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. Daniele Imbruglia nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università di Roma "La Sapienza" (https://web.uniroma1.it/deap/ogid - jodi.deap@uniroma1.it).

SOMMARIO: ***Le modifiche attinenti all'uso di tecnologie digitali recate al codice del consumo dall'attuazione della direttiva (UE) 2019/2161 c.d. Omnibus ad opera del D.lgs. n. 26 del 7.3.2023 – 2. Il nuovo art. 64-ter disp. att. c.p.p. sul diritto all'oblio su internet degli ex imputati e degli ex indagati introdotto con la riforma Cartabia (D.lgs. n. 150 del 10.10.2022) – 3. Il comunicato stampa dell'EDPB del 13.4.2023 sulla decisione vincolante relativa ai provvedimenti da adottarsi nei confronti di Meta per il trasferimento di dati personali EU-USA per il servizio Facebook e sulla costituzione di una task force su ChatGPT in conseguenza del relativo provvedimento cautelare emanato dal Garante privacy italiano il 30.3.2023 – 4. I pareri del 14 e del 28.2.2023 della Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo e dello EDPB sulla bozza di nuova decisione di adeguatezza della Commissione UE relativa al trasferimento dati personali UE-USA – 5. I provvedimenti del Garante privacy italiano del 30.3.2023 e dell'11.4.2023 relativi al servizio ChatGPT e il comunicato stampa del 28.4.2023 – 6. I provvedimenti del 31.12.2022 e del 12.1.2023 adottati dalla Data Protection Commission irlandese in ottemperanza alle tre decisioni vincolanti dell'EDPB del 5.12.2022 nei casi concernenti Meta (per i servizi Facebook e Instagram) e WhatsApp (per l'omonimo servizio) a proposito della base del contratto per il trattamento dei dati personali – 7. La luce verde del 10.2.2023 della Commissione UE a una joint venture tra Deutsche Telekom, Orange, Telefónica e Vodafone per una piattaforma di supporto al marketing digitale in Francia, Germania, Italia, Spagna e Regno Unito – 8. Il provvedimento della Datenschutzconferenz tedesca del 24.11.2022 contro Microsoft per il sistema di trattamento dati del cloud di Office 365 – 9. Le Linee Guida EDPB 3/2022 versione 2.0 del 14.2.2023 sui deceptive design (già dark) patterns – 10. La divulgazione del 30.1.2023 dei risultati dell'indagine a tappeto della Commissione europea e della rete CPC sulle pratiche di manipolazione online – 11. Le conclusioni rassegnate il 16.3.2023 dall'Avvocato generale della Corte di Giustizia UE nella causa C-634/21 (OQ vs Land Hassen; Schufa) sull'articolo 22 GDPR – 12. Il provvedimento cautelare del Garante privacy italiano del 2.2.2023 sulla chatbot Replika – 13. L'avvio di istruttoria AGCM del 21.3.2023 nei confronti di TikTok per omessa predisposizione di adeguati sistemi di monitoraggio dei contenuti pubblicati da terzi (il caso della "cicatrice francese") – 14. Il provvedimento del Garante privacy italiano del 24.11.2022 contro Areti sull'esattezza dei dati personali – 15. La relazione di ENISA del gennaio 2023 sull'ingegnerizzazione della condivisione dei dati personali con particolare focus sui dati del settore sanitario – 16. Il working paper dell'SDA del gennaio 2023 sull'insolvenza nei mercati degli assets digitali – 17. La determina dell'Agenzia per la cybersicurezza nazionale del 3.1.2023 sulla tassonomia degli incidenti informatici da notificare – 18. Il provvedimento del 21.2.2023 dello US Copyright Office su opera d'arte composita di testi creati da un uomo e immagini generate da un sistema di IA generativa (Midjourney) e la Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence del 16.3.2023 – 19. Gli obiter dicta dell'ordinanza della Corte di Cassazione I sez. n. 1107 del 16.01.2023 su diritto d'autore e computer generated content – 20. L'ordinanza cautelare del Tribunale di Venezia del 24.10.2022 in materia di riproduzione digitale di opere pubbliche in pubblico dominio. Il caso "puzzle dell'Uomo Vitruviano – Ravensburger" tra codice dei beni culturali e direttiva europea sul copyright nel mercato unico digitale – 21. Ultimi sviluppi del caso DABUS in Brasile e nel Regno Unito (a proposito della possibilità che un sistema di IA possa***

* 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.

1. Le modifiche attinenti all'uso di tecnologie digitali recate al codice del consumo dall'attuazione della direttiva (UE) 2019/2161 c.d. *Omnibus* ad opera del D.lgs. n. 26 del 7.3.2023.

Il D.lgs. n. 26 del 7 marzo 2023, entrato in vigore il 2 aprile 2023, ha dato attuazione alla direttiva (UE) 2019/2161 che modifica la direttiva 93/13/CEE e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, c.d. direttiva *Omnibus*.
Esso ha modificato in più parti il codice del consumo (D.lgs. 206/2005).
Per quanto riguarda in particolare le modifiche al codice del consumo relative ai rapporti incisi dalle tecnologie digitali, si segnalano le seguenti.
Nella disciplina delle pratiche commerciali scorrette, nell'art. 18 *Definizioni:*

- è stata sostituita la definizione di «prodotto» (art. 18, co. 1 lett. *c)*), con la seguente: "qualsiasi bene o servizio, compresi i beni immobili, *i servizi digitali e il contenuto digitale*, nonché i diritti e gli obblighi";
- è stata inserita la definizione di «classificazione» (art. 18, co. 1 lett. *n-bis)*) come segue: "rilevanza relativa attribuita ai prodotti, come illustrato, organizzato o comunicato dal professionista, a prescindere dai mezzi tecnologici usati per tale presentazione, organizzazione o comunicazione";
- è stata inserita la definizione di «mercato online» (art. 18, co. 1 lett. *n-ter)*) come segue: "*un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione*, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori".

Sempre nella disciplina delle pratiche commerciali scorrette, nell'art. 22 *Omissioni ingannevoli:*

- è stata inserita, nell'elenco degli elementi rilevanti per stabilire nel caso di un invito all'acquisto, l'ingannevolezza dell'omissione, la seguente previsione (art. 22, co. 4, lett. *e-bis*): "*per i prodotti offerti su mercati online*, se il terzo che offre i prodotti è un professionista o meno, sulla base della dichiarazione del terzo stesso al *fornitore del mercato online*";
- sono stati inseriti i seguenti nuovi commi 4-*bis* e 5-*bis*:
  "4 -*bis*) Nel caso in cui sia fornita ai consumatori la possibilità di cercare prodotti offerti da professionisti diversi o da consumatori sulla base di una *ricerca sotto forma di parola chiave, frase o altri dati*, indipendentemente dal luogo in cui le operazioni siano poi effettivamente concluse, sono considerate rilevanti *le informazioni generali, rese disponibili in un'apposita sezione dell'interfaccia online che sia direttamente e facilmente accessibile dalla pagina in cui sono presentati i risultati della ricerca*, in merito ai parametri principali che determinano la *classificazione dei prodotti presentati al consumatore come risultato della sua ricerca* e all'importanza relativa di tali parametri rispetto ad altri parametri. *Il presente comma non si applica ai fornitori di motori di ricerca online definiti ai sensi dell'articolo 2, punto 6, del regolamento (UE) 2019/1150* [c.d. regolamento P2B]";
- "5-*bis*. Se un professionista fornisce l'*accesso alle recensioni dei consumatori sui prodotti*, sono considerate rilevanti le informazioni che indicano se e in che modo il professionista garantisce che le recensioni pubblicate provengano da consumatori che hanno effettivamente acquistato o utilizzato il prodotto".

Sempre nella disciplina delle pratiche commerciali scorrette, nell'art. 23 *Pratiche considerate in ogni caso ingannevoli*, sono state inserite le seguenti previsioni relative alle ricerche online, l'acquisto di biglietti per eventi con strumenti automatizzati, le recensioni sui prodotti e gli apprezzamenti sui social media:

- "m-*bis*) fornire *risultati di ricerca in risposta a una ricerca online del consumatore* senza che sia chiaramente indicato ogni eventuale annuncio pubblicitario a pagamento o pagamento specifico per ottenere una *classificazione migliore dei prodotti all'interno di tali risultati*;
- bb-*bis*) rivendere ai consumatori biglietti per eventi, se il professionista ha acquistato tali biglietti utilizzando *strumenti automatizzati* per eludere qualsiasi limite imposto riguardo al numero di biglietti che

una persona può acquistare o qualsiasi altra norma applicabile all'acquisto di biglietti;

- bb-*ter*) indicare che le *recensioni di un prodotto* sono inviate da consumatori che hanno effettivamente utilizzato o acquistato il prodotto senza adottare misure ragionevoli e proporzionate per verificare che le recensioni provengano da tali consumatori;
- bb-*quater*) inviare, o incaricare un'altra persona giuridica o fisica di inviare, *recensioni di consumatori* false o falsi apprezzamenti o di fornire false informazioni in merito a recensioni di consumatori o ad *apprezzamenti sui media sociali*, al fine di promuovere prodotti".

Nella disciplina del *Rapporto di consumo* (Parte III del codice del consumo), in particolare nel Capo I, rubricato *Dei diritti dei consumatori nei contratti*, del Titolo III, rubricato *Modalità contrattuali*, al comma 1 dell'art. 45 *Definizioni* sono state apportate le seguenti modificazioni:

- la definizione di «beni» (lettera *c)*) è stata sostituita con la seguente definizione composta di tre categorie tra cui quella di '*beni con elementi digitali*': "[…] 2) *qualsiasi bene mobile materiale che incorpora, o è interconnesso con, un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni proprie del bene, anche denominati 'beni con elementi digitali')* […]";
- la definizione di «contratto di servizi» (lettera *f)*) è stata sostituita dalla seguente: "qualsiasi contratto diverso da un contratto di vendita in base al quale il professionista fornisce o si impegna a fornire un servizio, *compreso un servizio digitale*, al consumatore";
- è stata aggiunta la definizione di «servizio digitale» (lettera q-*bis*) comprendente le seguenti due categorie: "1) *un servizio che consente al consumatore di creare, trasformare, archiviare i dati o di accedervi in formato digitale*; oppure 2) *un servizio che consente la condivisione di dati in formato digitale, caricati o creati dal consumatore e da altri utenti di tale servizio, o qualsiasi altra interazione con tali dati*;"
- è stata aggiunta la definizione di «mercato online» (lettera q-*ter*): "*un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori*";
- è stata aggiunta la definizione di «*fornitore di mercato online*» (lettera q-*quater*): "*qualsiasi professionista che fornisce un mercato online ai consumatori*";
- è stata aggiunta la definizione di «compatibilità» (lettera q-*quinquies*): "*la capacità del contenuto digitale o del servizio digitale di funzionare con hardware o software con cui sono normalmente utilizzati contenuti digitali o servizi digitali dello stesso tipo, senza che sia necessario convertire il contenuto digitale o il servizio digitale*";
- è stata aggiunta la definizione di «funzionalità» (lettera q-*sexies*): "la capacità del contenuto digitale o del servizio digitale di svolgere tutte le sue funzioni in considerazione del suo scopo";
- è stata aggiunta la definizione di «interoperabilità» (lettera q-*septies*): "*la capacità del contenuto digitale o del servizio digitale di funzionare con hardware o software diversi da quelli con cui sono normalmente utilizzati i contenuti digitali o i servizi digitali dello stesso tipo*".

