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).

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/

* Contributo non sottoposto a referaggio ai sensi dell'art. 9, V co., del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 42 del 20.02.2019.

2023/2(1)AF

Approvato il MiCA: il regolamento (UE) 2023/1114 del 31.5.2023 relativo ai mercati delle cripto-attività

Il 16 maggio 2023 il Consiglio dell'Unione europea ha adottato un regolamento sui mercati delle cripto-attività, ponendo fine ad un processo avviato con una proposta della Commissione europea nel settembre 2020. All'inizio di giugno 2023, il Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 ("**Regolamento MiCA**") è stato pubblicato nella Gazzetta ufficiale dell'Unione europea, entrando così in vigore. Il nuovo regime si applicherà dal 30 dicembre 2024, ad eccezione per le norme sui *token* di moneta elettronica e sui *token* collegati ad attività che si applicheranno dal 30 giugno 2024.

Il Regolamento MiCA proteggerà gli investitori e i consumatori- fornendo tutele contro i reati finanziari e la manipolazione del mercato- e preserverà la stabilità finanziaria. Al contempo, favorirà l'innovazione e l'attrattività del settore delle cripto-attività. Il nuovo quadro normativo contribuirà anche alla riduzione dell'elevata impronta di carbonio delle cripto-attività.

La proposta di regolamento MiCA è stata presentata dalla Commissione europea nel settembre 2020 [v. in questa rubrica la notizia n. 2 sul numero 2020/4 (2020/4(2)MS): http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf] nell'ambito di un pacchetto più ampio inteso a sviluppare un approccio europeo in materia di finanza digitale. Il Consiglio ha adottato il suo mandato negoziale nel novembre 2021. I triloghi tra i co-legislatori sono iniziati a marzo 2022 e si sono conclusi con l'accordo provvisorio del 30 giugno 2022 [v. la notizia n. 3 sul numero 2022/2 (2022/2(3)AF): http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf].

L'adozione formale del regolamento rappresenta la fase finale del processo legislativo.

Il Regolamento MiCA definisce le cripto-attività in generale come rappresentazioni digitali di valore o di diritti. Le cripto-attività possono essere trasferite e custodite tramite tecnologia a registro distribuito o tecnologie analoghe. Il nuovo quadro regolamentare disciplina le cripto-attività che non ricadono nell'ambito d'applicazione della normativa UE esistente, favorendone così la certezza del diritto. Le cripto-attività già disciplinate dalla normativa dell'UE continueranno a essere soggette alle norme vigenti. Il Regolamento MiCA si applicherà in generale a tre tipi di cripto-attività- i *token* collegati ad attività, i *token* di moneta elettronica e, da ultimo, altre cripto-attività quali gli *utility token*. I *token* collegati ad attività sono definiti come cripto-attività che mantengono un valore stabile ancorandosi a diverse attività, tra cui monete fiduciarie, merci o altre cripto- attività. I *token* collegati ad attività sono intesi come cripto-attività da poter impiegare come mezzo di pagamento per comprare beni e servizi e come riserva di valore. Anche i *token* di moneta elettronica- come i *token* collegati ad attività- ambiscono a mantenere un valore stabile ancorandosi, però, al valore di una sola moneta fiduciaria. Vengono considerati, quindi, come surrogati elettronici di banconote e monete. Da ultimo, le altre cripto-attività quali *utility token* sono da intendersi come una categoria residuale che vada a ricomprendere tutte le cripto-attività diverse dai *token* collegati ad attività i *token* di moneta elettronica.

Il Regolamento MiCA stabilisce requisiti di trasparenza e di informativa per l'offerta al pubblico e l'ammissione alla negoziazione di cripto-attività. Dispone, inoltre, requisiti di supervisione e di autorizzazione per gli emittenti di *token* collegati ad attività e per gli emittenti di *token* di moneta elettronica, nonché per i fornitori di servizi per le cripto-attività- come, ad esempio, le piattaforme di negoziazione e i portafogli in cui sono detenute le cripto-attività. Tali requisiti riguardano il funzionamento, la organizzazione e la governance di tali soggetti. Il regolamento dispone anche misure di tutela dei possessori di cripto-attività e dei clienti di fornitori di servizi per le cripto- attività. Ad esempio, i portafogli in cui sono detenute le cripto-attività dovranno garantire la protezione dei consumatori e saranno ritenuti responsabili in caso di perdita delle cripto-attività degli investitori. I fornitori di servizi per le cripto-attività non conformi verranno indicati in un registro pubblico gestito dall'Autorità bancaria europea. Si prevedono anche delle norme specifiche in materia di comunicazione dell'impatto ambientale delle cripto-attività, considerato l'elevato consumo energetico di alcune cripto-attività che si stima essere equivalente al quantitativo di energia consumato da alcuni paesi di medie dimensioni in un anno. In particolare, i fornitori di servizi per le cripto-attività dovranno dichiarare le informazioni sulla loro impronta ambientale e climatica.

Da ultimo, il Regolamento MiCA dispone misure di prevenzione contro gli abusi di mercato relativamente alle cripto-attività così da garantire l'integrità del relativo mercato.

ALICE FILIPPETTA

https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32023R1114

2023/2(2)AF

Verso l'euro digitale: la proposta di regolamento del 28.6.2023 COM(2023) 369 *final* sulla istituzione dell'euro digitale

Il 28 giugno 2023 la Commissione Europea ha presentato il c.d. "Pacchetto moneta unica", contenente, tra l'altro, la proposta legislativa COM(2023) 369 *final* che delinea il quadro giuridico per un possibile euro digitale (la "**Proposta**").

La Banca centrale europea ("**BCE**") insieme alle banche centrali nazionali dei paesi dell'area dell'euro sta valutando se introdurre un euro digitale. Attualmente, è ancora in corso la fase istruttoria, iniziata a ottobre 2021, in cui si stanno esaminando possibili caratteristiche e canali di distribuzione di un euro digitale [sulla decisione del Consiglio direttivo della BCE del 12 luglio 2021 di avviare l'analisi del progetto per un euro digitale v. in questa rubrica la notizia n. 7 del numero 2021/3 (2021/3(7)AF): http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf]. L'euro digitale sarebbe moneta della BCE in forma digitale, a integrazione delle banconote e delle monete in euro. L'euro digitale offrirebbe un mezzo di pagamento elettronico disponibile per chiunque nell'area dell'euro, sicuro e facile da usare.

La crescente digitalizzazione ha mutato le preferenze di pagamento che stanno propendendo oramai sempre più per mezzi digitali. Così facendo, cresce l'affidamento verso mezzi di pagamento emessi da entità private e diminuisce l'uso della moneta emessa dalla BCE in forma fisica, vale a dire il contante. Un euro digitale permetterebbe agli esercenti e ai consumatori di continuare ad avere accesso alla moneta pubblica- emessa dalla BCE- anche in un contesto digitale e andando ad affiancare il contante e le monete in euro. Come il contante, inoltre, un euro digitale garantirebbe un elevato livello di *privacy* e sarebbe accessibile a tutti i cittadini dell'area euro. L'euro digitale diventerebbe così il perno del sistema monetario e del sistema dei pagamenti odierno, sempre più digitalizzato. In tal modo, si rafforzerebbe anche la sovranità monetaria dell'area dell'euro a fronte di valute digitali di banca centrale dei paesi terzi e di altri mezzi di pagamento innovativi- quali, ad esempio, gli *stablecoin*-, favorendo al contempo la concorrenza e l'efficienza.

Un euro digitale non può essere emesso se non si delinei prima un quadro legislativo che ne getti le fondamenta dal punto di vista giuridico. Per tale ragione, la Commissione Europea ha presentato un possibile quadro legislativo su un euro digitale, inquadrandone gli elementi essenziali da un punto di vista giuridico. La Proposta tratta alcuni degli aspetti più rilevanti e al contempo discussi e controversi di un euro digitale.

In particolare, la Proposta prevede la distribuzione dell'euro digitale tramite banche commerciali e altri prestatori di servizi di pagamento (art. 13). L'euro digitale verrebbe distribuito agli utenti in cambio di depositi o di contante. Gli utenti diventerebbero così titolari di un conto di pagamento in euro digitale. L'emissione, invece, avverrebbe da parte della BCE e delle banche centrali nazionali degli stati membri dell'area euro (art. 4).

La Proposta affronta anche il tema della coesistenza dell'euro digitale con il contante e con altri mezzi di pagamento offerti da entità private. La Proposta dà libera scelta agli utenti sul mezzo di pagamento da impiegare per le transazioni, tra banconote e moneta in euro, euro digitale o altri mezzi di pagamento digitali privati. In tal modo, si garantisce sia l'accesso alle banconote e alle monete in euro che l'innovazione e la concorrenza nel settore dei pagamenti, prevedendo la coesistenza di più soggetti. La Proposta dà però corso legale all'euro digitale, come il contante, imponendone l'accettazione e garantendone un'ampia diffusione nonché un facile accesso (art. 7).

Solo utenti residenti o aventi sede in un paese dell'area euro avrebbero accesso all'euro digitale, fatta eccezione di alcuni casi particolari quali, ad esempio, residenti non dell'area euro che siano in viaggio per motivi professionali o personali nell'area euro. Simili restrizioni si applicherebbero all'uso dell'euro digitale al di fuori dell'area euro.

La Proposta prevede per le banche commerciali e per i prestatori di servizi di pagamento un obbligo di erogazione dei servizi di pagamento di base in euro digitale nel momento in cui un utente ne faccia richiesta (art. 17). L'erogazione di tali servizi avverrebbe gratuitamente, similarmente a quanto già accade con i servizi di pagamento esistenti. I prestatori di servizi di pagamento potrebbero prevedere delle commissioni nel momento in cui l'euro digitale sia collegato a conti da loro offerti o in cui si prestino dei servizi considerati non di base.

Uno degli obiettivi che si tentano di perseguire tramite un euro digitale è quello di assicurare l'inclusione finanziaria. La Proposta prevede alcune

disposizioni a tal fine. Innanzitutto, come già accennato, si dispone che le entità pubblicate designate dagli stati membri- quali, ad esempio, uffici postali o autorità regionali o locali- possano provvedere alla distribuzione di un euro digitale (art. 14). Ciò assicurerebbe l'accesso all'euro digitale anche a coloro che non desiderino aprire un conto di euro digitale con una banca o un altro prestatore di servizi di pagamento. Sarebbe poi possibile sia pagare tramite euro digitale *online* che detenere l'euro digitale localmente su dispositivi elettronici *offline* (art. 23). La possibilità di eseguire pagamenti e detenere euro digitale *offline* aumenta il rischio di riciclaggio e di finanziamento del terrorismo. Pertanto, la Proposta prevede che le transazioni in euro digitale siano soggette alla legislazione in materia, similarmente a quanto già accade per i mezzi di pagamento digitali privati. In futuro, si potrebbero prevedere limiti alle transazioni o all'ammontare detenuto di euro digitale.

Uno dei temi più controversi e più preoccupanti per il grande pubblico sull'euro digitale è anche la *privacy*. L'accesso ai dati personali degli utenti sarebbe equivalente a quello che si ha al momento per i pagamenti *online*, tramite conto ad esempio, e per il contante in caso di uso dell'euro digitale *offline* (art. 34). La BCE e le banche centrali nazionali non avrebbero accesso a dati sull'identità dei detentori dell'euro digitale e sull'uso che ne facciano (art. 35). La BCE e le banche centrali nazionali avrebbero accesso solo ai dati necessari al regolamento delle transazioni e al supporto dei prestatori dei servizi di pagamento nell'espletamento delle loro funzioni.

Altro punto fortemente dibattito è l'impatto che l'euro digitale avrebbe sul sistema bancario e finanziario e, da ultimo, sulla stabilità finanziaria. Come già visto, la Proposta fa sì che gli intermediari mantengano un ruolo essenziale, prevedendo che questi ne siano responsabili per la distribuzione. Tuttavia, la Proposta prevede delle tutele della stabilità monetaria e finanziaria ulteriori nel caso in cui si diffonda l'uso dell'euro digitale come riserva di valore. In particolare, stabilisce una serie di criteri che, se soddisfatti, potrebbero condurre all'imposizione di limiti sull'ammontare di euro digitale detenuto su base individuale (art. 16).

Quanto alla tecnologia di supporto dell'euro digitale, nell'articolato normativo della bozza di regolamento, la Proposta non offre indicazioni definitive. Nel Considerando 64 della Proposta si afferma che l'infrastruttura di regolamento dell'euro digitale dovrebbe cercare di garantire l'adattamento alle nuove tecnologie, compresa la tecnologia a registro distribuito. Tra le risposte alle FAQ della pagina dedicata all'euro digitale dalla BCE si dice che per la realizzazione dell'euro digitale l'Eurosistema sta sperimentando diverse soluzioni e tecnologie, sia accentrate che decentrate come la DLT, ma che non è stata presa ancora una decisione.

