer* era, dunque, parte integrante del software e l'installazione di un altro browser prevedeva processo un lungo e complesso. Alla sentenza seguì la richiesta di dividere Microsoft in due società distinte (la parte che si occupava di Windows e la parte che si occupava di *Explorer*). Dopo il processo in appello, si raggiunse un compromesso e, di fatto, non cambiò nulla. Il tramonto di *Internet Explore*r è stato più che altro legato all'evoluzione del mercato, dove all'inizio degli anni 2000 iniziarono a comparire nuovi browser, gratuiti, open source più moderni di *Explorer*.

In altri termini, il giudizio contro Google rappresenta una seconda possibilità per il Dipartimento di Giustizia, a seguito del "fallimento" nel caso Microsoft, per cercare di contrastare un dominio ritenuto anticoncorrenziale di una grande azienda tecnologica in un settore chiave.

Inoltre il Dipartimento di Giustizia americano starebbe considerando rimedi comportamentali e strutturali per impedire a Google di dare al suo motore di ricerca un vantaggio rispetto ai concorrenti o ai nuovi entranti in relazione all'utilizzo di suoi prodotti come *Chrome*, l'app store *Play* e il sistema operativo *Android*. Il Dipartimento di Giustizia potrebbe anche cercare di costringere Google a condividere i dati di ricerca degli utenti con i concorrenti e limitare la sua capacità di utilizzare i risultati di ricerca per addestrare nuovi modelli e prodotti di intelligenza artificiale generativa.

ISSN 2239-8570

Per quanto riguarda le misure a favore della concorrenza previste in Europa dal Regolamento (UE) 2022/1925 (**Digital Markets Act** o **DMA**), si può ricordare la recente indagine avviata nel marzo di quest'anno dalla Commissione europea ai sensi dell'art. 20 del DMA al fine di verificare, *inter alia*, un'eventuale violazione delle disposizioni del medesimo regolamento da parte di Alphabet - con riguardo alle regole in materia di "steering" di *Google Play* e di "self-preferencing" di *Google Search* - di Apple - con riguardo alle relative regole in materia di "steering" dell'*App Store* e di "choice screen" di *Safari* - e di Meta - con riguardo al modello "*pay or consent*" adottato dalla società (sull'avvio di questa indagine, v. in questa Rubrica la notizia n. 3 del numero 1/2024: 2024/1(3)RA).

GIORGIA DIOTALLEVI

https://static01.nyt.com/newsgraphics/documenttools/f6ab5c368725101c/43d7c2a0-full.pdf

ISSN 2239-8570