Nel successivo art. 46 c. cons., rubricato *Ambito di applicazione*, è stato aggiunto il seguente comma 1-*bis*, che riprende la dirompente definizione di contratto (di fornitura di contenuto digitale o di servizi digitali) nel quale *il consumatore fornisce o si impegna a fornire suoi dati personali* di cui alla direttiva (UE) 2019/770, la cui attuazione nel nostro ordinamento ad opera del D.Lgs. 173/2021 ha comportato l'introduzione, dopo il Capo I del Titolo III della Parte IV c. cons., il nuovo Capo I-bis (artt. 135 *octies* ss. c. cons.), relativo ai contratti di fornitura di contenuto digitale e di servizi digitali, ed in particolare l'introduzione dell'art. 135-*octies* co. 3 c. cons. che contiene quella definizione (v. notizia sub 1 nel numero 4/2021 di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf):

"1-*bis*. Ferma la disciplina dettata dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e dal decreto legislativo 30 giugno 2003, n. 196, le disposizioni delle sezioni da I a IV del

presente capo si applicano *anche se il professionista fornisce o si impegna a fornire un contenuto digitale mediante un supporto non materiale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali al professionista*, tranne i casi in cui i dati personali forniti dal consumatore siano trattati dal professionista esclusivamente ai fini della fornitura del contenuto digitale su supporto non materiale o del servizio digitale a norma delle predette disposizioni o per consentire l'assolvimento degli obblighi di legge cui il professionista è soggetto, e questi non tratti tali dati per nessun altro scopo".

Nell'art. 48 co. 1 c. cons., rubricato *Obblighi d'informazione nei contratti diversi dai contratti a distanza o negoziati fuori dei locali commerciali*, sono state sostituite le lettere *e)*, *g)* e *h)* come segue: "*e)* oltre a un richiamo dell'esistenza della *garanzia legale di conformità per i beni, il contenuto digitale e i servizi digitali*, l'esistenza e le condizioni del servizio postvendita e delle garanzie convenzionali, se applicabili"; *"g)* se applicabile, *la funzionalità dei beni con elementi digitali, del contenuto digitale e dei servizi digitali, comprese le misure applicabili di protezione tecnica*"; "*h) qualsiasi compatibilità e interoperabilità pertinente dei beni con elementi digitali, del contenuto digitale e dei servizi digitali*, di cui il professionista sia a conoscenza o di cui ci si può ragionevolmente attendere che sia venuto a conoscenza, se applicabili".

Anche per i contratti a distanza e negoziati fuori dai locali commerciali sono stati introdotti una consistente serie di nuovi obblighi informativi, attraverso la modifica dell'art. 49 c. cons. e la previsione del nuovo art. 49-*bis* c. cons.

Quanto all'art. 49 c. cons., rubricato *Obblighi di informazione nei contratti a distanza e nei contratti negoziati fuori dei locali commerciali*, al co.1 sono state modificate alcune previsioni ed inserite nuove previsioni, tra le quali spicca l'*obbligo di informazione che il prezzo è stato personalizzato sulla base di un processo decisionale automatizzato* (nuova lettera e-*bis*). Nel dettaglio, queste sono le modifiche:

- la previsione della lettera *c*) è stata sostituita come segue "*c)* l'indirizzo geografico dove il professionista è stabilito, il suo numero di telefono e il suo *indirizzo elettronico*. Inoltre, *se il professionista fornisce qualsiasi altro mezzo di comunicazione elettronica che garantisca al consumatore di poter intrattenere con lui una corrispondenza scritta, che rechi la data e l'orario dei relativi messaggi, su un supporto durevole, il professionista deve fornire anche le informazioni relative a tale altro mezzo*. Tutti questi mezzi di comunicazione forniti dal professionista devono consentire al consumatore di contattarlo rapidamente e di comunicare efficacemente con lui. Ove applicabile, il professionista fornisce anche l'indirizzo geografico e l'identità del professionista per conto del quale agisce";
- è stata introdotta la lettera e-*bis* contenente la seguente previsione: "e-*bis* se applicabile, *l'informazione che il prezzo è stato personalizzato sulla base di un processo decisionale automatizzato, ferme le garanzie di cui all'articolo 22 del [GDPR]*";
- le previsioni delle lettere *n*), *t)*, e *u)* sono stata sostituite come segue "*n)* un promemoria dell'esistenza della *garanzia legale di conformità per i beni, il contenuto digitale e i servizi digitali*;" "*t)* se applicabile, la *funzionalità dei beni con elementi digitali, del contenuto digitale e dei servizi digitali, comprese le misure applicabili di protezione tecnica*;" "*u)* qualsiasi *compatibilità e interoperabilità pertinente dei beni con elementi digitali, del contenuto digitale e dei servizi digitali*, di cui il professionista sia a conoscenza o di cui ci si può ragionevolmente attendere che sia venuto a conoscenza, se applicabile".

Quanto al nuovo art. 49-*bis* c. cons., rubricato *Obblighi di informazione supplementari specifici per i contratti conclusi su mercati online*, esso così reca: "1. Prima che un consumatore sia vincolato da un contratto a distanza , o da una corrispondente offerta, su un mercato online, il fornitore del mercato online, fermo restando quanto previsto dalla parte II, Titolo III, indica altresì al consumatore, in maniera chiara e comprensibile e in modo appropriato al mezzo di comunicazione a distanza: a) informazioni generali, rese disponibili *in un'apposita sezione dell'interfaccia online che sia direttamente e facilmente accessibile dalla pagina in cui sono presentate le offerte, in merito ai principali parametri che determinano la classificazione*, quale definita dall'art. 18, comma 1, lettera n-*bis*), *delle offerte presentate al consumatore come un risultato della sua ricerca e all'importanza relativa di tali parametri*

rispetto ad altri parametri; b) se il terzo che offre beni, servizi o contenuto digitale è un professionista o meno, sulla base della dichiarazione del terzo stesso al fornitore del mercato online; c) nel caso in cui il terzo che offre i beni, i servizi o il contenuto digitale non sia un professionista, che al contratto non si applicano i diritti dei consumatori dei consumatori derivanti dal diritto dell'Unione europea sulla tutela dei consumatori; d) *se del caso, il modo in cui gli obblighi relativi al contratto sono ripartiti tra il terzo che offre i i beni, i servizi o il contenuto digitale e il fornitore del mercato online*. Tali informazioni lasciano impregiudicata la responsabilità che il fornitore del mercato online o il professionista terzo ha in relazione al contratto in base ad altre norme di diritto europeo o nazionale. 2. Le presenti disposizioni lasciano impregiudicata l'applicazione, per quanto di competenza, delle norme contenute nel decreto legislativo 9 aprile 2003, n. 70, in materia di obblighi di informazione per i fornitori dei mercati online".

Il comma 4 dell'art. 51 c. cons., rubricato *Requisiti formali dei contratti a distanza*, è stato modificato per chiarire che se il contratto è concluso mediante un mezzo di comunicazione a distanza che consente uno spazio o un tempo limitato per comunicare le informazioni, le informazioni essenziali ivi previste che il professionista deve fornire su o mediante quello specifico mezzo e prima della conclusione del contratto (ossia almeno le informazioni precontrattuali riguardanti le caratteristiche principali dei beni o servizi, l'identità del professionista, il prezzo totale, il diritto di recesso, la durata del contratto e, nel caso di contratti a tempo indeterminato, le condizioni di risoluzione del contratto, come indicato rispettivamente all'articolo 49, co. 1, lett. *a), b), e), h)* e *q)* c. cons.) non comprendono il modulo di recesso tipo figurante all'allegato I, parte B, di cui alla lettera *h)* della medesima disposizione; e che le altre informazioni di cui all'articolo 49, co.1 c. cons., compreso il modello del modulo di recesso, sono fornite dal professionista in un modo appropriato conformemente al comma 1 dell'art. 51 c. cons.

All'art. 56 cod. cons., rubricato *Obblighi del professionista nel caso di recesso* (del consumatore), sono stati introdotti una serie di nuovi commi (da 3-*ter* a 3-*sexies*) relativi al c.d. *user generated content*, ossia ai contenuti generati dall'utente, in questo caso utente-consumatore: "3-*ter*. Il professionista si astiene dall'utilizzare qualsiasi contenuto, diverso dai dati personali [per i dati personali il nuovo comma 3-*bis* richiama al dovere da parte del professionista del rispetto del GDPR nel suo complesso] che è stato fornito o creato dal consumatore durante l'utilizzo del contenuto digitale o del servizio digitale fornito dal professionista, salvo quando tale contenuto: a) è privo di utilità fuori del contesto del contenuto digitale o del servizio digitale fornito dal professionista; b) riguarda unicamente l'atticità del consumatore durante l'utilizzo del contenuto digitale o del servizio digitale fornito dal professionista; c) è stato aggregato dal professionista ad altri dati e non può essere disaggregato o può esserlo soltanto con sforzi sproporzionati; d) è stato generato congiuntamente dal consumatore e da altre persone, e se altri consumatori possono continuare a farne uso. 3-*quater*. Fatta eccezione per le situazioni di cui al comma 3-*ter*, lettera a), b) o c), il professionista, su richiesta del consumatore, mette a disposizione di questi qualsiasi contenuto, diverso dai dati personali, fornito o creato dal consumatore durante l'utilizzo del contenuto digitale o del servizio digitale fornito dal professionista. 3-*quinquies*. Il consumatore ha il diritto di recuperare dal professionista tali contenuti digitali gratuitamente e senza impedimenti, entro un lasso di tempo ragionevole e in un formato di uso comune e leggibile da dispositivo automatico. 3-*sexies*. In caso di recesso dal contratto [da parte del consumatore], il professionista può impedire qualsiasi ulteriore utilizzo del contenuto digitale o del servizio digitale da parte del consumatore, in particolare rendendogli inaccessibile tale contenuto o servizio digitale o disattivando il suo account utente, fatto salvo quanto previsto al comma 3-*quater* [del medesimo articolo 56 c. cons.].