La proposta getta le fondamenta per euro digitale come nuova forma di moneta di banca centrale e ne regola gli elementi essenziali. Tuttavia, non ne sancisce la creazione. Una eventuale emissione dell'euro digitale avverrebbe solo su decisione del Consiglio Direttivo della BCE. La fase di istruttoria terminerà a ottobre 2023. Al termine, si avrà la decisione del Consiglio Direttivo se procedere con la fase successiva del progetto ed, eventualmente, se dare il via allo sviluppo di un euro digitale.

ALICE FILIPPETTA

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=comnat%3ACOM_2023_0369_FIN

https://www.ecb.europa.eu/paym/digital_euro/html/index.it.html

https://italy.representation.ec.europa.eu/notizie-ed-eventi/notizie/pacchetto-moneta-unica-nuove-proposte-sostenere-luso-del-contante-e-presentare-un-quadro-leuro-2023-06-28_it

2023/2(3)BC

(Segue) la proposta di regolamento del 28.6.2023 COM(2023) 368 *final* sulla fornitura di servizi di euro digitale da parte di fornitori di servizi di pagamento costituiti in Stati Membri la cui valuta non è l'euro

Unitamente alla proposta normativa contenente il quadro giuridico per l'adozione dell'euro digitale [su cui v. la notizia precedente], il 28 giugno 2023 la Commissione europea ha pubblicato la proposta COM(2023) 368 *final* contenente una bozza di regolamento denominata *"Proposal for a Regulation of the European Parliament and of the Council on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro and amending Regulation (EU) 2021/1230 of the European Parliament and the Council"* (la "**Proposta di Regolamento**").

La Proposta di Regolamento, come si intuisce dal titolo, è destinata a disciplinare, una volta

approvata, l'uso, la circolazione dell'euro digitale e la prestazione di servizi di pagamento in euro digitale da parte dei prestatori di servizi di pagamento (i "**PSP**") stabiliti negli Stati membri dell'Unione Europea che non adottano l'euro quale valuta nazionale (di seguito, per semplicità descrittiva, definiti "**Stati UE non-Euro**"). Dal punto di vista del perimetro applicativo, il regolamento si applicherà, pertanto, ai PSP costituiti e aventi sede legale in Stati UE non-Euro quali Danimarca, Bulgaria, Repubblica Ceca, Ungheria, Polonia, Romania e Svezia.

La Proposta di Regolamento, una volta approvata, andrà dunque a incidere in modo rilevante sulla prestazione dei servizi di pagamento da parte dei PSP dei paesi che non adottano l'euro; per tale ragione la Proposta di Regolamento si armonizza ed è conforme anche ai contenuti della Direttiva (UE) 2015/2366 sui servizi di pagamento nel mercato interno (la c.d. "**PSD2**" o Payment Services Directive 2) che, peraltro, è in predicato di essere emendata dalla direttiva PSD3 il cui contenuto è stato presentato, sotto forma di proposta, lo stesso giorno in cui è stato presentato il framework sull'euro digitale.

Per effetto di tale Proposta di Regolamento, i fornitori di servizi di pagamento di uno Stato UE-non Euro potranno offrire ai residenti dell'area euro servizi di pagamento in euro digitale unitamente ad altri servizi di pagamento o bancari, in regime di libera prestazione di servizi o in regime di stabilimento.

L'art. 1 della Proposta di Regolamento definisce, in dettaglio, gli scopi del futuro regolamento che, in sintesi, si possono riassumere in tre macroaree di intervento, ovvero:

(a) l'individuazione degli obblighi che i PSP costituiti negli Stati UE non-Euro devono adempiere quando forniscono servizi di pagamento basati sull'euro digitale;

(b) regole per la supervisione e l'applicazione degli obblighi di cui al punto (a) da parte degli Stati UE-non Euro;

(c) ulteriori obblighi specifici rivolti a produttori di *device* mobili di comunicazione e fornitori di servizi di comunicazione stabiliti negli Stati UE non-Euro.

Il perno su cui ruota il futuro impianto normativo della Proposta di Regolamento è l'art. 3 che stabilisce che i PSP costituiti negli Stati UE non-Euro possono fornire servizi di pagamento in euro digitale soltanto a:

a) persone fisiche e giuridiche residenti o stabilite all'interno di uno Stato membro che adotta l'Euro;
b) persone fisiche e giuridiche che hanno aperto un conto in euro digitale quando erano ancora residenti o stabiliti in uno Stato membro che adotta l'euro ma non risiedono più in tali Stati;
c) visitatori occasionali all'interno dello Stato UE-non Euro;
d) persone fisiche e giuridiche residenti o stabilite in uno Stato UE non-Euro purché – in questo caso - siano soddisfatte le condizioni stabilite dall'articolo 18 dell'adottando regolamento sull'euro digitale;
e) persone fisiche e giuridiche residenti o stabilite in paesi terzi, compresi territori soggetti a un accordo monetario con l'Unione europea, a condizione che siano soddisfatte le condizioni stabilite agli articoli 19 e 20 dell'adottando regolamento sull'euro digitale.

L'art. 18 della proposta di regolamento sull'euro digitale individua, in dettaglio, le condizioni da soddisfare affinché i PSP di uno Stato UE non-Euro possano prestare servizi di pagamento (in regime di libera prestazione di servizi o stabilimento) all'interno di tale Stato.

Tale articolo stabilisce infatti, al primo comma, che "*i fornitori di servizi di pagamento possono distribuire l'euro digitale solo a persone fisiche e giuridiche residenti o stabilite in uno Stato membro la cui valuta non è l'euro se la Banca centrale europea e la banca centrale nazionale di tale Stato membro hanno sottoscritto un accordo a tal fine*".

La sottoscrizione di tale accordo tra la BCE e la banca centrale dello Stato UE non-Euro deve rispettare determinati, inoltre, i requisiti previsti al secondo comma dell'art. 18, tra cui ad esempio: la notifica preliminare alla Commissione Europea e alla BCE, da parte dello Stato UE non-Euro, della richiesta di fornire accesso e utilizzo dell'euro digitale a persone fisiche e giuridiche residenti o stabilite in tale Stato; l'impegno da parte dello Stato UE non-Euro a garantire che la propria banca centrale si conformi a norme, linee guida, istruzioni o richieste della BCE aventi ad oggetto l'euro digitale; l'impegno a garantire, ancora, che la propria banca centrale fornisca informazioni sull'accesso e l'utilizzo dell'euro digitale alla BCE.

Il quarto comma dell'art. 18 della proposta di regolamento sull'euro digitale prevede, ulteriormente, che i PSO di uno Stato UE non-Euro devono rispettare determinati limiti quantitativi stabiliti dalla BCE in conformità all'articolo 16, paragrafo 4, sull'utilizzo dell'euro digitale da parte di persone fisiche e giuridiche.

Quanto invece alle condizioni richieste affinché i PSP residenti in uno Stato UE non-Euro prestino servizi di pagamento (in euro digitale) verso paesi terzi, l'art. 19 della proposta di regolamento sull'euro digitale prevede che tale valuta digitale possa essere distribuita a persone fisiche e giuridiche residenti o stabilite in paesi terzi a condizione che l'Unione Europea e il paese terzo interessato firmino preliminarmente un accordo.
In assenza di tale accordo tra l'Unione Europea e il singolo paese terzo, i PSP non potranno operare in euro digitale verso paesi terzi.
Il successivo art. 4 della Proposta di Regolamento prevede che i requisiti stabiliti all'articolo 13, all'articolo 14, paragrafo 1, al Capitolo V, all'articolo 18, al Capitolo VII, al Capitolo VIII e al Capitolo IX dell'adottando regolamento sull'euro digitale siano applicabili anche ai PSP di uno Stato UE non-Euro. Si rinvia pertanto, per l'analisi di tali articoli, al contributo dedicato al regolamento sull'euro digitale.
Va evidenziato che l'art. 4 della Proposta di Regolamento stabilisce che l'art. 33 del futuro regolamento sull'euro digitale si applicherà anche ai produttori di apparecchiature e dispositivi mobili, nonché ai fornitori di servizi di comunicazione elettronica, anche se residenti negli Stati UE non-Euro.
Per effetto di questo richiamo, i produttori di *device* mobili e i fornitori di servizi di comunicazione elettronica dovranno assicurare l'interoperabilità e l'accesso ai fornitori di servizi front-end e ai fornitori di servizi per l'identità digitale europea (anche nota come European Digital Identity Wallet, ancora in corso di sviluppo a livello europeo) garantendo, quindi, che siano disponibili le caratteristiche hardware e software necessarie per elaborare transazioni in euro digitale.
Infine, l'art. 5 della Proposta di Regolamento prevede che il quadro normativo inerente a (i) la vigilanza da parte delle autorità nazionali competenti, (ii) il regime sanzionatorio, (iii) le disposizioni di vigilanza e gli accordi di cooperazione le autorità competenti degli Stati membri di origine e degli Stati membri ospitanti troveranno applicazione anche in relazione alle attività dei PSP stabiliti in uno Stato UE non-Euro in relazione ai servizi aventi ad oggetto l'euro digitale.

BENEDETTO COLOSIMO

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=comnat%3ACOM_2023_0368_FIN

2023/2(4)SO

Gli emendamenti alla proposta di AI Act approvati dal Parlamento europeo il 14.6.2023

Il 14 giugno 2023, in sede di prima lettura nella procedura legislativa ordinaria, il Parlamento europeo (il **Parlamento**) ha approvato a larga maggioranza 771 emendamenti alla proposta di regolamento sull'intelligenza artificiale, c.d. **AI Act** o **AIA**, pubblicata dalla Commissione europea (la **Commissione**) il 21.4.2021 [sulla proposta della Commissione COM(2021) 206 *final* del 21.4.2021 v. in questa rubrica la notizia n. 1 sul numero 2021/2 (2021/2(1)SO): http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf; sul parere congiunto di EDPB e EDPS del 21.6.2021 alla proposta della Commissione in particolare quanto alla disciplina dei sistemi di IA di riconoscimento facciale v. la notizia n. 3 sul numero 2021/3 (2021/3(3)CR): http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf; sul parere della BCE del 29.12.2021 alla medesima proposta, v. la notizia n. 8 sul numero 2022/2 (2022/2(8)ES): http://www.personaemercato.it/wp-content/uploads/2022/08/Osservatorio-2-2022.pdf].
In precedenza, il 6 dicembre 2022, il Consiglio UE (il **Consiglio**) aveva approvato un testo di orientamento generale ("*general approach*") datato 25 novembre 2022, inteso, come da prassi, a facilitare le successive interlocuzioni e un possibile futuro accordo con il Parlamento (https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/).
In esito all'approvazione di questi emendamenti da parte del Parlamento, sono stati avviati i negoziati interistituzionali (triloghi) con il Consiglio e la Commissione per finalizzare l'iter legislativo, secondo la procedura legislativa ordinaria di codecisione, la quale prevede che il Consiglio esamini la posizione del Parlamento e decida se accettarla – nel qual caso il regolamento sarebbe adottato - o modificarla – nel qual caso la proposta tornerebbe al Parlamento per una seconda lettura.
Nel Parlamento, le discussioni sono state condotte in una procedura congiunta tra due Commissioni: quella sul mercato interno e la protezione del consumatore (IMCO) con il *rapporteur* italiano Brando Benifei, e quella sulle libertà civili, la giustizia e gli affari interni (LIBE) con il *rapporteur* rumeno Dragos Tudorache.