Al successivo art. 57 cod. cons., *Obblighi del consumatore in caso di recesso* (del consumatore), è stato aggiunto il comma 2-*bis*, che prevede che in caso di suo recesso dal contratto, il consumatore deve astenersi dall'utilizzare il contenuto digitale o il servizio digitale e dal metterlo a disposizione di terzi.

Infine, nell'elenco dei casi elencati dal comma 1 dell'art. 59 c.cons., rubricato *Eccezioni al diritto di recesso*, relativamente ai quali il consumatore non ha il diritto di recesso previsto

dagli artt. 52 e 58 c. cons. per i contratti a distanza e i contratti negoziati fuori dei locali commerciali, è stata modificata la norma della lettera *o)*, al fine di escludere il diritto di recesso del consumatore relativamente ai contratti per la fornitura di contenuto digitale mediante un supporto non materiale qualora l'esecuzione sia iniziata e, nei casi in cui il contratto impone al consumatore l'obbligo di pagare, qualora: 1) il consumatore abbia dato il suo previo consenso espresso a iniziare la prestazione durante il periodo di diritto di recesso; 2) il consumatore abbia riconosciuto di perdere così il proprio diritto di recesso; 3) il professionista abbia fornito la conferma conformemente all'art. 50, co. 2, o all'art. 51, co.7 c. cons.

SALVATORE ORLANDO

https://www.gazzettaufficiale.it/eli/id/2023/03/18/23G00033/sg

2. Il nuovo art. 64-ter disp. att. c.p.p. sul diritto all'oblio degli ex imputati e degli ex indagati introdotto con la riforma Cartabia (D.lgs. n. 150 del 10.10.2022).

Il D.lgs. n.150 del 2022 (c.d. riforma Cartabia) ha introdotto tra le disposizioni di attuazione del codice di procedura penale l'art. 64-*ter*, rubricato *Diritto all'oblio degli imputati e delle persone sottoposte ad indagini*.

La novella attribuisce alla persona nei cui confronti siano stati pronunciati una sentenza di proscioglimento o di non luogo a procedere, ovvero un provvedimento di archiviazione, la facoltà di chiedere relativamente ai "*dati personali riportati nella sentenza o nel provvedimento*" ***(i)*** che ne sia preclusa l'indicizzazione, o ***(ii)*** che ne sia disposta la deindicizzazione sul *web;* in entrambi i casi "*ai sensi e nei limiti dell'articolo 17 del regolamento (UE) n. 2016/679*" (il **GDPR**), e fermo restando – si aggiunge – quanto previsto dall'art.52 del D. Lgs. 196/2003 (il **Codice privacy**).

La previsione *sub* ***(i)*** *supra*, ossia la richiesta che sia "preclusa l'indicizzazione" costituisce una novità nel nostro sistema, a differenza di quella *sub* ***(ii)*** *supra*, essendo la deindicizzazione sussumibile nello schema normativo dell'art. 17 GDPR e avendo la stessa formato oggetto di una ormai numerosa casistica giurisprudenziale anche in epoca precedente al GDPR (v. in questa rubrica: notizia n. 12 nel numero 1/2022 sulla sentenza della Cassazione n. 3952 del 8 febbraio 2022 sul diritto all'oblio e le copie *cache* http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf; e anche la notizia n. 14 nel numero 4/2022 sulla ordinanza della Cassazione Prima Sez. Civile n. 34658/2022 del 24.11.2022 sul diritto all'oblio e l'ordine di rimozione c.d. globale http://www.personaemercato.it/wp-content/uploads/2023/01/Osservatorio.pdf).

L'inserimento del richiamo all'art. 52 Codice privacy nell'art. 64-*ter* disp. att. c.p.p. risulta essere stato raccomandato dal Garante per la protezione dei dati personali (di seguito il "**Garante privacy**"). In proposito, in un parere espresso dal Garante privacy il 1.9.2022 sullo schema del decreto legislativo in questione (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9802612 di seguito il "**Parere**"), la medesima autorità osservava che le nuove norme dell'art. 64-*ter* disp. att. c.p.p. costituiscono uno strumento di cautela "ulteriore rispetto all'oscuramento, in particolare su istanza di parte, delle generalità di cui all'art. 52, co. 1, [del Codice privacy]".

Sempre leggendo il citato Parere, si ricava che, invece, in questo contesto il richiamo operato dall'art. 64-*ter* disp. att. c.p.p. all'art. 17 GDPR ("*ai sensi e nei limiti dell'articolo 17 del regolamento (UE) n. 2016/679"*) può risultare foriero di dubbi relativamente alla previsione della preclusione della indicizzazione. Ciò in quanto, si legge nel Parere, tale richiamo sembrerebbe comportare una discrezionalità (i.e. la discrezionalità prevista dall'art. 17 GDPR) nell'accogliere o respingere la relativa richiesta, che dovrebbe tuttavia sussistere (così si argomenta nel Parere) solo nel caso della deindicizzazione -i.e. solo nel caso della richiesta sub ***(ii)*** - e non anche nel caso della richiesta di preclusione della indicizzazione, i.e. la richiesta sub ***(i)***.

L'art. 64-*ter* disp. att. c.p.p. prevede che l'interessato possa fare istanza alla cancelleria del giudice che ha emesso il provvedimento affinché questa proceda ad apporre e sottoscrivere specifica annotazione volta a precludere l'indicizzazione del provvedimento ovvero affinché il provvedimento costituisca titolo per richiedere la deindicizzazione.

In particolare, l'art. 64-*ter* co. 2 disp. att. c.p.p. prevede che nel caso di richiesta volta a precludere l'indicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone e sottoscrive la seguente annotazione, recante sempre l'indicazione degli estremi del medesimo articolo: «Ai sensi e nei limiti dell'articolo 17 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, è

preclusa l'indicizzazione del presente provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'istante»; mentre il co. 3 del medesimo articolo prevede che nel caso di richiesta volta ad ottenere la deindicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone e sottoscrive la seguente annotazione, recante sempre l'indicazione degli estremi dello stesso articolo: «Il presente provvedimento costituisce titolo per ottenere, ai sensi e nei limiti dell'articolo 17 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, un provvedimento di sottrazione dell'indicizzazione, da parte dei motori di ricerca generalisti, di contenuti relativi al procedimento penale, rispetto a ricerche condotte a partire dal nominativo dell'istante».

SERENA MIRABELLO

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2022-10-10;150

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9802612

3. Il comunicato stampa dell'EDPB del 13.4.2023 sulla decisione vincolante relativa ai provvedimenti da adottarsi nei confronti di Meta per il trasferimento di dati personali EU-USA per il servizio Facebook e sulla costituzione di una *task force* su ChatGPT in conseguenza del relativo provvedimento cautelare emanato dal Garante privacy italiano il 30.3.2023

Con un comunicato stampa del 13 aprile 2023, lo *European Data Protection Board* (**EDPB** o il **comitato**) ha annunciato di aver adottato una decisione vincolante ai sensi dell'art. 65 del regolamento (UE) 2016/679 (**GDPR**) concernente un progetto di decisione dell'autorità di controllo irlandese (il **Garante privacy irlandese**) sulla legittimità dei trasferimenti dei dati personali da parte di Meta Platforms Ireland Limited (**Meta Ireland**) negli Stati Uniti d'America per il suo servizio Facebook.
La decisione vincolante dell'EDPB affronta importanti questioni sollevate dal progetto di decisione del Garante privacy irlandese nella sua qualità di autorità capofila - ai sensi dell'art. 65(1)(a) GDPR - per quanto riguarda Meta Ireland.
Nel comunicato stampa si sottolinea che la decisione vincolante dell'EDPB ha un ruolo centrale nell'assicurare una corretta e coerente applicazione del GDPR da parte delle autorità di controllo nazionali.
L'intervento dell'EDPB si è reso necessario ai sensi dell'art. 65 GDPR (*Composizione delle controversie da parte del comitato*) poiché non è stato trovato un accordo sulle obiezioni sollevate da molte autorità di controllo sul progetto di decisione del Garante privacy irlandese.
Nella sua decisione vincolante, l'EDPB ha composto la controversia sulla questione relativa al provvedimento o ai provvedimenti che devono essere disposti dalla decisione finale del Garante privacy irlandese, ossia se tali provvedimenti debbano consistere in una sanzione amministrativa pecuniaria e/o in un ordine di rendere le operazioni di trattamento dei dati personali conformi al GDPR.
Il Garante privacy irlandese, quale autorità capofila, dovrà adesso adottare la sua decisione finale, nei confronti del titolare del trattamento dei dati personali, sulla base della decisione vincolante dell'EDPB, entro un mese dalla notifica della decisione dell'EDPB. L'EDPB pubblicherà la sua decisione vincolante sul suo sito web solo dopo che il Garante privacy irlandese avrà notificato la sua decisione finale al titolare del trattamento.
Nello stesso comunicato stampa del 13.4.2023, il comitato ha reso pubblico che i suoi membri (i.e. per ciascun Stato membro, la figura di vertice o un rappresentante delle autorità di controllo nazionali e il garante europeo della protezione dei dati) hanno discusso il recente provvedimento adottato dall'autorità di controllo italiana contro Open AI a proposito del servizio ChatGPT (su cui v. *infra* notizia n. 5 in questa rubrica).
A tal riguardo, il comunicato ha aggiunto che l'EDPB ha organizzato una *task force* per rafforzare la cooperazione e scambiare informazioni su eventuali ulteriori provvedimenti da parte delle varie autorità di controllo nazionali.

SALVATORE ORLANDO

https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_it

4. I pareri del 14 e del 28.2.2023 della Commissione per le libertà civili, la giustizia e gli affari interni del

Parlamento europeo e dello EDPB sulla bozza di nuova decisione di adeguatezza della Commissione UE relativa al trasferimento dati personali UE-USA

Il 14 e il 28 febbraio 2023, rispettivamente la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento UE e lo *European Data Protection Board* ("**EDPB**") hanno espresso il proprio parere sulla bozza di decisione di adeguatezza pubblicata il 13 dicembre 2022 dalla Commissione europea sull'accordo UE-USA Data Privacy Framework raggiunto nel marzo 2022 (rispettivamente la "**Bozza di decisione di adeguatezza**" e l'"**Accordo**").

La Bozza di decisione di adeguatezza era intervenuta a seguito dell'*Executive Order* 14086 *Enhancing Safeguards for United States Signals Intelligence Activities* emesso dal Presidente Biden il 7 ottobre 2022 ("**EO**") e si era pronunciata sull'Accordo.

L'Accordo è volto a superare le obiezioni sollevate dalla Corte di giustizia dell'UE ("**CGUE**") nella nota sentenza c.d. Schrems II del luglio 2020 che aveva annullato il *Privacy Shield* (su cui v. in questa rubrica la notizia n. 1 del numero 3/2020 http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf). In particolare, l'Accordo ha introdotto limiti più stringenti all'accesso e all'utilizzo dei dati dei cittadini UE da parte delle autorità statunitensi e una maggiore tutela dei diritti dei cittadini europei attraverso un nuovo sistema di ricorso a due livelli per l'esame e la risoluzione dei reclami attraverso l'istituzione di una apposita autorità denominata *Data Protection Review Court* ("**DPRC**"). L'Accordo prevede anche un meccanismo periodico di controllo della sua applicazione e un sistema di certificazione dell'adesione da parte delle società statunitensi ad opera del Dipartimento del Commercio USA.

Sulla base dell'Accordo la Commissione ha avviato il processo di emissione della decisione di adeguatezza previsto e disciplinato dall'art. 45 GDPR con cui la Commissione è chiamata a valutare se il paese di destinazione dei dati (in questo caso gli Stati Uniti) soddisfi il requisito di "equivalenza essenziale" del livello di protezione dei dati personali rispetto a quello garantito dall'ordinamento dell'UE. Nella sua valutazione la Commissione ha prestato particolare attenzione ai punti attenzionati dalla CGUE nella sentenza "Schrems II", in particolare l'accesso ai dati da parte delle autorità pubbliche statunitensi per l'applicazione del diritto penale e per finalità di sicurezza nazionale.

All'esito della valutazione della Commissione europea e della conseguente Bozza di decisione di adeguatezza, sono intervenuti i pareri della Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento UE e dell'EDPB.

La Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento UE, pur apprezzando i passi avanti fatti con l'EO, ha espresso un parere negativo sulla Bozza di decisione di adeguatezza, spingendo la Commissione a continuare i negoziati con gli Stati Uniti in modo da arrivare a un accordo quadro che garantisca una effettiva equivalenza rispetto al livello di protezione offerto dall'UE.

Tra i principali punti sollevati, la Commissione ha rilevato come i principi di proporzionalità e necessità delineati nell'EO non risultino in linea con la normativa EU e l'interpretazione della CGUE. Il principio di proporzionalità, infatti, è suscettibile di un'interpretazione eccessivamente ampia in quanto l'EO prevede che in presenza di motivi legittimi di sicurezza nazionale possa essere giustificata la raccolta in massa dei dati, e l'elenco di tali motivi può essere ampliato dal Presidente degli Stati Uniti anche senza che ne venga data pubblica notizia.

In secondo luogo, la Commissione parlamentare ha espresso dei dubbi sull'effettiva indipendenza e imparzialità della DPRC, essendo questa parte dell'organo esecutivo e non di quello giudiziario. Inoltre, il sistema di ricorso delineato dall'EO non garantisce in maniera adeguata il diritto di difesa dell'interessato in quanto non è previsto un obbligo di notifica del trattamento dei dati personali, né la possibilità di appellare la decisione della DPRC davanti una corte federale.

Anche l'EDPB ha espresso il proprio parere sulla bozza di decisone di adeguatezza, secondo il meccanismo previsto dall'art. 70 GDPR, avendo riguardo sia agli aspetti commerciali che all'accesso e all'utilizzo dei dati personali da parte delle autorità pubbliche statunitensi.

In linea generale, l'EDPB ha accolto con favore i numerosi passi avanti fatti dall'EO sul tema dell'accesso da parte del Governo statunitense ai dati personali trasferiti negli USA, in particolare l'introduzione dei principi di necessità e proporzionalità e il nuovo meccanismo di ricorso per i cittadini europei. Allo stesso tempo, l'autorità ha individuato alcuni persistenti punti di criticità, *in primis* l'assenza di un'autorizzazione preventiva di un'autorità indipendente per la raccolta in massa dei dati – nei casi in cui questa è consentita ai sensi dell'EO – e di un controllo sistematico *ex post* da parte di un'autorità giudiziaria.

Con riferimento al meccanismo di reclamo, l'EDPB ha visto con favore l'introduzione di un'apposita

Corte (la DPRC) dotata di un livello di indipendenza significativamente superiore rispetto all'*Ombudsperson* previsto nel sistema precedente. Rimangono tuttavia – ha osservato l'EDPB – dei dubbi sul piano della trasparenza e dell'appellabilità delle decisioni della medesima Corte.

Anche per quanto riguarda gli aspetti commerciali, l'EDPB ha accolto con favore i nuovi principi introdotti dall'Accordo, ma ha rilevato che alcuni principi sono rimasti essenzialmente gli stessi del *Privacy Shield*. Pertanto, rimangono le preoccupazioni già sollevate dalla CGUE nella sentenza "Schrems II", ad esempio per alcune esenzioni al diritto di accesso, l'assenza di definizioni chiare, la mancanza di chiarezza sull'applicazione dei principi dell'Accordo agli incaricati del trattamento, l'ampia esenzione dal diritto di accesso per le informazioni disponibili al pubblico e la mancanza di norme specifiche sul processo decisionale automatizzato e sulla profilazione.

Altro punto cruciale è quello dei trasferimenti successivi. L'EDPB ha ribadito che il livello di protezione dei dati non deve essere compromesso dai trasferimenti successivi e ha invitato la Commissione a chiarire che le garanzie imposte dal destinatario iniziale all'importatore nel Paese terzo devono essere efficaci alla luce della legislazione del Paese terzo prima di un trasferimento successivo.

Infine, l'EDPB ha sottolineato la necessità che vengano adottate politiche e procedure aggiornate per l'attuazione dell'EO da parte delle agenzie di intelligence statunitensi prima dell'adozione della decisione di adeguatezza e ha raccomandato alla Commissione europea di valutare tali politiche e procedure aggiornate ai fini della decisione condividendo in via preliminare la propria valutazione con l'EDPB.

In conclusione, nel comunicato del 28 febbraio con cui è stato rilasciato il parere, il presidente dell'EDPB Andrea Jelinek ha dichiarato: "Un elevato livello di protezione dei dati è essenziale per salvaguardare i diritti e le libertà degli individui dell'UE. Pur riconoscendo che i miglioramenti apportati al quadro giuridico statunitense sono significativi, raccomandiamo di affrontare le preoccupazioni espresse e di fornire i chiarimenti richiesti per garantire la validità della decisione di adeguatezza. Per lo stesso motivo, riteniamo che dopo la prima revisione della decisione di adeguatezza, le revisioni successive debbano avvenire almeno ogni tre anni e ci impegniamo a contribuirvi".

https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf
https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

5. I provvedimenti del Garante privacy italiano del 30.3.2023 e dell'11.4.2023 relativi al servizio ChatGPT e il comunicato stampa del 28.4.2023

Con due provvedimenti adottati nell'arco di 12 giorni, l'Autorità garante per la protezione dei dati personali (**Garante**) ha dapprima disposto in via d'urgenza ai sensi dell'art. 58, par. 2, lett. f), del regolamento (UE) 2016/679 (**GDPR**) nei confronti di OpenAI L.L.C. (**OpenAI**), in relazione al suo servizio ChatGPT e in qualità di titolare del trattamento dei dati personali effettuato attraverso la relativa applicazione, la misura della limitazione provvisoria del trattamento dei dati personali degli interessati stabiliti nel territorio italiano (provvedimento del 30.3.2023 doc. web 9870832: il **Primo provvedimento**); e, successivamente, ha disposto la sospensione del Primo provvedimento a far data da (e quindi, condizionatamente a) l'adempimento delle prescrizioni di cui ai punti da 1 a 7 del secondo provvedimento (provvedimento dell'11.4.2023 doc. web 9874702: il **Secondo provvedimento**).

Le prescrizioni di cui ai punti da 1 a 7 del Secondo Provvedimento sono qui di seguito riportate. Per comprendere il contesto, e prima di ripercorrere anche il contenuto del Primo provvedimento, si aggiunge che, in conseguenza del Primo provvedimento, in data 1.4.2023, OpenAI disponeva la disabilitazione del servizio ChatGPT per gli utenti in Italia.

Le prescrizioni rivolte a OpenAI nei punti da 1 a 7 del Secondo provvedimento sono le seguenti:

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

2) mettere a disposizione, sul suo sito Internet, almeno agli interessati, anche diversi dagli utenti del servizio ChatGPT, che si collegano dall'Italia,

uno strumento attraverso il quale possano esercitare il diritto di opposizione rispetto ai trattamenti dei propri dati personali, ottenuti da terzi, svolti dalla società ai fini dell'addestramento degli algoritmi e dell'erogazione del servizio;

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

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

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

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

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

Altre due prescrizioni, contenute ai punti 8) e 9) del Secondo provvedimento, non sono comprese tra quelle condizionanti la sospensione del Primo provvedimento. Si tratta, in particolare, delle prescrizioni di:

8) sottoporre al Garante, entro il 31 maggio 2023, un piano, da implementarsi entro il 30 settembre 2023, per l'adozione di strumenti di *age verification* idoneo a escludere l'accesso al servizio agli utenti infratredicenni e a quelli minorenni in assenza di un'espressa manifestazione di volontà da parte di chi esercita sugli stessi la responsabilità genitoriale;

9) promuovere, entro il 15 maggio 2023, una campagna di informazione, di natura non promozionale, su tutti i principali mezzi di comunicazione di massa italiani (radio, televisione, giornali e Internet) i cui contenuti andranno concordati con il Garante, allo scopo di informare le persone dell'avvenuta probabile raccolta dei loro dati personali ai fini dell'addestramento degli algoritmi, dell'avvenuta pubblicazione sul sito internet di OpenAI di un'apposita informativa di dettaglio e della messa a disposizione, sempre sul sito internet di OpenAI, di uno strumento attraverso il quale tutti gli interessati possono chiedere e ottenere la cancellazione dei propri dati personali.

La motivazione dell'esclusione degli adempimenti delle prescrizioni *sub* 8) e 9) dal novero di quelli condizionanti la sospensione del Primo provvedimento sembra essere di carattere temporale, e consistere nell'aspettativa che le prescrizioni da 1) a 7) possano adempiersi da parte di OpenAI entro il 30 aprile 2023, come effettivamente ritenuto e ordinato nel Secondo Provvedimento, nel quale, oltre alla disposizione della sospensione del Primo provvedimento, come sopra condizionata, si ingiunge ad OpenAI ai sensi dell'art. 58, par. 2, lett. d) del GDPR di adempiere alle varie prescrizioni da 1) a 9) nei predetti termini temporali, ossia: entro il 30 aprile 2023 per le prescrizioni da 1) a 7); ed entro i successivi termini per le prescrizioni da 8) a 9) come indicati specificamente nei medesimi punti: 31 maggio e 30 settembre per il punto 8) e 15 maggio per il punto 9).