Il Parlamento ha adottato la sua posizione con 499 voti a favore, 28 contrari e 93 astensioni, apportando significative modifiche al testo della Commissione, tra le quali, le seguenti:

- È stata modificata la definizione di sistema di IA, dichiaratamente per allinearsi alla definizione proposta dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) [v. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449]. Nella nuova definizione, oltre all'abolizione del riferimento alle tecniche e agli approcci prima elencati nell'Allegato I della proposta della Commissione, si nota anche l'abolizione del riferimento ai "contenuti" tra le tipologie di *output* dei sistemi di IA: "un sistema automatizzato [*a machine-based system*] progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare *output* quali previsioni, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali".
- Sono state inserite alcune nuove definizioni, tra cui quelle di *foundation model* e *general purpose AI system*, ed è stato sostituito il termine *user* ('utente' in italiano) con *deployer* (in italiano reso con 'operatore', nonostante la stessa parola fosse già utilizzata, e sia tuttora utilizzata, nel testo italiano per *operator*).
- *Foundation model*, in italiano "modello di base", viene definito come "un modello di sistema di IA addestrato su un'ampia scala di dati, progettato per la generalità dell'*output* e che può essere adattato a un'ampia gamma di compiti distinti".
- *General purpose AI system*, in italiano "sistema di IA per finalità generali" viene definito come "un sistema di IA che può essere utilizzato e adattato a un'ampia gamma di applicazioni per le quali non è stato intenzionalmente e specificamente progettato".
- Sono stati formulati e definiti alcuni principî generali applicabili a tutti i sistemi di IA e anche a tutti i modelli di base (*foundation models*). Le definizioni dei principî enunciano i soli sistemi di IA ma la norma che li introduce fa chiaro che essi si applicano anche ai modelli di base ("Tutti gli operatori che rientrano nel presente regolamento si adoperano al massimo per sviluppare e utilizzare sistemi di IA o modelli di base conformemente ai seguenti principi generali che istituiscono un quadro di alto livello che promuova un approccio europeo antropocentrico coerente a un'intelligenza artificiale etica e affidabile, che sia pienamente in linea con la Carta e con i valori su cui si fonda l'Unione"). I principî generali sono dunque formulati e definiti come segue:
  "a) intervento e sorveglianza umani: i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani;
  b) robustezza tecnica e sicurezza: i sistemi di IA sono sviluppati e utilizzati in modo da ridurre al minimo i danni involontari e inaspettati, nonché per essere robusti in caso di problemi involontari e resilienti ai tentativi di alterare l'uso o le prestazioni del sistema di IA in modo da consentirne l'uso illegale da parte di terzi malintenzionati;
  c) vita privata [*privacy* in inglese] e governance dei dati: i sistemi di IA sono sviluppati e utilizzati nel rispetto delle norme vigenti in materia di vita privata [*privacy* in inglese] e protezione dei dati, elaborando al contempo dati che soddisfino livelli elevati in termini di qualità e integrità;
  d) trasparenza: i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente gli utenti delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti;
  e) diversità non discriminazione ed equità: i sistemi di IA sono sviluppati e utilizzati in modo da includere soggetti diversi e promuovere la parità di accesso, l'uguaglianza di genere e la diversità culturale, evitando nel contempo effetti discriminatori e pregiudizi ingiusti vietati dal diritto dell'Unione o nazionale;
  f) benessere sociale ed ambientale: i sistemi di IA sono sviluppati e utilizzati in modo sostenibile e rispettoso dell'ambiente e in modo da apportare benefici a tutti gli esseri umani, monitorando e valutando gli impatti a lungo termine sull'individuo, sulla società e sulla democrazia.
- È stato modificato e significativamente ampliato l'elenco dei sistemi di IA sottoposti ai divieti di immissione sul mercato, messa in servizio ed uso di cui all'art. 5 della proposta di AI Act (c.d. pratiche di IA vietate). Nel testo della Commissione, l'elenco comprendeva solo quattro tipologie di sistemi di IA; ora l'elenco

ne prevede nove. Secondo la proposta della Commissione, le prime due tipologie di sistemi di IA erano quelli idonei a falsare il comportamento delle persone in modo tale da procurare un "*danno fisico o psicologico*"; il nuovo testo parla di un "*danno significativo*". Come terza tipologia, la proposta della Commissione assoggettava al regime del divieto i sistemi di IA di c.d. *social scoring*, tuttavia solo relativamente al loro uso da parte di autorità pubbliche o per loro conto; mentre il nuovo testo ha eliminato questa limitazione. Infine, la proposta della Commissione vietava l'uso di sistemi di IA di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico soltanto se effettuato a fini di attività di contrasto svolte dalle autorità per la prevenzione, indagine, accertamento o perseguimento di reati o per esecuzione di sanzioni penali, fatta salva l'applicazione di talune eccezioni limitate; mentre nel testo adottato dal Parlamento, il divieto (sempre soltanto di uso) riguarda tutti i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico, senza limitazioni. Il testo adottato dal Parlamento ha aggiunto nello stesso articolo la previsione delle seguenti cinque tipologie di sistemi di IA e dei seguenti relativi divieti:

- divieto di immissione sul mercato, messa in servizio ed uso di sistemi di categorizzazione biometrica che classificano le persone fisiche in base ad attributi o caratteristiche sensibili o protetti o basati sulla deduzione di tali attributi o caratteristiche, ad eccezione di quelli destinati a essere utilizzati per scopi terapeutici approvati sulla base del consenso informato;
- divieto di immissione sul mercato, messa in servizio ed uso di sistemi di IA per effettuare valutazioni di rischio di reato o di recidiva di un reato o di un illecito amministrativo;
- divieto di immissione sul mercato, messa in servizio ed uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante *scraping* non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;
- divieto di immissione sul mercato, messa in servizio ed uso di sistemi di IA di riconoscimento delle emozioni nei settori dell'applicazione della legge, della gestione delle frontiere, sul luogo di lavoro e negli istituti di insegnamento;
- divieto di messa in servizio e di uso di sistemi di IA per l'analisi di filmati registrati di spazi accessibili al pubblico attraverso sistemi di identificazione biometrica remota "a posteriori". Il divieto non si applica nel caso di previa autorizzazione giudiziaria conformemente alla normativa dell'Unione e relativamente alle operazioni strettamente necessarie per la ricerca mirata collegata a uno specifico reato grave quale definito all'articolo 83, paragrafo 1, TFUE, già avvenuto, a fini di contrasto.

➢ I modelli di base (*foundation models*) hanno una loro specifica ed ampia disciplina, che contempla numerosi obblighi e requisiti per il fornitore, tra cui, in sintesi, e salvo specificazioni di dettaglio:

- l'obbligo di previa individuazione, riduzione e attenuazione dei rischi ragionevolmente prevedibili per la salute, la sicurezza, i diritti fondamentali, l'ambiente, la democrazia e lo Stato di diritto;
- l'obbligo di elaborare e incorporare soltanto insiemi di dati soggetti a idonee misure di *governance* dei dati;
- l'obbligo di progettare e sviluppare il modello di base al fine di conseguire, durante l'intero ciclo di vita, opportuni livelli di prestazioni, prevedibilità, interpretabilità, corregibilità, protezione e cibersicurezza;
- l'obbligo di utilizzare in fase di progettazione e di sviluppo del modello di base, gli *standard* applicabili per ridurre l'uso di energia, l'uso di risorse e i rifiuti, nonché per aumentare l'efficienza energetica e l'efficienza complessiva del sistema, nonché l'obbligo di progettare il modello di base in modo da consentire la misurazione e la registrazione del consumo di energia e risorse e, se tecnicamente fattibile, degli altri effetti ambientali che l'adozione e l'utilizzo dei sistemi può avere sul loro intero ciclo di vita;
- l'obbligo di redigere una documentazione tecnica e istruzioni per l'uso che possano consentire ai fornitori a valle di adempiere a determinati loro obblighi;
- l'obbligo di porre in essere un sistema di gestione della qualità per garantire e documentare l'osservanza ai suddetti obblighi;
- l'obbligo di registrare i modelli di base in una apposita banca dati dell'UE, conformemente a quanto previsto dal regolamento e nelle disposizioni di un suo allegato.

➢ Novità consistenti riguardano anche i «sistemi di IA ad alto rischio». Come nella proposta della Commissione, due sono le categorie dei sistemi di IA ad alto rischio: (i) i sistemi di IA destinati ad essere utilizzati come componenti

di sicurezza di prodotti, o che sono essi stessi prodotti, soggetti a valutazione di conformità *ex ante* da parte di terzi, ai sensi della normativa di armonizzazione dell'Unione di cui all'Allegato II, e (ii) altri sistemi di IA che rispondono alle categorie o ai casi di uso di cui all'Allegato III. Tuttavia, nel testo approvato dal Parlamento, ai fini della qualificazione dei sistemi di IA come sistemi ad alto rischio, non è più sufficiente, per questa seconda categoria, la loro sussumibilità in una delle categorie o casi di uso previsti dall'apposito allegato, in quanto, in aggiunta a ciò, è necessario che venga riscontrato anche in concreto un "rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche", e, per la categoria dei sistemi di IA nel settore della gestione e del funzionamento di infrastrutture critiche, "un rischio significativo di danno per l'ambiente". In proposito, si prevede che entro 6 mesi prima dall'entrata in vigore del regolamento (l'*AI Act*) la Commissione emani delle linee guida intese a "specificare chiaramente le circostanze in cui l'*output* dei sistemi di IA di cui all'Allegato III comporterebbe un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche e i casi in cui non lo farebbe".

- Lo stesso elenco delle categorie e casi di uso dei sistemi di IA contenuto nell'Allegato III è stato significativamente modificato ed ampliato. Tra le altre modifiche ed integrazioni, si segnala:
  - l'inclusione dei sistemi di riconoscimento delle emozioni e, più generalmente, dei sistemi di IA "destinati a essere utilizzati per trarre conclusioni sulle caratteristiche personali delle persone fisiche sulla base di dati biometrici o basati su elementi biometrici";
  - l'ampliamento delle tipologie di sistemi di IA nel settore dell'istruzione e della formazione professionale;
  - l'eliminazione della previsione dei sistemi di IA, ora assoggettati al regime del divieto dell'art. 5, destinati a essere utilizzati dalle autorità di contrasto per effettuare valutazioni individuali dei rischi delle persone fisiche al fine di determinare il rischio di reato o recidiva;
  - l'ampliamento delle tipologie di sistemi di IA nel settore della gestione della migrazione, dell'asilo e del controllo delle frontiere;
  - l'inclusione dei sistemi di IA di *marketing* politico;
  - l'inclusione dei sistemi di IA destinati a essere utilizzati dalle piattaforme di *social media* che sono state designate come piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33 del regolamento (UE) 2022/2065 (c.d. VLOPs [su cui v. notizia successiva in questa rubrica]), per quanto concerne i loro sistemi di raccomandazione usati per raccomandare al destinatario del servizio i contenuti generati dagli utenti disponibili sulla piattaforma.
- Il testo approvato dal Parlamento ha rafforzato le competenze delle autorità nazionali e prevede l'istituzione di un Ufficio per l'IA, come nuovo organo per supportare l'applicazione armonizzata dell'*AI Act*, offrire orientamenti e coordinare le indagini *cross-border*.

SALVATORE ORLANDO

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.pdf

https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_IT.html

https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

2023/2(5)RA

La decisione della Commissione europea del 25.4.2023 per la designazione del primo gruppo di piattaforme e motori di ricerca online "*very large*": VLOPs e VLOSEs

Il 25 aprile 2023, la Commissione europea ha adottato la prima decisione *ex* art. 33(4) del regolamento (UE) 2022/2065 (c.d. *Digital Services Act* o **DSA**), con la quale ha individuato e designato taluni soggetti quali "*piattaforme online di dimensioni molto grandi e motori di ricerca online di dimensioni molto grandi*", in quanto aventi "*un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni*" ex art. 33(1) DSA.
In particolare, la Commissione ha identificato quali "*piattaforme online di dimensioni molto grandi*" (**VLOPs**) i seguenti soggetti: Alibaba AliExpress; Amazon Store; Apple AppStore; Booking.com; Facebook; Google Play; Google Maps; Google Shopping; Instagram; LinkedIn; Pinterest;

Snapchat; TikTok; Twitter; Wikipedia; YouTube; Zalando.

Quali "*motori di ricerca online di dimensioni molto grandi*" (**VLOSEs**) sono stati, invece, individuati i soli Bing e Google Search.