Il contenuto del Secondo provvedimento si spiega in relazione al contenuto del Primo provvedimento nonché – deve ritenersi, almeno in qualche misura – in relazione agli incontri e alle interlocuzioni che il Garante ha avuto con OpenAI successivamente all'emanazione del Primo provvedimento, dei quali è dato atto nei comunicati stampa del Garante del 4.4.2023 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9872284), e del 6.4.2023 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9872832).

Nel Primo provvedimento, il Garante aveva motivato l'adozione "in via d'urgenza" dell'ordine di limitazione provvisoria sulla base della contestazione di una violazione degli artt. 5, 6, 8, 13 e 25 del GDPR, con la precisazione che tale valutazione doveva ritenersi compiuta sulla base dell'istruttoria fino a quel momento espletata e che la misura della limitazione provvisoria si giustificava "nelle more del completamento della necessaria istruttoria rispetto a quanto sin qui emerso".

Successivamente, in data 28.4.2023, OpenAI ha riaperto il servizio ChatGPT in Italia ritenendo di aver assolto alle richieste del Garante italiano, il quale, a sua volta, con comunicato in pari data, ha espresso soddisfazione per "*i passi in avanti*" compiuti da OpenAI, pur dichiarando che proseguirà nella sua istruttoria e nel lavoro con l'apposita task force costituita in seno allo *European Data Protection Board* con le altre Autorità privacy europee al livello dell'EDPB (v. notizia n. 3 *supra* in questa rubrica).
Nel predetto comunicato, il Garante italiano ha comunicato di aver ricevuto da OpenAI una nota nella quale la medesima società ha rappresentato di aver:

- predisposto e pubblicato sul proprio sito un'informativa rivolta a tutti gli utenti e non utenti, in Europa e nel resto del mondo, per illustrare quali dati personali e con quali modalità sono trattati per l'addestramento degli algoritmi e per ricordare che chiunque ha diritto di opporsi a tale trattamento;
- ampliato l'informativa sul trattamento dei dati riservata agli utenti del servizio rendendola ora accessibile anche nella maschera di registrazione prima che un utente si registri al servizio;
- riconosciuto a tutte le persone che vivono in Europa, anche non utenti, il diritto di opporsi a che i loro dati personali siano trattati per l'addestramento degli algoritmi anche attraverso un apposito modulo compilabile online e facilmente accessibile;
- introdotto una schermata di benvenuto alla riattivazione di ChatGPT in Italia, con i rimandi alla nuova informativa sulla privacy e alle modalità di trattamento dei dati personali per il training degli algoritmi;
- previsto per gli interessati la possibilità di far cancellare le informazioni ritenute errate dichiarandosi, allo stato, tecnicamente impossibilitata a correggere gli errori;
- chiarito, nell'informativa riservata agli utenti, che mentre continuerà a trattare taluni dati personali per garantire il corretto funzionamento del servizio sulla base del contratto, tratterà i loro dati personali ai fini dell'addestramento degli algoritmi, salvo che esercitino il diritto di opposizione, sulla base del legittimo interesse;
- implementato per gli utenti già nei giorni scorsi un modulo che consente a tutti gli utenti europei di esercitare il diritto di opposizione al trattamento dei propri dati personali e poter così escludere le conversazioni e la relativa cronologia dal training dei propri algoritmi;
- inserito nella schermata di benvenuto riservata agli utenti italiani già registrati al servizio un pulsante attraverso il quale, per riaccedere al servizio, dovranno dichiarare di essere maggiorenni o ultratredicenni e, in questo caso, di avere il consenso dei genitori;
- inserito nella maschera di registrazione al servizio la richiesta della data di nascita prevedendo un blocco alla registrazione per gli utenti infratredicenni e prevedendo, nell'ipotesi di utenti ultratredicenni ma minorenni che debbano confermare di avere il consenso dei genitori all'uso del servizio.

Su questa base, il Garante ha espresso soddisfazione per le misure intraprese e ha auspicato – sempre nel comunicato stampa - che OpenAI, nelle prossime settimane, ottemperi alle ulteriori richieste impartitele con lo stesso provvedimento dell'11 aprile con particolare riferimento all'implementazione di un sistema di verifica dell'età e alla pianificazione e realizzazione di una campagna di comunicazione finalizzata a informare tutti gli italiani di quanto accaduto e della possibilità di opporsi all'utilizzo dei propri dati personali ai fini dell'addestramento degli algoritmi.

SALVATORE ORLANDO

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490

6. I provvedimenti del 31.12.2022 e del 12.1.2023 adottati dalla Data Protection Commission irlandese in ottemperanza alle tre decisioni vincolanti dell'EDPB del 5.12.2022 nei casi concernenti Meta (per i servizi Facebook e Instagram) e WhatsApp (per l'omonimo servizio) a proposito della base del contratto per il trattamento dei dati personali.

L'ultimo giorno del 2022 l'Autorità di controllo irlandese in materia di protezione dei dati personali (la *Data Protection Commission*, "**DPC**") ha sanzionato Meta Platforms Ireland Limited ("**Meta**") per 210 milioni di euro con riferimento alla fornitura del suo servizio più famoso, il social network Facebook, per la violazione degli artt. 5(1)(a), 6(1)(b), 12(1) e 13(1)(c) del Regolamento UE 2016/679 (in seguito, anche, "Regolamento" o "GDPR"),

Tale pronuncia, insieme a quella "gemella", di pari data, contro Meta per il servizio Instagram , con una sanzione di 180 milioni di euro, acquisisce enorme importanza per le conclusioni che se ne traggono in materia di pubblicità personalizzata online. La scelta della base giuridica su cui fondare la profilazione per fini commerciali e pubblicitari è infatti centrale nel modello di business non solo di Meta ma della gran parte delle piattaforme digitali, ivi compresi gli editori, come le testate giornalistiche online, o gli altri fornitori di servizi, anche più piccoli.

Ecco perché, al di fuori delle conseguenze per Meta, la decisione avrà ripercussioni per tutti i fornitori di servizi digitali laddove suscettibile di mettere potenzialmente in crisi i modelli di business basati sull'offerta di servizi "gratuiti" o a "prezzo zero" e, quindi, di cambiare o quanto meno influire sul modo in cui i fornitori di servizi digitali remunerano la loro attività.

Il provvedimento segna la fine di una lunga istruttoria che ha avuto origine da un reclamo presentato il 25 maggio 2018, giorno della effettiva applicabilità del GDPR, contro le nuove condizioni contrattuali ("*Terms of Service*" o "TOS") e informativa privacy da poco adottate da Facebook. Tra gli aspetti di particolare interesse, si contestava la modifica della base giuridica per la fornitura di pubblicità comportamentale (*rectius*, del trattamento dei dati degli utenti per l'invio di una particolare forma di pubblicità personalizzata e particolarmente invasiva): dal consenso dell'interessato *ex* art. 6(1)(a) del Regolamento al contratto *ex* art. 6(1)(b) dello stesso Regolamento. In altre parole, l'invio di pubblicità comportamentale diveniva parte essenziale del servizio offerto dalla piattaforma Facebook e per questo assoggettato alla medesima base giuridica: il contratto con il fornitore del servizio così come regalato dai TOS. Dunque, per accedere o continuare a usufruire di Facebook bisognava "accettare" i TOS e, quindi, necessariamente anche la pubblicità comportamentale. Secondo Meta, infatti, la fornitura di pubblicità comportamentale è necessaria all'esecuzione del contratto con l'utente e quindi alla fornitura del servizio.

Con il reclamo, presentato con il supporto dell'associazione Noyb, si contestava l'effetto del mutamento della base giuridica: "costringere" gli utenti ad acconsentire al trattamento dei loro dati per fini di pubblicità comportamentale. L'utente non avrebbe più potuto scegliere se ricevere o meno pubblicità basata sulla profilazione della sua attività.

Nella sua bozza di decisione, condivisa con le altre autorità di controllo europee in base alla procedura del *One-Stop Shop* di cui agli artt. 60 e ss. del Regolamento, la DPC ha sostenuto che Meta: avesse violato le norme sulla trasparenza non avendo chiarito agli utenti quali fossero i trattamenti realizzati, le finalità e le relative basi giuridiche; che questa può scegliere la base giuridica che ritiene più adeguata per i trattamenti effettuati; e che, con riferimento ai servizi personalizzati, ivi compresa la pubblicità, Meta non era tenuta ad adottare il consenso e nello specifico aveva legittimamente scelto il contratto.

Questo perché, nella ricostruzione della DPC, il servizio Facebook è chiaramente basato sulla pubblicità personalizzata e un utente ragionevolmente informato è al corrente del fatto che il contenuto principale ("*core*") del modello Facebook è proprio la pubblicità comportamentale ("*an advertising model*"). Conseguentemente, tale forma di pubblicità integra un elemento essenziale del contratto che rientra nelle reciproche aspettative sia di Facebook che di un suo potenziale utente. Soprattutto, si tratta di un elemento necessario per dare esecuzione allo "specifico" contratto sottoscritto dalle parti nella misura in cui la necessità non può essere considerata del tutto in astratto ma bisogna tenere in considerazione le clausole contrattuali che in concreto delineano il funzionamento del servizio.

Sulla bozza di decisione si sono concentrate le "obiezioni pertinenti e motivate" (ex art. 65, par. 1, lett. a GDPR) delle autorità di controllo europee per le quali la pubblicità comportamentale, quale parte più ampia dei servizi personalizzati offerti da Facebook, non può fondarsi sul contratto perché si tratta di prestazioni non necessarie per l'esecuzione del servizio richiesto dall'utente.

Sulla base di tali obiezioni, il Comitato europeo per la protezione dei dati personali (EDPB), organo che riunisce a livello europeo i rappresentanti di tutte le autorità di controllo, ha emesso in data 5 dicembre 2022 una decisione vincolante ai sensi dell'art. 65 GDPR: la decisione n. 3/2022.

Similmente ha provveduto, nella stessa data, emettendo altre due decisioni vincolanti ai sensi dell'art. 65 GDPR: la n. 4/2022 relativa al servizio Instagram (decisione n. 4/2022), riguardante sempre la base del contratto come base giuridica del trattamento per finalità di pubblicità comportamentale; e la n.5/2022 relativa al servizio WhatsApp riguardante sempre la base del contratto come base giuridica del trattamento, in questo caso però in relazione alle particolare finalità dello sviluppo del servizio (*service improvement*) e della sicurezza (*security*).

Nella decisione 3/2022 l'EDPB ha innanzitutto rilevato come la pubblicità comportamentale sia un

trattamento complesso, su larga scala e intrusivo nella dimensione giuridica degli utenti, difficilmente compreso dagli stessi che spesso non ne sono al corrente e che, dall'altro lato, la disciplina in materia di protezione dei dati personali si fonda sul riconoscimento alla persona fisica del potere di controllo sui propri dati. In tal senso, le norme del Regolamento, ivi compresa la base giuridica contrattuale, non possono essere interpretate e applicate in modo da ridurre il potere di controllo sui dati da parte degli interessati perché così facendo si annullerebbe l'effetto utile delle norme a tutela dell'interessato.

Ciò premesso, ha affermato che la valutazione della "necessità" di un trattamento all'esecuzione del contratto deve essere effettuata in relazione alla *ratio* del contratto, vale a dire la sua sostanza e il suo obiettivo o finalità fondamentale. È dunque con riferimento alla finalità di un contratto che si misura la necessità del trattamento.

Per ricorrere al contratto come base giuridica *ex* art. 6(1)(b) del Regolamento bisogna che il trattamento sia oggettivamente necessario per la finalità perseguita e parte integrante della fornitura del servizio all'interessato.

Meta presenta il servizio Facebook come uno strumento che consente agli utenti di connettersi con i loro amici e comunicare con il mondo. In altre parole, dal punto di vista dell'utente la pubblicità comportamentale, laddove l'utente sia al corrente della sua presenza, non è comunque un elemento necessario del contratto.

Soprattutto, secondo l'EDPB è il modello di business che deve adattarsi e conformarsi ai requisiti che il GDPR stabilisce per il trattamento dei dati personali, non il contrario. In tal senso, la valutazione di ciò che è necessario deve tener conto anche di quale sia l'opzione meno invasiva per raggiungere lo stesso obiettivo. Se esistono alternative realistiche e meno invadenti, il trattamento non sarà "necessario" *ex* art. 6(1)(b) GDPR. Tale articolo, infatti, non è invocabile per trattamenti che sono solo "utili" ma non "oggettivamente necessari" per l'esecuzione della prestazione contrattuale, anche se ciò è necessario per altri scopi come quelli commerciali.

L'EDPB conclude quindi che, poiché l'obiettivo principale per cui un utente usufruisce del servizio Facebook è comunicare con gli altri, la pubblicità comportamentale ancorché inserita come obbligazione contrattuale, non è un trattamento oggettivamente necessario alla fornitura del servizio Facebook.

Pertanto, nel suo parere vincolante del 5 dicembre 2022, l'EDPB ha ritenuto che il contratto non fosse l'adeguata base giuridica per la pubblicità comportamentale con riferimento al servizio Facebook, che nella scelta di tale base giuridica Meta abbia violato le norme del Regolamento e ha imposto alla DPC di modificare la bozza di decisione in modo da recepire l'orientamento dell'EDPB.

In ottemperanza al parere dell'EDPB, nella sua decisione finale del 31 dicembre 2022, in aggiunta alle violazioni in materia di corretta informazione, la DPC ha stabilito che la scelta di ricorrere al contratto quale base giuridica per la pubblicità comportamentale costituisce una violazione dell'articolo 6 del GDPR.

Ha inoltre imposto a Meta di adeguare i suoi trattamenti alle norme del GDPR entro un periodo di 3 mesi.

La stessa misura è stata adottata nella decisione "gemella" della DPC del 31.12.2022 relativa al servizio Instagram, riguardante, come dichiarato dalla stessa DPC, "*the same basic issues*", e culminata anche in questo caso – e sulla base delle stesse argomentazioni sostanziali - nell'affermazione dell'inidoneità della base del contratto per il trattamento dei dati personali con particolare riferimento alla finalità della pubblicità comportamentale.

Invece, in ottemperanza alla richiamata decisione vincolante dell'EDPB n.5/2022, la DPC ha adottato il 12.1.2023 nei confronti di WhatsApp Ireland una decisione finale comminando una sanzione di 5,5 milioni di euro e imponendo in questo caso un termine maggiore, di 6 mesi, per rendere le sue operazioni di trattamento dei dati personali conformi al GDPR. Anche per il servizio WhatsApp la decisione vincolante dell'EDPB e la decisione finale della DPC sono culminate nell'affermazione dell'inidoneità della base del contratto per il trattamento dei dati personali, in questo caso, tuttavia, vertendosi in particolare, come detto, sulle diverse finalità dello sviluppo del servizio e della sicurezza.

Degno di nota, infine, che in entrambi i comunicati stampa emanati dalla DPC a commento dei provvedimenti in questione (un comunicato stampa per i provvedimenti contro Meta per i servizi Facebook e Instagram e l'altro per il provvedimento contro WhatsApp Ireland), si annuncia un ricorso della DPC alla Corte di Giustizia dell'Unione Europea per proporre una questione interpretativa sui poteri dello EDPB, in conseguenza del fatto che l'EDPB avrebbe, ad avviso della DPC, oltrepassato i suoi limiti di competenza nel sollecitare separatamente la DPC ad avviare nuove indagini sulle operazioni di trattamento dei dati relativi ai tre

servizi in oggetto (Facebook, Instagram e WhatsApp).

GUIDO D'IPPOLITO

Sul servizio Facebook:
https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland
https://edpb.europa.eu/system/files/2023-01/facebook-18-5-5_final_decision_redacted_en.pdf
https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf

Sul servizio Instagram:
https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland
https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf

Sul servizio WhatsApp:
https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-inquiry-whatsapp
https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf

7. La luce verde del 10.2.2023 della Commissione UE a una joint venture tra Deutsche Telekom, Orange, Telefónica e Vodafone per una piattaforma di supporto al marketing digitale in Francia, Germania, Italia, Spagna e Regno Unito

Con decisione del 10 febbraio 2023, la Commissione europea (di seguito, **Commissione**) ha approvato senza condizioni la creazione di una *joint venture* tra Deutsche Telekom AG, Orange SA, Telefónica S.A. e Vodafone Group plc. finalizzata a predisporre una piattaforma di supporto alle attività di marketing e pubblicità digitale di marchi ed editori in Francia, Germania, Italia, Spagna e Regno Unito.
Com'è noto, se, da un lato, le fusioni e le *joint ventures* tra imprese possono portare benefici all'economia, espandendo segmenti di mercato, efficientando lo sviluppo di nuovi prodotti e/o favorendo la riduzione dei costi di produzione o distribuzione, dall'altro esse possono, in potenza, ridurre il gioco concorrenziale, creando o rafforzando posizioni dominanti. Per tali ragioni, pur non figurando espressamente agli artt. 101 ss. TFUE, alle concentrazioni è stata destinata un'apposita disciplina di diritto derivato, condensata nel Regolamento (CE) n. 139/2004. Ai sensi dell'art. 4 di tale regolamento, alle imprese coinvolte è fatto obbligo di notificare alla Commissione le concentrazioni cc.dd. di dimensione comunitaria prima della loro realizzazione e dopo la conclusione dell'accordo, la comunicazione dell'offerta d'acquisto o di scambio o l'acquisizione di una partecipazione di controllo. Inoltre, la notificazione è ammessa anche quando le imprese interessate dimostrino di avere, in buona fede, intenzione di concludere un accordo o di procedere a un'offerta pubblica che dia luogo a una concentrazione di dimensione comunitaria. Ricevuta la notificazione, la Commissione procede all'esame dell'operazione, verificandone la compatibilità col mercato interno. In estrema sintesi, ai sensi dell'art. 6, gli esiti dell'indagine possono essere i seguenti: una decisione di non pertinenza dell'operazione all'ambito di applicazione del regolamento; una decisione di compatibilità della concentrazione col mercato comune; una decisione di compatibilità sottoposta a condizioni o oneri per le imprese partecipanti; in caso di seri dubbi sull'alterazione del gioco concorrenziale, l'avvio del procedimento, con esercizio dei poteri di cui all'art. 8; una decisione di rinvio dell'esame alle autorità competenti dello Stato membro interessato (art. 9).
Ebbene, in data 6 gennaio 2023 Deutsche Telekom, Orange, Telefónica e Vodafone, imprese operanti nel settore delle telecomunicazioni, hanno notificato alla Commissione l'intenzione di procedere alla creazione di una piattaforma di supporto alle attività di marketing e pubblicità digitale. Nello specifico, la *joint venture*, raccolto il previo consenso dell'utente, genererà un codice digitale unico derivato dall'abbonamento alla rete mobile o fissa dell'utente che consentirà ai marchi e agli editori di riconoscere gli utenti sui loro siti web o applicazioni su base pseudonima, di raggrupparli in diverse categorie e di adattare i loro contenuti a gruppi di utenti specifici.
Come anticipato, all'esito del pertinente esame, la Commissione ha concluso che l'operazione non solleva problemi di concorrenza nello Spazio economico europeo (SEE), adottando una decisione incondizionata di compatibilità della concentrazione col mercato comune ai sensi dell'art. 6, par. 1, lett. *b*) Regolamento (CE) n. 139/2004. L'indagine di mercato condotta dalla Commissione ha rivelato che l'operazione, come notificata, non ridurrebbe in

modo significativo la concorrenza nei mercati francese, tedesco, italiano e spagnolo con riferimento a: la fornitura di servizi di identificazione digitale per la pubblicità mirata e/o l'ottimizzazione dei siti; la fornitura al dettaglio di servizi di telecomunicazione mobile; la fornitura al dettaglio di servizi di accesso a internet fisso; la fornitura al dettaglio di servizi audiovisivi; la fornitura di spazi pubblicitari online. Di seguito, in sintesi, le ragioni.

Nel corso dell'indagine, è stato anzitutto esaminato il legame verticale tra le attività delle quattro società come fornitori al dettaglio di servizi di accesso a internet e alla rete mobile e i servizi di marketing e pubblicità digitale affidati alla *joint venture*. Le società forniscono a quest'ultima un codice digitale con il quale essa eroga i propri servizi di identificazione digitale per le attività di marketing e pubblicità digitale. Al riguardo, la Commissione ha ritenuto che, a seguito dell'operazione, vi sarebbero sufficienti fornitori alternativi di input per il medesimo scopo. Inoltre, si è constatato che i *competitors* delle imprese sarebbero in grado di fornire fattori di produzione alla stessa *joint venture* e/o ai fornitori rivali di servizi di identificazione digitale.

Oggetto di verifica è stato, poi, il legame verticale tra le attività delle quattro imprese come clienti di pubblicità online e le attività della *joint venture* quale fornitore di servizi di identificazione digitale per la pubblicità mirata e/o l'ottimizzazione dei siti. Sul punto, si è rilevato che la *joint venture* non avrà la capacità di – o costituirà l'incentivo a – escludere altri inserzionisti e fornitori rivali di servizi di telecomunicazione mobile, limitando il loro accesso ai servizi di identificazione digitale. Dipoi, le società non avrebbero la capacità di escludere fornitori rivali di servizi di identificazione digitale.