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

- tali soggetti "*individuano, analizzano e valutano con diligenza gli eventuali rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei suoi relativi sistemi, compresi i sistemi algoritmici, o dall'uso dei loro servizi*", con tale valutazione del rischio che "*deve essere specifica per i loro servizi e proporzionata ai rischi sistemici, tenendo in considerazione la loro gravità e la loro probabilità, e deve comprendere i seguenti rischi sistemici: a) la diffusione di contenuti illegali tramite i loro servizi; b) eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali* […]*; c) eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica; d) qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona*" (art. 34(1) del DSA);
- una volta individuati i rischi sistemici ai sensi dell'art. 34 DSA, i "*fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi adottano misure di attenuazione ragionevoli, proporzionate ed efficaci* [di tali rischi], *prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali*", potendo prevedere – tra l'altro – a tal fine "*l'adeguamento della progettazione, delle caratteristiche o del funzionamento dei loro servizi, anche delle loro interfacce online*", "*l'adeguamento delle condizioni generali e la loro applicazione*", "*l'adeguamento delle procedure di moderazione dei contenuti*", "*la sperimentazione e l'adeguamento dei loro sistemi algoritmici, compresi i loro sistemi di raccomandazione*", "*l'adeguamento dei loro sistemi di pubblicità e l'adozione di misure mirate volte a limitare o ad adeguare la presentazione della pubblicità associata al servizio da esse prestato*", "*il rafforzamento dei processi interni, delle risorse, della sperimentazione, della documentazione o della vigilanza sulle loro attività*", "*l'adozione di misure di sensibilizzazione e l'adattamento della loro interfaccia online al fine di dare ai destinatari del servizio maggiori informazioni*" e "*l'adozione di misure mirate per tutelare i diritti dei minori*" (art. 35(1) DSA);
- in caso di crisi - e ciò, stando all'art. 36(2) DSA, nell'ipotesi in cui si verificano "*circostanze eccezionali* [che] *comportano una grave minaccia per la sicurezza pubblica o la salute pubblica nell'Unione o in parti significative della stessa*"- la "*Commissione, su raccomandazione del comitato, può adottare una decisione che impone a uno o più fornitori di piattaforme online di dimensioni molto grandi o di motori di ricerca online di dimensioni molto grandi di intraprendere una o più delle seguenti azioni: a) la valutazione sull'eventualità e, in caso affermativo, sulla relativa portata e sul modo in cui il funzionamento e l'uso dei loro servizi contribuiscano, o possano contribuire, in maniera significativa a una minaccia grave di cui al paragrafo 2; b) l'individuazione e l'applicazione di misure specifiche, efficaci e proporzionate, quali quelle di cui all'articolo 35, paragrafo 1, o all'articolo 48, paragrafo 2, per prevenire, eliminare o limitare tale contributo alla grave minaccia individuata a norma della lettera a) del presente paragrafo; c) una relazione alla Commissione, entro una certa data o a intervalli regolari specificati nella decisione, in merito alle valutazioni di cui alla lettera a), sul contenuto preciso, l'attuazione e l'impatto qualitativo e quantitativo delle misure specifiche adottate a norma della lettera b) e su qualsiasi altra questione connessa a tali valutazioni o misure, come specificato nella decisione*" (art. 36(1) DSA);
- essi siano sottoposti "*a proprie spese e almeno una volta all'anno, a revisioni indipendenti volti a valutare la conformità: a) agli obblighi stabiliti al Capo III; b) agli impegni assunti a norma dei codici di condotta di cui agli articoli 45 e 46 e dei protocolli di crisi di cui all'articolo 48*" (art. 37(1) DSA); tali revisioni devono

essere effettuate da organizzazioni "*indipendenti e in assenza di conflitti di interessi*", "*dotate di comprovata esperienza nel settore della gestione dei rischi, di competenze e di capacità tecniche*" e di "*comprovata obiettività e deontologia professionale*" (art. 37(3) DSA). Ove la revisione risulti non positiva, i fornitori di VLOPs e VLOSEs "*tengono debitamente conto delle raccomandazioni operative ad essi rivolte al fine di adottare le misure necessarie per attuarle*" (art. 37(6) DSA);

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

Entro 4 mesi dalla notifica della decisione di designazione, le piattaforme e i motori di ricerca così individuati sono tenuti ad adeguare i propri sistemi, risorse e processi alle disposizioni poc'anzi illustrate, al fine di garantire la conformità al regolamento.

Tale nuova architettura di queste piattaforme *online* dovrebbe così garantire maggiore consapevolezza e potere di decisione agli utenti con riguardo ai propri diritti, una migliore protezione dei minori e degli altri soggetti particolarmente vulnerabili, una minor diffusione della disinformazione (oltre a una mediazione dei contenuti *online* più diligente), nonché una maggiore trasparenza dei servizi offerti sul *web*.

RICCARDO ALFONSI

https://ec.europa.eu/commission/presscorner/detail/it/IP_23_2413

2023/2(6)RA

La contestazione di Zalando alla sua designazione quale VLOP

Il 27 giugno 2023, Zalando ha contestato dinnanzi alla Corte di Giustizia dell'Unione Europea la designazione della propria piattaforma quale "*piattaforma online di dimensioni molto grandi*" (VLOP) [su cui v. la notizia precedente].
Segnatamente, Zalando ha sostenuto che la Commissione europea – nell'effettuare tale designazione – non avrebbe correttamente tenuto conto della natura precipuamente *retail* del *business model* della società, natura che non implicherebbe alcun "*rischio sistemico*" di diffusione, da parte di terzi, di contenuti dannosi per gli utenti o comunque illegali. Al contrario, la società destinataria del provvedimento della Commissione ha ribadito che essa offre ai propri clienti un ambiente *online* sicuro, con prodotti altamente curati, offerti da società *leader* del settore, accuratamente controllate prima di essere selezionate.
Ancora, Zalando ha sostenuto l'erroneità della designazione effettuata dalla Commissione, in virtù del fatto che la media mensile dei destinatari attivi del servizio offerto dalla società sarebbe pari a circa 31 milioni, e quindi una cifra di gran lunga inferiore rispetto a quella – di 45 milioni di utenti al mese – postulata dall'art. 34(1) DSA al fine della individuazione di una VLOP.
Infine, in ogni caso, Zalando ha denunciato una presunta disparità di trattamento lamentando in proposito l'assenza di una metodologia chiara e coerente utilizzata dalla Commissione al fine di valutare se una società rientri o meno nella categoria di "*piattaforma online di dimensioni molto grandi*" per l'applicazione della Sezione 5 del Capo III del DSA.

RICCARDO ALFONSI

https://www.just-style.com/news/german-fashion-retailer-zalando-sues-eu-over-landmark-digital-services-act/

2023/2(7)GDI

La sentenza del Tribunale della CGUE del 26.4.2023 nella causa T-557/20 sulla nozione di dato personale

Il 26 aprile 2023 il Tribunale della Corte di Giustizia dell'Unione Europea, nella causa T-557/20, ha annullato la decisione del Garante europeo della protezione dei dati (**GEPD**) del 24 novembre 2020 con la quale quest'ultimo aveva dichiarato che il Comitato di Risoluzione Unico (l'autorità di risoluzione delle crisi dell'Unione bancaria europea, di seguito: **CRU**) aveva violato l'art. 15 del regolamento (UE) 2018/1725 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni dell'Unione e sulla libera circolazione di tali dati, in quanto non aveva informato i reclamanti della possibilità che i loro dati personali fossero comunicati ad una società di consulenza del gruppo Deloitte (**Deloitte**).
Sebbene la sentenza sia espressamente rivolta all'interpretazione del regolamento (UE) 2018/1725, le indicazioni in essa contenute possono essere estese al regolamento (UE) 2016/679 (il GDPR) per sostanziale omogeneità delle nozioni contenute nei due testi normativi. *A fortiori*, lo stesso Tribunale, nelle sue argomentazioni, richiama l'interpretazione che la Corte di Giustizia ha dato alla nozione di dato personale ai sensi della direttiva 95/46/CE.
Nell'ambito di un processo di indennizzo conseguente alla risoluzione di un ente creditizio spagnolo, il CRU si era avvalso di Deloitte per alcune elaborazioni sulla documentazione presentata da azionisti e creditori. A tal fine, il CRU ha trasferito a Deloitte alcune informazioni contraddistinte da un codice alfanumerico.
Successivamente, alcuni azionisti e creditori hanno inviato al GEPD cinque reclami sostenendo che il CRU non li aveva informati che i loro dati sarebbero stati trasmessi a terzi, tra cui Deloitte.
All'esito della sua istruttoria, nel ritenere che i dati trasmessi a Deloitte fossero dati pesudonimizzati e, in quanto tali "dati personali" *ex* art. 3, punto 1, del regolamento 2018/1725, il GEPD ha rilevato la violazione dell'obbligo di informazione previsto dall'art. 15, par. 1, lett. d), del medesimo regolamento.
Nel contestare tale pronuncia, il CRU ricorre al Tribunale ai sensi dell'art. 263 TFUE contestando la natura di dati personali delle informazioni inviate a Deloitte e chiedendo l'annullamento della decisione del GEPD. Sosteneva il CRU che le informazioni trasmesse a Deloitte non costituivano dati personali in quanto: le informazioni trasmesse erano indipendenti dalle persone dei reclamanti e non connesse alla loro vita privata; la comunicazione del codice alfanumerico non ha portato a pseudonimizzare i dati che, invece, sarebbero anonimi in quanto il CRU non avrebbe condiviso le informazioni che consentivano di reidentificare gli autori delle osservazioni. In altre parole, il solo codice alfanumerico non consentirebbe a Deloitte di reidentificare le persone.

Di contro, alla base della decisione del GEPD vi era la constatazione che: le osservazioni degli interessati sono informazioni che di per sè li "concernono"; il fatto che Deloitte non abbia avuto accesso alle ulteriori informazioni detenute dal CRU non comporta che i dati pseudonimizzati siano divenuti anonimi e, a prescindere se fosse "ragionevolmente" probabile la reidentificazione degli interessati e in considerazione del fatto che la nozione di dato personale considera identificabile la persona anche "indirettamente", conclude che i dati pseudonimizzati rimarrebbero tali anche quando vengono trasmessi a terzi.

Nel risolvere la questione, la sentenza del Tribunale acquisisce interesse per le valutazioni sulla nozione di "dato personale" e per l'accertamento in concreto che l'interprete deve porre per verificarne i requisiti. Rileva il Tribunale, infatti, che per aversi dati personali l'informazione deve essere «concern[ente]» una persona fisica che, tramite questa, sarà «identificata o identificabile».

Nel premettere che la nozione di dato personale è interpretata in senso estensivo (v. Sentenza 20 dicembre 2017, Nowak, punto 34) e comprende ogni tipo di informazione purché "concernente" la persona interessata, il Tribunale rileva che l'informazione integra un dato personale quando «in ragione del suo contenuto, della sua finalità o del suo effetto, l'informazione era connessa a una determinata persona» (§69).

L'accertamento di tali condizioni non può però essere presunto, sicché: «Certamente, non si può escludere che punti di vista personali o opinioni costituiscano dati personali. Tuttavia, […] tale conclusione non può basarsi su una presunzione […] ma deve basarsi su un esame volto ad accertare se, per il suo contenuto, scopo o effetto, un punto di vista sia collegato a una persona specifica. Ne consegue che, non avendo effettuato un siffatto esame, il GEPD non poteva concludere che le informazioni trasmesse a Deloitte costituissero un'informazione "concernente" una persona fisica» (§§ 73-74).

Con riferimento al rapporto tra dati pseudonimizzati (e quindi "personali") e anonimizzati (quindi esclusi dall'ambito di applicazione della normativa), nel rilevare che le informazioni trasmesse a Deloitte non riguardavano persone "identificate", il Tribunale esamina se le informazioni in possesso di Deloitte concernessero una persona fisica "identificabile".

A tal fine, il Tribunale fa riferimento alla sentenza "Breyer" della Corte di Giustizia del 19 ottobre 2016 sulla possibilità di un "indirizzo IP" di essere qualificato come informazione riferita a una «persona fisica identificabile», tenendo conto, da un lato, del fatto che esso non offre, di per sé, la possibilità di identificare l'utente e, dall'altro, che altre informazioni aggiuntive, se combinate con tale indirizzo IP, avrebbero consentito di identificare detto utente.

Affinché un dato possa essere qualificato come "personale" non è necessario che tutte le informazioni utili siano in possesso di una sola persona e, quindi, il fatto che le informazioni aggiuntive necessarie per identificare l'utente siano in mano a un altro soggetto non è idoneo a escludere che gli indirizzi IP possano essere dati personali. Tuttavia occorre determinare la ragionevole possibilità di combinare un indirizzo IP con le informazioni aggiuntive detenute da altro soggetto. Tale situazione non si verifica laddove l'identificazione della persona sia vietata dalla legge o praticamente irrealizzabile, per esempio a causa del fatto che implicherebbe un dispendio di tempo, di costo e di manodopera, facendo così apparire insignificante il rischio di identificazione.

Sicché, conclude il Tribunale: «il fatto che le informazioni aggiuntive […] non fossero in possesso di Deloitte, bensì del CRU, non è idoneo a escludere a priori che le informazioni trasmesse a Deloitte costituissero dati personali per quest'ultima. Tuttavia, […] per stabilire se le informazioni trasmesse a Deloitte costituissero dati personali, occorre porsi dal punto di vista di quest'ultima per determinare se le informazioni che le sono state trasmesse si riferiscano a "persone identificabili"» (§§ 96-97).

Tale accertamento doveva essere effettuato dal GEPD che si è limitato ad esaminare la possibilità di reidentificare gli interessati dal punto di vista del CRU e non di Deloitte.

Secondo il Tribunale: «incombeva al GEPD stabilire se la possibilità di combinare le informazioni fornite a Deloitte con le informazioni aggiuntive in possesso del CRU costituisse un mezzo che poteva essere ragionevolmente attuato da Deloitte per identificare gli autori delle osservazioni. Pertanto, poiché il GEPD non ha verificato se Deloitte disponeva di mezzi legali e realizzabili in pratica che le consentissero di accedere alle informazioni aggiuntive necessarie per la reidentificazione degli autori delle osservazioni, il GEPD non poteva concludere che le informazioni trasmesse a Deloitte costituissero informazioni concernenti una "persona fisica identificabile"» (§§ 104-105).

In conclusione: la valutazione del fatto che i dati "concernano" una persona fisica deve essere svolta in concreto e non presunta; l'analisi del rischio di

reidentificazione dell'interessato deve essere svolta in concreto e dal punto di vista del destinatario dei dati.
Il Tribunale ha dunque annullato la decisione del GEPD non perché le informazioni trasmesse a Deloitte fossero dati anonimizzati piuttosto che pseudonimizzati ma perché il GEPD non ha accertato che le informazioni fornite a un destinatario dei dati fossero informazioni "concernenti" una persona fisica e che la rendessero "identificabile".

GUIDO D'IPPOLITO

https://curia.europa.eu/juris/document/document.jsf?text=&docid=272910&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4409733

2023/2(8)CR

Lo standard ISO 31700-1:2023 sul privacy by design dei prodotti e servizi di consumo

Il 31 gennaio 2023 l'*International Organization for Standardization* ("**ISO**") ha adottato il nuovo standard ISO 31700 che delinea il principio di *privacy by design* nel trattamento dei dati personali collegato alla gestione di un prodotto o servizio di consumo. Lo standard si compone di due parti: una lista di 27 requisiti operativi (31700-1) e 3 casi pratici che mostrano come svolgere un adeguamento ai nuovi processi introdotti (31700-2).
Lo standard riprende il concetto di *privacy by design* ("**PbD**") introdotto negli anni '90 da Anna Cavoukian, Commissario per l'informazione e la privacy dell'Ontario, e poi ripreso anche dall'art. 25 del GDPR secondo cui i titolari del trattamento devono garantire che "*per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".
Lo standard ISO 31700 si ricollega alla previsione del GDPR (da cui riprende anche la definizione di "dato personale"), e la va ad integrare specificando i requisiti necessari per la corretta applicazione della PbD e fornendo dei casi d'uso per aiutare i titolari del trattamento nella effettiva implementazione di questo principio. Rispetto al GDPR, lo standard ISO si concentra però più sull'aspetto commerciale della PbD che sul piano della tutela dei diritti fondamentali, come confermato dal fatto che non parla di "interessato" ma di "consumatore finale".
In ogni caso, il rispetto dello standard ISO 31700 non costituisce un requisito legale e non garantisce di per sé la *compliance* con le previsioni del GDPR. Si tratta di una certificazione disponibile sul mercato di cui gli operatori possono avvalersi per dimostrare di fronte ai consumatori e alle autorità di controllo il loro impegno nell'adottare misure di protezione dei dati personali al fine di ottenere la fiducia dei consumatori e guadagnare una posizione di vantaggio competitivo rispetto alle aziende concorrenti.
Ai sensi dello standard, come si legge nell'introduzione, il concetto di *privacy by design* può essere applicato a prodotti, processi, sistemi e software e consiste nel garantire che le impostazioni di *default* siano orientate alla tutela del consumatore, in modo da assicurare già un elevato livello di protezione dei dati personali senza che il consumatore debba farsi carico di intervenire per ottenere tale protezione.
Questo risultato può essere raggiunto attraverso una pluralità di metodologie che afferiscono al design e allo sviluppo del prodotto/servizio considerandone l'intero ciclo di vita, dalla fase di creazione all'acquisto e all'utilizzo da parte dei consumatori, fino alla fine del ciclo di vita.
Uno dei pilastri su cui si fonda lo standard 31700 riguarda i requisiti di comunicazione con i consumatori al fine di garantire la trasparenza sul trattamento dei dati personali così da facilitare un processo decisionale sicuro e informato sia prima dell'acquisto che durante il successivo utilizzo del prodotto/servizio. In quest'ottica vengono menzionate una serie di modalità attraverso cui è possibile comunicare al consumatore in modo trasparente, tra cui ad esempio interfacce, pagine di istruzioni e documenti sul prodotto, sezioni F.A.Q., pagine di avvisi ai consumatori, servizi di assistenza, ecc.
Altro pilastro è quello della gestione del rischio che in parte riprende i requisiti dell'art. 32 GDPR in tema di sicurezza del trattamento, dell'art. 35 in tema di valutazione d'impatto e dell'art. 28 sulla gestione dei rapporti con i responsabili del trattamento. Le attività di *risk management* devono quindi essere volte a valutare, prevenire, mitigare e trasferire i rischi, considerando le conseguenze dell'esposizione dei consumatori al prodotto/servizio.
Infine, gli ultimi due capitoli dello standard riguardano i requisiti di sviluppo, implementazione e gestione dei controlli sulla privacy (per tali intendendosi l'insieme delle azioni, misure e contromisure che consentono di mitigare i rischi per la privacy) e i requisiti per la fine del ciclo di vita del prodotto/servizio, posto che per anche questa fase può avere importanti impatti sulla privacy dei consumatori.

CHIARA RAUCCIO

https://www.iso.org/obp/ui/#iso:std:iso:31700:-1:ed-1:v1:en

2023/2(9)FP

Il report finale dell'Autorità antitrust tedesca sull'indagine di settore sull'online advertising

A distanza di circa un anno dalla pubblicazione dell'indagine di settore sull'*online advertising* (29 agosto 2022), l'Autorità *antitrust* tedesca (Bundeskartellamt, **BKartA**) ha diffuso un report che raccoglie e analizza criticamente i commenti ricevuti dai principali stakeholders in esito alla consultazione pubblica (30 maggio 2023).

L'indagine e il report finale sono accessibili esclusivamente in lingua tedesca sulla pagina web del BKartA, dove è però disponibile un *executive summary* dell'indagine in lingua inglese.

L'indagine nasce con l'obiettivo di mappare un settore che, nel corso dell'ultimo ventennio, ha conosciuto una crescita esponenziale, tanto da sovrastare oggi, per volume e valore degli scambi, le forme tradizionali di *advertising* a mezzo stampa o telecomunicazioni.

Il *report* mira a fornire una ricostruzione delle diverse tecniche impiegate dai processi di *online advertising* e a identificare i principali attori coinvolti, al fine di addivenire a una possibile delimitazione del mercato di riferimento e delle problematiche sottese alla sua distribuzione. Il *focus* dell'analisi, data l'area di competenza del BKartA, è relativo al livello di competitività del settore, in particolar modo rispetto ai rischi posti dalla concentrazione dei processi di scambio in mano a pochi *players* con posizione di assoluto predominio.

Attraverso la pubblicazione del *report*, l'intenzione del BKartA non è tuttavia quella di anticipare giudizi in ordine ad asserite violazioni delle regole *antitrust* – eventualmente rimesse a futuri procedimenti individuali – quanto piuttosto di suggerire la necessità di un'analisi più ampia e approfondita, specialmente alla luce dell'oramai prossima introduzione di una cornice regolatoria di riferimento.

Dopo un'iniziale approccio votato al "*laissez faire*", lo scenario futuro sembra difatti destinato a mutare radicalmente in conseguenza dell'imminente entrata in vigore di nuove legislazioni che intercettano il fenomeno dell'*online advertising*: tanto a livello nazionale (*in primis*, il nuovo § 19a della legge tedesca sulle restrizioni alla concorrenza, il **GWB**, che stabilisce nuovi poteri del BKartA in caso di condotte abusive di imprese con importanza significativa su diversi mercati), quanto euro-unitario, su tutte, il *Digital Markets Act*, **DMA** e il *Digital Services Act*, **DSA** [su cui v. le notizie, rispettivamente sub 1 e sub 2 del numero 4/2022 in questa rubrica: http://www.personaemercato.it/wp-content/uploads/2023/01/Osservatorio.pdf].

A livello definitorio, il *report* muove da una generale distinzione fra advertising «*search-based*» e «*non-search-based*», a seconda che il contenuto proposto all'utente sia basato prevalentemente sulla sua *query* di ricerca, ovvero su altre informazioni relative al singolo profilo utente (cui l'*advertiser* ha avuto accesso attraverso *tracking* o scambio di dati) o al contesto nel quale è inserito il *banner* pubblicitario. Nonostante alcuni commenti al *report* suggeriscano una certa sovrapponibilità fra queste tipologie, solo la seconda è presa di fatto in considerazione nell'indagine, dando essa più facilmente luogo a problemi di asimmetria informativa e di opacità dei processi di acquisizione e trattamento dati.

La variante di *non-search advertising* su cui il report si sofferma più in dettaglio è quella del «*programmatic advertising*» (**PA**). In sintesi, la vendita di uno spazio pubblicitario online secondo questo meccanismo avviene in via totalmente automatizzata, attraverso la sua pubblicazione da parte di un «*Publisher-AdServer*» su una o più «*Supply Side Platforms*» (**SSPs**), unitamente alle condizioni base d'offerta, quali un prezzo minimo o un contenuto compatibile con lo spazio dove compare il banner.

Lo spazio messo in vendita sulle SSPs diviene così oggetto di un'asta in tempo reale («*Real Time Bidding*», **RTB**) – di regola, al momento in cui l'utente accede al sito web o all'applicazione che ospita lo spazio pubblicitario – diretta a selezionare la miglior offerta presentata dai vari «*advertisers*» su «*Demand Side Platforms*» (**DSPs**); in questa fase, le DSPs hanno di regola accesso a una serie di informazioni critiche sul profilo individuale dell'utente o sulle caratteristiche dello spazio pubblicitario, al fine di aggiustare le singole offerte e individuare quella al maggior prezzo. L'identificativo dell'*advertiser* che si è aggiudicato l'offerta viene infine comunicato dalla SSP al *publisher*, il quale provvede all'inserimento dello specifico contenuto pubblicitario all'interno del *banner*.

Sebbene SSPs e DSPs siano concettualmente distinti, la consultazione mette in luce la circostanza per cui questo riparto di competenze risulta nella prassi molto più sfumato, giacché i più importanti DSPs appartengono a SSPs che sono al contempo

publishers, evidenziando così potenziali conflitti di interesse [sulla decisione del 2 febbraio 2022 del Garante privacy belga sul *Real Time Bidding* e le attività di online advertising a proposito del Quadro di Trasparenza e Consenso elaborato e gestito da IAB Europe –v. in questa rubrica la notizia n. 11 del numero 1/2022: http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf]. Un ruolo chiave nel processo di *online advertising* mediante PA è svolto da intermediari che si occupano di raggruppare spazi messi a disposizione dei publishers offrendoli poi ai diversi acquirenti attraverso un singolo punto di contatto. L'opera di intermediazione si accompagna, di regola, alla prestazione di servizi ulteriori a favore degli *advertisers*, quali il *targeting* degli utenti, la prevenzione di frodi e il monitoraggio della visibilità degli annunci pubblicitari («*ad verification*»).

L'attuale geografia del mercato mostra un elevatissimo grado di concentrazione per volume di vendite e guadagni in mano a Google (Alphabet), tanto in qualità di *publisher* di *ad services* (tra l'80 e il 100% del mercato), quanto di venditore di spazi di terze parti.

L'indagine si limita alla mappatura del mercato tedesco ma, secondo il BKartA, tali risultati restituiscono una tendenza del tutto uniforme fra le diverse aree geografiche del mercato europeo. Le ragioni della larga maggioranza di preferenze degli *advertisers* per i servizi di Google si legano principalmente al controllo, da parte di quest'ultima, del più ampio *database* di informazioni sugli utenti, tale da consentire una maggior granularità dell'offerta pubblicitaria loro destinata.

Allo stesso tempo, la consultazione ha reso noti i problemi di opacità che caratterizzano la prestazione dei servizi di Google, su tutti, la comunicazione ai *publishers* del solo dato relativo all'ammontare di offerte che hanno avuto successo, non anche di quelle non riuscite.

A parere del BKartA, della soluzione di questo problema dovrà farsi carico l'art. 5, parr. 9-10 DMA, il quale assegna al «*gatekeeper*» obblighi più penetranti di informazione a *advertisers* (inserzionisti) e *publishers* (editori) su base giornaliera e senza oneri aggiuntivi. L'assoluta preminenza del ruolo dei dati nell'infrastruttura dell'*online advertising* induce il BKartA a soffermarsi con particolare attenzione sulle ripercussioni che potranno verosimilmente prodursi in esito al processo in atto di restrizione nell'accesso ai dati personali. L'incremento di consapevolezza da parte della generalità degli utenti nel valore dei dati personali, unitamente all'introduzione di vincoli normativi alla loro acquisizione e trattamento impone difatti di valutare come il mercato possa reagire all'inversione di tendenza rispetto a modelli, finora prevalenti, di business «*data-intensive*».