Inoltre, sono stati analizzati i legami conglomerati tra le attività delle società come distributori di canali televisivi e le attività della *joint venture* come fornitore di servizi di identificazione digitale per la pubblicità mirata e/o l'ottimizzazione dei siti. In proposito, la Commissione ha ritenuto che le società non avrebbero la capacità di – o l'incentivo a – costringere le emittenti televisive ad abbonarsi ai servizi di identificazione digitale offerti dalla *joint venture*, data la limitata platea di clienti comuni a questi due diversi prodotti.

Merita infine evidenziare che la Commissione ha dichiarato che le verifiche illustrate sono state condotte in costante contatto con le autorità preposte alla protezione dei dati personali, e che, in ogni caso, a prescindere dall'avvenuta autorizzazione alla fusione, le norme sulla protezione dei dati personali rimangono pienamente applicabili.

VALENTINO RAVAGNANI

https://ec.europa.eu/commission/presscorner/detail/%20en/ip_23_721

8. Il provvedimento della *Datenschutzconferenz* tedesca del 24.11.2022 contro Microsoft per il sistema di trattamento dati del cloud di Office 365.

Il 22 settembre 2020, la *Datenschutzkonferenz* (**DSK** o **Conferenza**) aveva preso atto di una valutazione compiuta da parte di un gruppo di lavoro da essa incaricato avente ad oggetto l'amministrazione dei termini di servizio online alla base dell'utilizzo del servizio cloud Microsoft Office 365 e l'allora vigente «Addendum relativo alla Protezione dei Dati Personali dei Servizi Online Microsoft» (*Microsoft Online Services Data Protection Addendum*, **DPA**: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2020) per quanto riguarda la sua conformità ai requisiti dell'art. 28, paragrafo 3, del Regolamento generale sulla protezione dei dati (UE) 2016/679 (**GDPR**), ai sensi del quale "i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento" e che prevede i requisiti di tale atto giuridico. La DSK è un'organizzazione composta dall'autorità indipendente per la protezione dei dati della Federazione tedesca e da quelle dei singoli Länder. La Conferenza ha il compito di salvaguardare il diritto alla protezione dei dati, di ottenere un'applicazione uniforme della legislazione europea e nazionale in materia di protezione dei dati e di promuovere congiuntamente il suo ulteriore sviluppo. I suoi strumenti sono risoluzioni, decisioni, linee guida, standardizzazione, dichiarazioni, comunicati stampa e indagini specifiche.

Più in particolare, il gruppo di lavoro incaricato dalla DSK costituisce una *task force*, sotto la guida

degli uffici delle autorità per la protezione dei dati di Brandeburgo e della Bavaria (BayLDA). Ad esso (innanzi anche il **Gruppo di lavoro**) la DSK chiede di effettuare delle indagini e verifiche sulla conformità della contrattualistica di aziende target rispetto alla normativa sulla protezione dei dati. Avendo il Gruppo di lavoro accertato che, sulla base dei documenti forniti da Microsoft, non fosse possibile utilizzare Office 365 in modo conforme ai requisiti in materia di protezione dei dati, la DSK ha richiesto di avviare colloqui con Microsoft al fine di ottenere tempestivamente miglioramenti e adeguamenti conformi alla protezione dei dati personali agli standard per i trasferimenti, come indicato dalla c.d. sentenza Schrems II della Corte di giustizia europea (su cui v. in questa rubrica la notizia n. 1 del numero 3/2020 http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf).

La questione essenziale per l'autorità di vigilanza tedesca era se le attività di trattamento dei dati personali da parte del responsabile fossero legittime e, in particolare, se il DPA, come contratto di trattamento ai sensi dell'art. 28 GDPR soddisfacesse i requisiti di cui al medesimo articolo. Il Gruppo di lavoro ha specificato, tuttavia, che il contenuto del suo rapporto si è limitato ad una valutazione che copre i soli requisiti legali del GDPR, e non ha ad oggetto il complessivo sistema di protezione dei dati del servizio cloud Microsoft 365. Non vi è difatti alcun esame tecnico indipendente da parte del Gruppo di lavoro e neppure un'analisi dei flussi di dati e dei trattamenti effettivamente effettuati o in corso. Di conseguenza, il rapporto del Gruppo di lavoro non fornisce un'analisi conclusiva e (naturalmente) non esclude un diverso risultato al mutare delle condizioni. La valutazione si basa sull'ultimo aggiornamento del DPA che Microsoft ha presentato nel settembre 2022 (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2022). Questa nuova versione, in risposta ai rilievi dal Gruppo di lavoro, apporta modifiche principalmente nell'area della formulazione contrattuale della responsabilità di Microsoft nel contesto del trattamento «per scopi commerciali legittimi».

Il 24 novembre 2022, con la pubblicazione del rapporto in commento, il Gruppo di lavoro ha accertato che i miglioramenti nei punti critici indicati siano stati solo lievi, specialmente per quanto riguarda la definizione dei tipi e delle finalità del trattamento. La questione centrale è stata quella di stabilire, in particolare, in quali casi Microsoft agisca come responsabile e in quali come titolare del trattamento. I responsabili del trattamento devono difatti essere in grado di adempiere in qualsiasi momento ai loro obblighi di rendicontazione ai sensi dell'art. 5, par. 2 GDPR. Quando si utilizza Microsoft 365, l'azienda non rivela però in dettaglio quali operazioni di trattamento avvengono per conto del cliente e quali per scopi propri. Restano dunque necessari miglioramenti, che dovrebbero mirare a descrivere l'oggetto del trattamento in modo completo e il più dettagliato possibile. Ciò potrebbe essere ottenuto, ad esempio, attraverso una specifica per il cliente sulla falsariga dell'Allegato II delle clausole contrattuali standard della Commissione ai sensi dell'art. 28, par. 7, GDPR.

Per quanto riguarda poi la responsabilità di Microsoft nel contesto del trattamento «per scopi commerciali legittimi», il Gruppo di lavoro è riuscito a ottenere modifiche solo modeste agli accordi contrattuali. Un esame attento della riformulazione contrattuale mostra, a parere del Gruppo di lavoro, che Microsoft sta mantenendo l'approccio di base del precedente modello normativo di concedersi diritti illimitati per alcune operazioni di trattamento per l'elaborazione dei dati personali. Non è ancora chiaro quali dati personali siano trattati nel contesto di quelle che Microsoft chiama «legittime finalità commerciali» o «attività commerciali». Non è inoltre chiara la base giuridica sulla quale avviene il trasferimento dei dati personali trattati per scopi di Microsoft. Lo stesso vale per dati come quelli telemetrici e diagnostici, che, a quanto risulta al gruppo di lavoro, Microsoft raccoglie su larga scala e di regola per i propri scopi. Il DPA del settembre 2022 contiene modifiche alle precedenti disposizioni che regolano la divulgazione dei dati forniti a Microsoft in qualità di incaricato del trattamento per i propri scopi commerciali «al fine di ottemperare agli obblighi di legge». Sebbene le modifiche contengano una nuova formulazione, il risultato è che i poteri rimangono ugualmente ampi. Ad esempio, il regolamento limita il diritto del cliente di dare istruzioni in merito alla divulgazione dei dati trattati per conto del cliente. L'Addendum consente le divulgazioni se sono richieste per legge o comunque descritte al suo interno. Tali divulgazioni non sono limitate alle istruzioni del responsabile del trattamento; pertanto, sono consentite ai sensi dell'art. 28, par. 3, lett. a), seconda frase, GDPR solo se sono limitate agli obblighi previsti dal diritto dell'Unione o degli Stati membri a cui Microsoft è soggetta. Ciò significa che l'obbligo di Microsoft di impartire istruzioni non soddisfa i requisiti minimi legali ai sensi del suddetto articolo del GDPR. Le

indagini del Gruppo di lavoro mostrano che Microsoft si riserva anche contrattualmente un diritto di comunicare informazioni di ampia portata, che, se esercitato, non soddisferebbe i requisiti di cui all'articolo 48 del GDPR.

Microsoft ha inoltre illustrato al Gruppo di lavoro le procedure di cancellazione dei dati personali. Le spiegazioni mostrano che, ad eccezione del caso del trattamento dei dati oggetto del contratto per finalità di «difesa informatica», il trattamento per finalità commerciali di Microsoft non dovrebbe estendere i periodi di cancellazione dei dati personali. Inoltre, la rielaborazione del "supplemento per la protezione dei dati" ha comportato modifiche anche per quanto riguarda la cancellazione, che tuttavia comportano ancora ambiguità e contraddizioni. Secondo la valutazione del Gruppo di lavoro, la struttura dell'obbligo di restituzione e cancellazione non soddisfa i requisiti legali dell'art. 28, par. 3, lettera g), seconda frase, GDPR. A causa dell'ambiguità del regolamento, i responsabili del trattamento possono essere ritenuti responsabili ai sensi dell'art. 5, par. 2 GDPR, in combinato disposto con l'art. 5, par. 1, lettera a) GDPR.

Gli ultimi rilievi attengono al subappalto nel trattamento e al trattamento dati in paesi terzi. Nonostante le riserve iniziali, Microsoft è stata convinta ad apportare adeguamenti organizzativi e contrattuali alla procedura, che in precedenza era stata concepita come obbligo di raccolta dei dati da parte del responsabile del trattamento. Il Gruppo di lavoro sottolinea che l'art. 28 par. 2 GDPR prevede che le informazioni del responsabile del trattamento «in merito a qualsiasi modifica prevista per quanto riguarda l'utilizzo o la sostituzione di altri incaricati del trattamento» devono contenere la specifica modifica prevista e non solo l'indicazione della generica possibilità di modifiche. L'esempio di e-mail di notifica fornito da Microsoft contiene, tuttavia, solo generiche informazioni sulle modifiche. L'elenco dei rapporti di subappalto presentato al gruppo di lavoro distingue anche essenzialmente il servizio o la funzionalità per cui i subappaltatori sono utilizzati e specifica la loro ubicazione e le categorie di dati a cui hanno accesso. In confronto, le clausole contrattuali standard fornite dalla Commissione UE forniscono informazioni molto più dettagliate sul nome, l'indirizzo e la persona da contattare degli altri responsabili (sub-responsabili), nonché una descrizione del rispettivo trattamento, che dovrebbe consentire una chiara delimitazione delle responsabilità dei vari sub-responsabili.