A titolo esemplificativo, il report sottolinea le problematiche che possono affliggere il metodo di *tracking* ad oggi più diffuso, quello che si affida ai «*third party cookies*», in varia misura oggetto di limitazione da parte della Direttiva e-Privacy e del GDPR. La funzione principale del dato in questo settore è quella di evitare perdite imputabili all'effetto dispersione, in ragione della non coerenza fra il contenuto pubblicizzato, da un lato, e il profilo dell'utente, ovvero la sede dello spazio pubblicitario, dall'altro. La consultazione ha però evidenziato che, oltre al «*content targeting*», l'accesso ai dati riveste altre fondamentali funzioni, quali la misurazione del successo della campagna pubblicitaria e l'identificazione e prevenzione di comportamenti abusivi. In ragione di ciò, è stato suggerito dai partecipanti alla consultazione di distinguere fra «*user data*» e «*usage data*», per differenziare fra loro le caratteristiche dei dati necessari all'espletamento delle diverse funzioni.

Dal momento che diversi modelli di *business* fondano il principale canale di finanziamento nei meccanismi di *online advertising* e si basano sull'acquisizione dei dati, numerosi partecipanti alla discussione (in particolare, dal lato dei *publishers*) avversano l'introduzione di ulteriori restrizioni nell'accesso ai dati. Pur senza prendere posizione a riguardo, il report invita a considerare i possibili effetti derivanti dalle suddette restrizioni e, segnatamente, se *i*) queste ultime contribuiscano a diminuire il livello di diversificazione del settore e la sua competitività (a discapito dell'offerta agli utenti finali) e *ii*) possano altresì produrre effetti asimmetrici a vantaggio dei grandi *players* di mercato. Sul primo punto, la BKartA suggerisce di verificare la fattibilità di percorsi alternativi di sostenibilità di *business model* che fanno oggi eccessivo affidamento sul canale dell'*online advertising*, nell'ottica di rinunciare o di fare più limitato uso dei dati, anche in considerazione del fatto che l'obiettivo è quello per cui tutti gli operatori di mercato abbandonino progressivamente le strategie «*data-intensive*».

Allo stesso tempo, il *report* sottolinea che misure restrittive indiscriminate possano comunque produrre effetti asimmetrici sul mercato, dal momento che gli operatori attivi su larghi ecosistemi (come Alphabet) potranno comunque continuare ad avere accesso ai dati grazie all'ampio portafogli di servizi e ai «*first-party data*», laddove

altri attori perderebbero invece ogni possibilità di usufruirne.
L'elevata concentrazione del mercato, specie nel settore del *non-search online advertising*, impone dunque di considerare l'effettività di misure su base individuale, dirette a correggere le pratiche dell'operatore che occupa la fetta di mercato più ampia. A tal proposito, nel dicembre 2022, facendo uso dei poteri assegnati dal § 19 GWB, il BKartA ha informato Alphabet della necessità di effettuare modifiche alle proprie condizioni di trattamento dati, al fine di assicurare la scelta dei suoi utenti di consentire o meno al loro trattamento fra servizi differenti. Tuttavia, secondo l'Autorità tedesca, le misure su base individuale non sarebbero sufficienti a risolvere problematiche più radicali – come quelle dell'opacità e del conflitto di interessi – che richiederebbero riforme strutturali e su più larga scala.
Come monito conclusivo il report suggerisce però che considerazioni legate a possibili effetti anticoncorrenziali della restrizione all'accesso e al trattamento dati debbano venir bilanciate con l'esigenza di tutela del diritto all'autodeterminazione degli utenti, specie in considerazione del carattere sensibile di alcuni dati processati dai sistemi di *online advertising*.
Pur priva di valenza immediatamente precettiva sul versante dell'accertamento di condotte anticoncorrenziali, l'indagine del BKartA mira a fornire una base per futuri approfondimenti su un settore in rapidissimo sviluppo e per una discussione sulle misure di *policy* dirette a regolare il mercato della circolazione dei dati.

FEDERICO PISTELLI

Indagine sull'online advertising (lingua tedesca)
https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Online_Werbung_Diskussionsbericht_lang.html?nn=3599398
Executive summary on Sector Inquiry – Online Advertising (lingua inglese)
https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Sector%20Inquiries/Sektor_inquiry_online_advertising_report_discussion_summary.pdf?__blob=publicationFile&v=4
Report finale (lingua tedesca)
https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_Online_Werbung_Abschlussbericht.html?nn=3599398

2023/2(10)IG

Il parere del "Chirurgo Generale" degli USA del 23 maggio 2023 sulla salute mentale dei giovani e i social media

Il 23 maggio 2023 il *Surgeon General*, capo dell'Ufficio per la Salute Pubblica per gli Stati Uniti, con un documento intitolato "*Social Media and Youth Mental Health*", dopo aver riconosciuto gli indiscussi vantaggi connessi all'uso dei *social media*, ha richiamato l'attenzione dei cittadini americani sui rischi legati ad un uso eccessivo e problematico degli stessi e al relativo impatto sulla salute mentale dei minori. Nel parere si riportano gli esiti di studi ed esperimenti condotti su giovani universitari, dai quali è emersa una significativa correlazione fra l'uso dei social media e l'insorgenza (o aggravamento) della depressione e dell'ansia e inoltre come la limitazione del tempo di utilizzo degli stessi abbia portato ad una importante riduzione di tali fenomeni. Nel rapporto viene quindi spiegato come tali effetti siano ancora più evidenti negli adolescenti, di età compresa tra i 10 e i 19 anni, i quali stanno attraversando un periodo molto delicato dello sviluppo cerebrale, nel quale i comportamenti a rischio raggiungono il loro apice, il benessere subisce le maggiori fluttuazioni ed emergono problemi di salute mentale, come la depressione e l'ansia. Inoltre, all'inizio dell'adolescenza, quando si stanno formando l'identità e il senso di autostima, lo sviluppo cerebrale è particolarmente suscettibile alle pressioni sociali, alle opinioni dei coetanei e al confronto con gli altri. I social media possono anche perpetuare l'insoddisfazione del corpo, i comportamenti alimentari disordinati, il confronto sociale e la bassa autostima, specialmente tra le ragazze adolescenti. Il report sottolinea come l'influenza dei social media sulla salute mentale dei giovani sia determinata da diversi fattori, tra cui la quantità di tempo che i bambini e gli adolescenti trascorrono sulle piattaforme, il tipo di contenuti che consumano o a cui sono esposti in altro modo, le attività e le interazioni che i social media consentono e il grado di interruzione delle attività essenziali per la salute, quali il sonno e attività fisica. Inoltre bambini e adolescenti sono influenzati dai social media in modi diversi, in base ai loro punti di forza e di vulnerabilità individuali, nonché in base a fattori culturali, storici e socio-economici.
Nel parere si afferma che, dato il crescente numero di ricerche sui potenziali danni correlati all'uso dei social media, benché siano necessarie ulteriori ricerche per comprenderne pienamente l'impatto

sugli adolescenti, si debba agire con urgenza per creare ambienti digitali sicuri e salutari che riducano al minimo i danni e salvaguardino la salute mentale e il benessere di bambini e adolescenti durante le fasi critiche del loro sviluppo.

Per questo il *Surgeon General* rivolge un invito ai legislatori, alle aziende tecnologiche, alla comunità scientifica, alle famiglie e agli stessi giovani affinché si attivino con misure, precauzioni, azioni e iniziative in grado di ridurre i rischi, massimizzare i benefici e salvaguardare la salute mentale e il benessere dei minori.

In particolare ai responsabili politici raccomanda di adottare misure per rafforzare gli standard di sicurezza e limitare l'accesso in modo da rendere i social media più sicuri per i bambini di tutte le età, proteggere meglio la loro privacy, sostenere l'alfabetizzazione digitale e mediatica, nonché finanziare ulteriori ricerche; alle aziende tecnologiche, in particolare alle piattaforme digitali, di valutare in modo migliore e più trasparente l'impatto dei loro prodotti sui bambini, condividere i dati con ricercatori indipendenti per aumentare la comprensione collettiva degli impatti, prendere decisioni di progettazione e sviluppo che diano priorità alla sicurezza e alla salute, compresa la protezione della privacy dei minori, nonché migliorare i sistemi per fornire risposte efficaci e tempestive ai reclami; alle famiglie e agli assistenti sociali di monitorare e di educare al corretto utilizzo dei social media da parte dei minori, nonché di prendere provvedimenti all'interno delle loro famiglie, ad esempio istituendo zone libere dalla tecnologia che aiutino a proteggere il sonno e a favorire meglio le relazioni interpersonali; ai giovani raccomanda di limitare il tempo di permanenza sulle piattaforme, di bloccare i contenuti indesiderati e di fare attenzione a condividere informazioni personali. Ai ricercatori, infine, richiede un maggiore impegno nell'approfondire e nel chiarire l'impatto delle nuove tecnologie sulle persone minori di età, nel definirne gli standard di utilizzo e nel valutare le migliori pratiche per sostenere la salute dei minori, migliorando il coordinamento e la collaborazione nella ricerca anche al fine di diffonderne i risultati.

ILARIA GARACI

https://www.hhs.gov/surgeongeneral/priorities/youth-mental-health/social-media/index.html

https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

2023/2(11)LV

La denuncia del 31.5.2023 dalla Federal Trade Commission degli USA contro Amazon per l'assistente vocale 'Alexa' in relazione alle normative a protezione dei minori e dei consumatori

Il 31 maggio 2023 la *Federal Trade Commission* degli Stati Uniti (FTC) ha diffuso la seguente notizia: il *Department of Justice* (DOJ) ha presentato, su istanza della Commissione stessa, una denuncia contro Amazon, contestandole di aver violato una serie di previsioni relative alla protezione dei dati personali e, più in generale, alla tutela del consumatore.

Protagonista delle accuse è il noto assistente vocale "Alexa", prodotto proprio dal colosso di Seattle, che secondo la FTD e il DOJ presenta modalità di funzionamento del tutto incompatibili sia con la normativa a protezione del consumatore, sia con il *Children's Online Privacy Protection Act* (COPPA). Quest'ultima è una legge approvata dal Congresso statunitense nel 1998 e in vigore dal 2000, che detta regole destinate ai gestori di siti *web* e agli operatori di servizi *online* finalizzate a proteggere i dati personali e la sicurezza dei minori. Peraltro, il testo di tale legge è stato aggiornato nel 2013 per riflettere i cambiamenti tecnologici, con inasprimento anche delle sanzioni previste in caso di violazione delle relative prescrizioni.

In particolare, quando si trattino dati personali di minori di 13 anni, il COPPA prevede che siano i genitori a dover prestare il relativo consenso. Si tratta di un aspetto centrale che gioca un ruolo cruciale anche nella denuncia presentata contro Alexa: in effetti, l'*home speaker* viene accusata, *in primis*, di raccogliere e trattare i dati degli utenti con età inferiore a 13 anni, senza richiedere a monte alcun consenso esplicito ai genitori. Amazon non si preoccuperebbe dunque di richiedere né di verificare l'esistenza di un consenso genitoriale prima di procedere al trattamento dei dati dei loro figli.

Secondo la denuncia presentata, altre e numerose sono le regole inosservate: Amazon avrebbe non solo violato la regola del consenso, ma anche conseguentemente impedito ai genitori di esercitare il diritto di cancellazione, previsto dal COPPA, dei dati dei minori illecitamente raccolti.

Ancora, l'azienda viene accusata di conservare i dati vocali raccolti tramite l'assistente vocale Alexa illimitatamente quando, sempre in base al COPPA, la conservazione dei dati di minori di 13 anni dovrebbe perdurare soltanto per il periodo ragionevolmente necessario per fornire il servizio.

Peraltro, molte applicazioni di Amazon che utilizzano Alexa e sono rivolte specificamente ai bambini non avrebbero nemmeno una propria *privacy policy*.

Viene quindi evidenziato come tali condotte pongano anche dati "sensibili" dei minori a rischio di accessi illeciti da parte di terzi non autorizzati, amplificando così i pericoli che si profilano per i minori coinvolti.

Amazon viene poi accusata ulteriormente di conservare a tempo indefinito i dati di geolocalizzazione raccolti tramite l'app di Alexa.

Nella ricostruzione della Commissione, la protezione dei dati personali dei minori si considera sacrificata da Amazon sull'altare del profitto: da qualche tempo, le iniziative della FTC cercano di porre un freno proprio agli sfruttamenti dei dati e agli "esperimenti sociali" realizzati trattando illecitamente i dati dei più piccoli.

Le condotte del *Big Player* di Seattle vengono inoltre ritenute dalla FTC ingannevoli nei confronti dei consumatori in generale, poiché Amazon dichiara pubblicamente che i suoi servizi e dispositivi, Alexa inclusa, sarebbero progettati proprio per proteggere la *privacy* degli utenti, millantando possibilità di cancellazione dei dati di geolocalizzazione e delle registrazioni vocali, che in realtà non vengono affatto garantite.

Al contrario, infatti, tali dati continuano a venire conservati *sine die*, nonostante le richieste di cancellazione pervenute, e, ritiene la Commissione, anche utilizzati illegittimamente per migliorare il funzionamento dell'algoritmo di Alexa.

In particolare, secondo la denuncia, la conservazione delle registrazioni vocali dei bambini avviene per implementare le capacità di riconoscimento e di elaborazione vocale di Alexa. Le voci dei bambini differiscono infatti da quelli degli adulti, quindi le registrazioni vocali conservate illegittimamente fornirebbero ad Amazon un prezioso *dataset* per addestrare l'algoritmo di Alexa a interpretare al meglio le richieste dei minori, i cui dati sono particolarmente utili per lo sviluppo di software di intelligenza artificiale.

Dopo l'elenco delle contestazioni, la Commissione riepiloga le richieste avanzate nella denuncia presentata: *in primis* che Amazon paghi 25 milioni di dollari US per le violazioni commesse, e poi che tenga una serie di condotte finalizzate a interrompere gli illeciti in corso e a impedire la commissione di nuove violazioni. In tal senso, si propone che Amazon cancelli tutti gli *account* inattivi dei bambini, e anche alcune registrazioni vocali e informazioni di geolocalizzazione, che non utilizzi più tali dati per addestrare i propri algoritmi, e ancora che non utilizzi più i dati, specie di minori, che siano stati oggetto di richieste di cancellazione da parte degli utenti.

Inoltre, al colosso di Seattle si richiede l'adozione di un approccio proattivo alla materia del trattamento dei dati personali: in particolare Amazon dovrebbe informare gli utenti sulle sue pratiche di conservazione e cancellazione, garantendo trasparenza soprattutto per quanto attiene alle *policy* relative ai dati di geolocalizzazione e a alle registrazioni vocali, incluse quelle dei bambini. Sulla stessa linea, ad Amazon si richiede di implementare un vero e proprio programma (*privacy program*) sull'uso delle informazioni di geolocalizzazione da parte dell'azienda.

Infine, la notizia diffusa riporta ulteriormente che nella stessa giornata del 31 maggio 2023, la FTC ha annunciato un'ulteriore azione legale contro Ring, una società controllata dalla stessa Amazon, produttrice di citofoni *smart*, accusata di aver concesso l'accesso alle riprese dei propri clienti sia ai suoi dipendenti che ad alcuni appaltatori terzi, consentendo persino di scaricare e condividere liberamente tali video.

L'obiettivo della denuncia presentata contro Amazon evidenziato dalla stessa FTC nel proprio comunicato è quello di rendere più effettiva la protezione dei dati personali dei minori e al contempo di tutelare i consumatori in generale.

La notizia conferma il *trend* di significativo e progressivo accostamento di intenti tra Stati Uniti e Europa. Nel sistema statunitense, in cui la *privacy* è stata dai suoi esordi e a lungo tutelata attraverso l'equilibrio del mercato e ha rappresentato un'estensione della tutela del consumatore e della legittimità delle pratiche commerciali - tanto da riservare i più importanti compiti di controllo del suo rispetto alla stessa FTC - si sono registrate importanti iniziative di costruzione di approcci "integrati" tra protezione dei dati e *consumer protection*, con l'esperienza del *California Consumer Privacy Act* e, più di recente, del *Consumer Data Protection Act* dello stato della Virginia. L'attenzione da ultimo mostrata verso i dati dei minori costituisce un ulteriore tassello nella costruzione di un *right to privacy* più vicino alla *data protection* del Vecchio Continente.

Sul versante italiano ed europeo - dove ricordiamo l'intervento del nostro Garante per la protezione dei dati personali, che già nel 2020 aveva emanato una sorta di *vademecum* per l'utente contenente raccomandazioni per l'uso consapevole degli *smart assistant*, nonché le linee guida dello

European Data Protection Board (EDPB) del 7 luglio 2021 sugli assistenti vocali virtuali [su cui v. in questa rubrica la notizia 2021/3(5)LV - n. 5 del numero 3/2021: http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf] - non potranno ora certamente ignorarsi le contestazioni di una natura "fuorilegge" del più diffuso assistente vocale, mosse ad Amazon nel suo stesso paese di origine.

LAVINIA VIZZONI

https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever

2023/2(12)ES

La pronuncia della Corte Suprema USA del 18.5.2023 nel caso Twitter v. Taamneh et al. per diffusione di contenuti dell'ISIS e l'*opinion* del Justice Thomas

Il 18 maggio 2023 la Corte Suprema degli Stati Uniti d'America ha reso una pronuncia sulla responsabilità di alcune piattaforme digitali per i contenuti ivi pubblicati. La sentenza è preceduta dall'*opinion* del Justice Thomas, fatta propria dalla Corte all'unanimità.

Fatto - Nel 2017 il Sig. Abdulkadir Masharipov compiva un attentato terroristico ad Istanbul per conto dell'ISIS in cui morivano diverse persone, tra cui la Sig.ra Nawras Alassaf. I familiari di quest'ultima intentavano un'azione giudiziaria contro Twitter, Facebook e Google, quale proprietaria della piattaforma YouTube, ai sensi del par. 2333(d) (2), titolo 18 dello U.S.C.

In particolare, gli attori sostenevano che le suddette piattaforme digitali avrebbero sostenuto il terrorismo poiché avrebbero permesso all'ISIS e ai suoi proseliti l'utilizzo di Twitter, Facebook e YouTube trasformandoli in uno strumento per reclutare terroristi, propagandare le proprie idee e raccogliere denaro. Il sostegno al terrorismo si giustificherebbe con la considerazione che tali piattaforme guadagnano dalle inserzioni pubblicitarie, presenti anche nelle pagine ospitanti i contenuti dell'ISIS. Esse, inoltre, utilizzano sofisticati algoritmi che suggeriscono agli utenti i contenuti più appropriati in base alle loro preferenze; ne consegue che se gli individui sono indirizzati alle pagine utilizzate da gruppi terroristici, ancora una volta Twitter, Facebook e YouTube guadagnerebbero dalle inserzioni pubblicitarie. La posizione di Google (rectius, YouTube), inoltre, sarebbe ancora più grave poiché i video sono visualizzati e approvati dal gestore della piattaforma prima di essere pubblicati.

Il giudice di primo grado (District Court) aveva rigettato la domanda attorea, mentre la Ninth Circuit Court of Appeal l'aveva accolta. Twitter, Facebook e YouTube ricorrevano alla Corte Suprema americana.

Diritto - Gli attori invocano quale fonte di responsabilità il par. 2333(d) (2), titolo 18 dello U.S.C., introdotto nel 2016 dal Justice Against Sponsors of Terrorism Act (c.d. JASTA), che consente a ogni cittadino americano di perseguire chi supporta l'autore di fatti illeciti, qui gli atti terroristici, ("… *who aids and abets, by knowingly providing substantial assistance …*"). Si tratta di una forma di responsabilità secondaria o indiretta. I presunti danneggiati, quindi, non invocano il par. 2333(a) che, invece, consente di chiedere il risarcimento direttamente all'autore del danno.

Per stabilire la responsabilità dei convenuti, innanzitutto, occorre stabilire (a) cosa si intenda per "*aids and abets*" e, in secondo luogo, (b) se il supporto debba essere rivolto ad un individuo o anche ad un'azione.

In primo luogo, occorre ricordare che l'espressione "*aids and abets*" non è definita dalla citata normativa, ma è ricorrente dei sistemi di common law ed è stata chiarita nella nota sentenza Halberstam v. Welch, 705 F. 2d 472. Tale pronuncia ha precisato che il supporto presuppone: 1) un illecito compiuto dalla persona che il sostenitore - qui i social media - ha aiutato; 2) nel momento in cui l'assistenza è stata fornita, il sostenitore doveva essere stato consapevole del suo ruolo come parte di un'attività illecita; e 3) il sostenitore deve aver consapevolmente e sostanzialmente supportato il fatto illecito. Nondimeno, la sentenza Halberstam ha individuato sei fattori per stabilire se la collaborazione del sostenitore sia sostanziale. In particolare, bisogna considerare: *"(1) "the nature of the act assisted," (2) the "amount of assistance" provided, (3) whether the defendant was "present at the time" of the principal tort, (4) the defendant's "relation to the tortious actor," (5) the "defendant's state of mind," and (6) the "duration of the assistance" given*".

I suddetti criteri consentono di delimitare il concetto di "sostegno" ai fatti illeciti. Essi devono essere applicati in concreto e caso per caso e possono condurre ad una responsabilità non solo per il supporto dato al danneggiante, ma anche "*for*

other reasonably foreseeable acts done in connection with it".

Resta inteso che ogni responsabilità presuppone una volontà colpevole del responsabile, c.d. elemento soggettivo.

In secondo luogo, va detto che stabilire se il sostegno, generante corresponsabilità, debba essere rivolto ad un soggetto o ad un fatto non è una questione meramente terminologica. Da tale differenza, infatti, dipende la possibilità che un soggetto debba rispondere di un fatto illecito.

La sentenza e l'*opinion* del Justice Thomas - Nel presente caso, l'*opinion* of the Court specifica che "*the Ninth Circuit went astray through a series of missteps that, together, obscured the essence of aiding-and-abetting liability*". La Corte d'Appello avrebbe male interpretato e applicato i criteri stabiliti dalla sentenza Halberstam.

La Corte Suprema, infatti, rileva che nel presente caso non sarebbe stato dimostrato un supporto volontario al fatto illecito: "*plaintiffs must make a strong showing of assistance and scienter. Plaintiffs fail to do so*". Le tesi attoree sono basate sull'inerzia delle piattaforme digitali, ma una condotta passiva o la mera creazione delle piattaforme non è di per sé fonte di responsabilità; né tantomeno l'utilizzo di algoritmi - come quelli menzionati per veicolare i contenuti pubblicitari - implica una collaborazione attiva e sostanziale in favore dell'ISIS. Da ciò non può desumersi alcuna volontà di supportare il terrorismo.

La Corte suprema, inoltre, precisa che l'aiuto eventualmente generante responsabilità in capo ai social media deve essere riferito ad un fatto illecito ("*… the defendant must aid and abet "a tortious act*""). Senonché tale circostanza non è stata dimostrata dagli attori i quali sostenevano, invece, che il sostegno dovesse essere rivolto all'autore del fatto illecito.

In conclusione, la pronuncia, sulla base dell'*opinion* del Justice Thomas, riforma la sentenza d'appello - "w*e therefore reverse the judgment of the Ninth Circuit*" - e rigetta le tesi attoree affermando che non sussiste alcuna responsabilità di Twitter, Facebook e YouTube per i contenuti pubblicati sulle suddette piattaforme.

EMANUELE STABILE

https://www.supremecourt.gov/*opinions*/22pdf/21-1496_d18f.pdf

2023/2(13)VR

L'Online News Act canadese del 22.6.2023 e la decisione di Google di rimuovere i link alle notizie canadesi dai prodotti Search, News e Discover e di terminare il servizio Google News Showcase in Canada

Il 22 giugno 2023 il *Bill* C-18 (***Online News Act***) ha ricevuto il *Royal Assent* e ha acquisito forza di legge nell'ordinamento canadese.

Come può evincersi dal relativo Sommario, il provvedimento si propone di accrescere la correttezza nel mercato canadese delle notizie digitali e di contribuire alla sua sostenibilità, nel rispetto dei principi della libertà di espressione e dell'indipendenza giornalistica. In quest'ottica, l'*Online News Act* appronta un quadro di riferimento in seno al quale gli operatori di settore sono tenuti a stipulare accordi relativi ai compensi per i contenuti resi disponibili dagli intermediari di notizie digitali.

Le ragioni dell'intervento legislativo muovono dal ruolo assunto nell'ecosistema dell'informazione canadese dalle piattaforme digitali, che hanno radicalmente modificato le modalità di accesso ai contenuti giornalistici. Da ciò discende l'esigenza di garantire la diffusione di notizie affidabili, requisito cruciale per la vita democratica del Paese.

In quest'ottica, l'*Online News Act*: dovrebbe garantire un'equa ripartizione dei ricavi tra le piattaforme digitali e le testate giornalistiche; prevede espressamente il ricorso alla contrattazione collettiva da parte delle testate giornalistiche; promuove accordi commerciali tra piattaforme digitali e testate giornalistiche, con un intervento governativo minimo; in caso di mancato accordo, stabilisce in via suppletiva un quadro arbitrale obbligatorio; definisce il ruolo e gli strumenti della *Canadian Radio-television and Telecommunications Commission* (la **Commissione**) in qualità di regolatore.

Sul versante soggettivo, la nuova normativa è indirizzata agli intermediari di notizie digitali, ossia, ai sensi della Sezione 2(1), alle piattaforme di comunicazione online, compresi i motori di ricerca o i servizi di *social media*, che sono soggette all'autorità legislativa del Parlamento canadese e che mettono a disposizione di persone in Canada notizie prodotte da organi di informazione.

Quanto alle condizioni oggettive di applicabilità, si richiede che sussista un significativo squilibrio di potere contrattuale tra l'intermediario e l'impresa di informazione, avuto riguardo ai seguenti fattori: *a*) le dimensioni dell'intermediario; *b*) se il mercato dell'intermediario conferisce ad esso o a un suo operatore un vantaggio strategico rispetto alle

imprese di informazione; *c*) se l'intermediario occupa una posizione preminente sul mercato.

Ai sensi della Sezione 7(1), l'intermediario di notizie digitali che presenti le illustrate caratteristiche è tenuto a notificare tale circostanza alla Commissione, che provvede a stilare e mantenere la lista di cui alla Sezione 8(1).

Nei mesi successivi all'entrata in vigore dell'*Online News Act*, la Commissione pubblicherà le linee guida per le imprese giornalistiche che intendono avanzare istanza per beneficiare del nuovo regime. Potenzialmente, diverse sono le categorie che potranno goderne. Tra esse possono annoverarsi: le organizzazioni giornalistiche canadesi cui si applica l'*Income Tax Act*; le organizzazioni canadesi che producono contenuti giornalistici principalmente incentrati su questioni di interesse generale, a condizione che impieghino almeno due giornalisti e aderiscano a un codice di etica giornalistica; emittenti universitarie, comunitarie o indigene autorizzate ovvero testate indigene gestite da persone indigene.

Complessivamente, nei propositi del legislatore canadese, l'*Online News Act* dovrebbe comportare: un quadro normativo flessibile che promuova la correttezza nelle relazioni commerciali tra piattaforme digitali e testate giornalistiche; una maggiore sostenibilità dell'ecosistema giornalistico canadese, compresa quella delle imprese giornalistiche indipendenti e delle imprese giornalistiche delle comunità indigene e delle minoranze linguistiche ufficiali; un supporto di sostegno ai modelli di *business* innovativi; un panorama sufficientemente diversificato di aziende giornalistiche in grado di offrire servizi a popolazioni diverse in ogni provincia e territorio, comprese le comunità francofone e anglofone, le comunità di colore e altre comunità; il mantenimento dell'indipendenza della stampa.

Nondimeno, già prima della sua formale entrata in vigore l'intervento legislativo ha raccolto dubbi e perplessità da parte degli operatori di settore.

Si dà conto, di seguito, delle criticità segnalate da Kent Walker, *President of Global Affairs* di Google & Alphabet, in un comunicato online del 29.6.2023 (il **Comunicato**) che hanno condotto alla forte decisione di rimuovere i link alle notizie canadesi dai loro prodotti *Search*, *News* e *Discover* e di terminare il servizio *Google News Showcase* in Canada.

A detta della società, l'*Online News Act* sarebbe semplicemente inattuabile in quanto inconciliabile con le modalità con le quali il *web* e i motori di ricerca sono progettati per funzionare.

Più precisamente, si lamenta che i menzionati accordi tra piattaforme digitali e testate giornalistiche si tradurrebbero nell'imposizione di un prezzo per l'esposizione dei link alle notizie (c.d. *"**link tax**"*), rendendo così onerosa un'operazione finora gratuita (e che – beninteso – continuerà ad esserlo per gli intermediari ai quali il provvedimento non sarà applicabile). Ciò, secondo Google, non soltanto non consentirà di risolvere i problemi strutturali della trasparenza e dell'affidabilità delle notizie online ma creerebbe un'insostenibile incertezza finanziaria e di prodotto, esponendo la società a una responsabilità finanziaria imponderabile.

Nel Comunicato si dà inoltre conto degli sforzi collaborativi profusi e dei tentativi di dialogo col Governo canadese, anche mediante interventi davanti allo *Standing Committee on Canadian Heritage* e al *Senate Committee on Transport and Communications*, accompagnati dall'invio di raccomandazioni dettagliate. In particolare, proprio nei giorni a ridosso dell'approvazione finale e del *Royal Assent*, la società avrebbe richiesto al Governo maggiore chiarezza sulle aspettative finanziarie per le piattaforme e di elaborare un percorso specifico e praticabile per ottenere l'esenzione di cui alle Sezioni 11-17 dell'*Online News Act*, in virtù dei consolidati programmi di supporto alle notizie e dei numerosi accordi commerciali conclusi con gli editori. Nell'ambito del programma *Google News Showcase*, ad esempio, sarebbero già perfezionati accordi con oltre 150 testate giornalistiche in tutto il Canada. Nel 2022, inoltre, i link alle testate giornalistiche canadesi sarebbero stati più di 3,6 miliardi, senza previsione di costi, per un totale di traffico online dal valore stimato di 250 milioni di dollari. Infine, si segnala l'invio di costanti feedback costruttivi e di analisi dei rischi, accompagnati da proposte di soluzioni alternative quali, su tutte, quella – già testata altrove – di un fondo indipendente per il giornalismo canadese sostenuto dalle piattaforme e dal Governo.

Al netto di alcune aperture, secondo Google, l'entrata in vigore dell'*Online News Act* ha (per ora) soffocato le richieste di Google, mancando di offrire sufficienti rassicurazioni e rendendo tangibile la prospettiva dell'obbligo di pagamento per i link e dell'esposizione a una responsabilità finanziaria non quantificabile. Pertanto, nonostante sia confermato che la nuova normativa non sarà effettiva fino all'adozione dei regolamenti attuativi, in assenza di adeguati temperamenti la medesima società ha dichiarato la sua decisione di rimuovere i link alle notizie canadesi dai prodotti *Search*, *News* e *Discover* e ad interrompere l'erogazione in Canada del servizio *Google News Showcase*.

VALENTINO RAVAGNANI

https://www.canada.ca/en/canadian-heritage/services/online-news.html

https://blog.google/intl/en-ca/company-news/outreach-initiatives/an-update-on-canadas-bill-c-18-and-our-search-and-news-products/

2023/2(14)DDA

I passi avanti dei lavori sul copyright internazionale in materia di accesso digitale all'istruzione, alla ricerca e al patrimonio culturale nella 43ª riunione del Comitato permanente per il diritto d'autore e i diritti connessi dell'OMPI

Da diversi anni le eccezioni e limitazioni (E&L) al diritto d'autore sono al centro delle discussioni del Comitato permanente per il diritto d'autore e i diritti connessi (**SCCR**) dell'Organizzazione mondiale della proprietà intellettuale (**OMPI**). Come noto, i negoziati mirano a trovare un equilibrio tra il diritto d'autore e la promozione dell'accesso alla conoscenza, all'istruzione e alla cultura da parte della collettività, in particolare nell'ambiente *online* e transfrontaliero. L'obiettivo è quello di arrivare alla definizione di uno o più strumenti giuridici internazionali (modello di legge, raccomandazioni congiunte, trattati e/o altre forme) che prevedano eccezioni e limitazioni a favore di biblioteche, archivi, istituti di istruzione, istituti di ricerca e persone con disabilità.

Dal 13 al 17 marzo 2023, si è tenuta a Ginevra la 43° riunione del SCCR dell'OMPI, durante la quale il Comitato ha compiuto progressi significativi grazie all'adozione di un programma di lavoro sulle eccezioni e le limitazioni basato sulla proposta del Gruppo Africano (SCCR/43/8). Il programma è sostenuto dalla Access to Knowledge Coalition (A2K), di cui fanno parte Communia e il Capitolo italiano di Creative Commons, insieme a numerose altre associazioni che rappresentano educatori, ricercatori, studenti, biblioteche, archivi, musei, altri fruitori della conoscenza e comunità creative in tutto il mondo. La proposta del Gruppo Africano ha ricevuto un ampio consenso da parte delle delegazioni nazionali che hanno riconosciuto la necessità di muoversi verso un sistema di diritto d'autore equo ed equilibrato che sostenga la creatività e l'interesse pubblico, promuovendo l'accesso digitale all'istruzione e alla ricerca, così come al patrimonio culturale. Durante la riunione, è stata condivisa la pubblicazione di Communia "*Nobody puts research in a cage*" che ha evidenziato i limiti e le pressioni subite dai ricercatori scientifici durante le attività di ricerca in ambito digitale e transfrontaliero, mostrando la necessità di una misura internazionale in tale contesto.

Il programma del Gruppo Africano prevede che il Comitato discuta le "questioni prioritarie" relative alle tre seguenti fasi:

- promuovere l'adattamento delle eccezioni per garantire che le leggi a livello nazionale consentano le attività di conservazione da parte di biblioteche, archivi e musei, compreso l'uso dei materiali conservati;
- promuovere l'adattamento delle eccezioni all'ambiente online, ad esempio consentendo l'insegnamento, l'apprendimento e la ricerca attraverso strumenti digitali e online;
- rivedere l'attuazione del Trattato di Marrakech e garantire che le persone con altre disabilità (coperte anche dalla Convenzione sui diritti delle persone con disabilità) possano beneficiare di protezioni simili, in particolare per trarre vantaggio dalle nuove tecnologie.

Il Segretariato dovrebbe ora invitare a condividere ulteriori presentazioni da parte di esperti sulle questioni relative alla scelta della legge applicabile per gli usi transfrontalieri di opere protette dal diritto d'autore, concentrandosi su un approccio basato su casi di studio, come ad esempio l'analisi delle implicazioni di un corso di formazione online con studenti in più Paesi o nel caso in cui i ricercatori siano situati in Paesi diversi.

Inoltre, il piano di lavoro identifica ulteriori ambiti che potrebbero essere affrontati dal Comitato, una volta che le questioni di cui ai punti 1-3 siano state discusse. Il Comitato potrà prendere in considerazione la possibilità di facilitare le future discussioni e gli scambi di opinioni e informazioni riguardanti altre questioni rilevanti, come ad esempio:

- le eccezioni e limitazioni per la ricerca sull'estrazione di testi e dati, tenendo conto dei nuovi sviluppi nel settore;

- le implicazioni transfrontaliere in relazione alle eccezioni e limitazioni sulla conservazione, l'insegnamento e la ricerca;
- la raccomandazione dell'UNESCO sulla scienza aperta (2021) e le sue implicazioni per le leggi e le politiche internazionali sul diritto d'autore; e
- i modelli per la protezione delle eccezioni e limitazioni da clausole contrattuali contrarie, le clausole di protezione, c.d. "*safe harbor*", per le istituzioni educative, di ricerca e del patrimonio culturale, e le eccezioni alle misure tecnologiche di protezione e alle informazioni sulla gestione dei diritti per proteggere gli usi consentiti dalle limitazioni ed eccezioni.

Si sono riscontrati progressi anche in relazione alle disposizioni sulle eccezioni e limitazioni della seconda bozza di testo rivisto per il Trattato dell'OMPI sulle emittenti radiofoniche (SCCR/43/3). Sebbene la portata e l'ampiezza della bozza del trattato siano state ridotte, è ancora essenziale che siano previste solide eccezioni e limitazioni. Purtroppo, la bozza lascia alle parti contraenti la facoltà di decidere se recepire le eccezioni esistenti nel campo del diritto d'autore e dei diritti connessi. Il testo allo stato attuale non prevede, infatti, limitazioni ed eccezioni obbligatorie, che invece sono da ritenersi fondamentali per consentire un'immediata e ampia accessibilità ai contenuti radiofonici da parte di insegnanti, giornalisti, scienziati e ricercatori, soprattutto in relazione al ruolo delle emittenti pubbliche finanziate dallo Stato. Gli Stati membri, però, devono ancora raggiungere l'accordo su tale seconda bozza di testo, come osservato dal delegato italiano. Quest'ultimo, infatti, ha sottolineato che diverse definizioni già previste dalla Convenzione di Roma potrebbero sollevare problemi di interpretazione se non armonizzate nel testo in discussione.

Infine, il Comitato ha previsto una seconda riunione nel corso del 2023, che si svolgerà per soli tre giorni nella settimana del 6 novembre 2023. Sarà l'occasione per formare i gruppi di lavoro sulle eccezioni e limitazioni e per deliberare sulle prossime tappe specifiche del relativo piano di lavoro. È probabile, inoltre, che il trattato sulle emittenti radiofoniche contenga una nuova disposizione in materia di eccezioni e limitazioni.

In conclusione, i risultati della 43ª riunione del SCCR sono molto positivi per la posizione sostenuta dalla A2K, poiché rappresentano un passo avanti per l'adozione di uno strumento internazionale che preveda eccezioni e limitazioni in favore di biblioteche, archivi, istituti di istruzione, istituti di ricerca e persone con disabilità.

DEBORAH DE ANGELIS

https://www.wipo.int/edocs/mdocs/copyright/en/sccr_43/sccr_43_8.pdf

https://www.a2k-coalition.org/

https://communia-association.org/

https://creativecommons.it/chapterIT/

https://communia-association.org/wp-content/uploads/2023/03/Researchers-on-Copyright.pdf

https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=597061

https://digitalcommons.wcl.american.edu/research/84/