L'ultima versione del DPA contiene infine una disposizione secondo cui il cliente "autorizza Microsoft a trasferire (…) i Dati Personali negli Stati Uniti [d'America] o in qualunque altro paese in cui Microsoft o gli Altri suoi Responsabili del Trattamento sono presenti". Di conseguenza, le clausole contrattuali standard della Commissione UE del 2021 implementate da Microsoft si applicano a tutti i trasferimenti di dati personali. I colloqui del gruppo di lavoro con Microsoft hanno confermato che i dati personali sono in ogni caso trasferiti negli Stati Uniti d'America quando si utilizza Microsoft 365. Non è, dunque, possibile utilizzare il cloud senza trasferire i dati personali negli Stati Uniti d'America. A partire dal dicembre 2022, Microsoft intende offrire a tutti i clienti nell'area dell'UE la possibilità di memorizzare ed elaborare i dati dei clienti, i dati di supporto e altri dati personali dei clienti nell'area dell'UE come regola di *default*, vale a dire non senza eccezioni, ad esempio per determinate misure di sicurezza informatica ("Confine dei dati dell'UE"). Molti dei servizi inclusi in Microsoft 365 richiedono inoltre a Microsoft di accedere ai dati non criptati e non pseudonimizzati. L'opzione ovvia di criptare i dati elaborati non è sempre possibile, ad esempio se i dati devono essere visualizzati nel browser. Ciò significa che Microsoft ha regolarmente la possibilità di leggere i dati in chiaro per adempiere ai propri obblighi contrattuali. Si tratta quindi di una classica manifestazione del caso d'uso 6 dell'Allegato 2 delle Raccomandazioni 01/2020 del Comitato europeo per la protezione dei dati. Per questo caso d'uso, le autorità di controllo non sono ancora riuscite a individuare garanzie aggiuntive che possano portare alla liceità dell'esportazione dei dati. Le misure attualmente fornite da Microsoft nella sezione "Ubicazione dei dati a riposo" per l'archiviazione dei dati non portano all'esclusione di un trasferimento né giustificano garanzie sufficienti. Per quanto riguarda l'ulteriore trattamento (oltre alla conservazione), la sezione "Trasferimenti e localizzazione dei dati" non contiene alcuna dichiarazione sulla localizzazione dei dati. Anche le misure promesse da Microsoft nell'Addendum non sono idonee a compensare le carenze in materia di diritti fondamentali del diritto statunitense, valutate rispetto agli standard del diritto dell'UE. Inoltre, Microsoft si riserva anche contrattualmente il diritto di effettuare divulgazioni di ampia portata che, se attuate, non sarebbero conformi ai requisiti di cui all'articolo 48 GDPR.

In risposta alla valutazione della DSK, Microsoft ha diffuso un comunicato attraverso il quale si duole delle risultanze riscontrate, sottolineando il costante impegno dell'azienda nel trattamento e nella protezione dei dati dei propri utenti. Viene ribadito

che la DSK non avrebbe debitamente tenuto in conto le modifiche effettuate da Microsoft attraverso il DPA e che altre ne verranno realizzate, a garanzia della maggior trasparenza, come parte dell'EU *Data Boundary* per Microsoft Cloud. Il dibattito è dunque destinato ad evolversi con la diffusione del report completo delle violazioni riscontrate.

FEDERICO PISTELLI

https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

9. Le Linee Guida EDPB 3/2022 versione 2.0 del 14.2.2023 sui *deceptive design* (già *dark*) *patterns*

Il 14 febbraio 2023, l'*European Data Protection Board* (EDPB) ha adottato la versione 2.0 delle Linee guida 3/2022, dal titolo "*Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*" (le **Linee Guida**). La nuova versione aggiorna quella adottata circa un anno prima (14 marzo 2022) e presenta rilevanti novità, già a partire dal titolo, in cui l'espressione "*dark patterns*" viene sostituita con "*deceptive design patterns*".

Lo scopo delle Linee Guida è di fornire raccomandazioni e indicazioni per la progettazione delle interfacce delle piattaforme dei social media. Esse possono essere utilizzate sia nella fase di ideazione di una interfaccia utente, al fine di evitare l'implementazione di modelli di progettazione ingannevoli *ab origine*, sia su un servizio esistente, per valutarne la conformità della sua interfaccia, ovvero se *GDPR compliant*.

Nel contesto delle Linee Guida, i *deceptive design patterns* sono definiti come "interfacce degli utenti e percorsi degli utenti nelle piattaforme di *social media* che mirano a influenzare gli utenti al fine di indurli ad effettuare decisioni riguardanti il trattamento dei loro dati personali non consapevoli, non volute, potenzialmente dannose per gli utenti, sovente nella direzione di una scelta che risulta sfavorevole o non ottimale per gli interessi degli utenti e favorevole agli interessi delle piattaforme". Le Linee Guida aggiungono che l'influenza comportamentale esercitata dai *deceptive design patterns* si basa, generalmente, su *bias* cognitivi dell'utente, che si vede ostacolato nelle proprie capacità di assumere scelte che garantiscano la migliore protezione, in termini di efficacia, dei propri dati personali. Soluzioni di *design*, che vanno dalle scelte cromatiche al posizionamento dei contenuti, possono determinare scelte degli utenti in un senso diverso da quello che gli stessi perseguirebbero se non sottoposti a condizionamenti. Inoltre, questi modelli potrebbero comportare in aggiunta alla perdita di controllo sui propri dati personali, con conseguente violazione delle norme poste a tutela degli stessi, anche la violazione delle norme attigue sulla protezione dei consumatori.

L'EPDB individua sei principali categorie di deceptive design patterns (Annex I): *i) overloading*: agli utenti vengono fornite informazioni in eccesso per spingerli a fornire più dati personali del necessario; *ii) skipping*: l'interfaccia viene progettata in modo che gli utenti dimentichino o non prestino attenzione a tutti o ad alcuni aspetti della protezione dei propri dati; *iii) stirring*: influisce sulla scelta che gli utenti farebbero facendo appello alle proprie emozioni o utilizzando suggerimenti visivi; *iv) obstructing*: un ostacolo o un blocco degli utenti nel loro processo di informazione o gestione dei propri dati, rendendo l'azione difficile o impossibile da realizzare; *v) fickle*: il design dell'interfaccia è incoerente e non chiaro, rendendo difficile per gli utenti navigare tra i diversi strumenti di controllo della protezione dei dati e comprendere lo scopo del trattamento; *vi) left in the dark*: l'interfaccia viene progettata in modo da nascondere le informazioni o gli strumenti di controllo della protezione dei dati o per lasciare gli utenti nell'incertezza su come i loro dati vengono elaborati e sul tipo di controllo che potrebbero avere su di essi in merito all'esercizio dei loro diritti. Oltre all'individuazione di queste categorie corredate da esempi, le linee guida contengono una serie di *best practices* e di raccomandazioni (Annex II) per la progettazione di interfacce utente che facilitino l'effettiva implementazione del GDPR.

Il livello di dettaglio delle Linee Guida ha indotto alcuni commentatori a considerarle applicabili anche al di fuori del perimetro delle piattaforme di *social media*, configurandosi così come prima guida al *legal design* delle piattaforme, secondo un approccio *human-centred*.

LUCIO CASALINI

https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

10. La divulgazione del 30.1.2023 dei risultati dell'indagine a tappeto della Commissione europea e della rete CPC sulle pratiche di manipolazione online.

Il 30 gennaio 2023, la Commissione europea ha divulgato i risultati di una "indagine a tappeto" (*sweep*), come definita all'art. 3, n. 16 del regolamento (UE) 2017/2394, e cioè, una "*indagin*[e] *concertat*[a] *dei mercati al consumo attraverso azioni di controllo coordinate e simultanee volte a verificare la conformità o a individuare infrazioni delle norme dell'Unione sulla tutela degli interessi dei consumatori*", svolta dalla medesima Commissione e dalla rete di autorità nazionali per la tutela dei consumatori di 23 Stati Membri, Norvegia e Islanda (la "rete CPC", istituita con regolamento (CE) n. 2006/2004, così come abrogato e sostituito dal regolamento (UE) 2017/2394) che ha riguardato ben 399 siti *web* di vendita al dettaglio di prodotti tessili ed elettronici.
In particolare, l'indagine a tappeto – svolta ai sensi dell'art. 29 del regolamento (UE) 2017/2394 – si è dichiaratamente incentrata sull'analisi di tre tipi di pratiche manipolative o "modelli oscuri" (c.d. *dark patterns*), ossia – come si legge nel comunicato stampa della Commissione del 30.1.2023 – "pratiche che spingono sovente gli utenti della rete a compiere scelte che non si pongono necessariamente in linea con i loro interessi"; in particolare: *i)* "*fake countdown timers*", consistenti in conti alla rovescia fittizi, con scadenze per l'acquisto di specifici prodotti; *ii) "false hierarchy*", consistenti in interfacce *web* concepite per indurre e orientare i consumatori ad acquisti, abbonamenti o altre scelte; *iii) "hidden information*", consistenti nell'occultazione di informazioni importanti per i consumatori. Dai controlli effettuati dagli organi europei è emerso che 148 siti (e cioè, circa il 40% di quelli analizzati) si avvale di simili pratiche di manipolazione degli utenti al fine di trarre vantaggio dalle vulnerabilità dei consumatori mediante l'utilizzo di almeno uno dei predetti *dark patterns*. Segnatamente: 42 siti *web* utilizzano conti alla rovescia fittizi; 54 siti internet orientano i consumatori verso determinate scelte per mezzo della relativa progettazione visiva o comunque di scelte redazionali; 93 siti *online* occultano o rendono meno visibili informazioni importanti per i consumatori, quali i costi di consegna, la composizione dei prodotti, la disponibilità di alternative meno costose, ecc. L'indagine a tappeto, inoltre, ha interessato anche le *app* di 102 dei siti *web* controllati, riscontrando anche in 27 di esse la presenza di almeno una delle tre categorie di *dark pattern* poc'anzi citate.
Commentando tali risultati, il Commissario europeo per la giustizia, i diritti fondamentali e la cittadinanza, Didier Reynders, ha sollecitato l'attenzione degli Stati Membri su questa preoccupante situazione, affermando che "[a]*bbiamo già strumenti giuridicamente vincolanti per affrontare questi comportamenti e invito le autorità nazionali a fare uso dei loro poteri per contrastare con decisione queste pratiche*" e che "[p]*arallelamente, la Commissione sta rivedendo tutta la legislazione di tutela dei consumatori per garantire che sia adeguata all'era digitale e valutarne l'efficacia nel contrasto ai modelli oscuri*".
In particolare, la direttiva omnibus n. (UE) 2019/2161 (per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori) ha da tempo modificato gli strumenti esistenti in materia di tutela dei consumatori, incentivando la trasparenza in favore di chi effettua acquisti sui mercati *online*, andando a modificare e potenziare anche la direttiva 2011/83/UE sui diritti dei consumatori.
Per altro verso, con il regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali, recentemente approvato e denominato *Digital Services Act* (**DSA**) (v. in questa rubrica notizia n. 1 nel numero 4/2022: http://www.personaemercato.it/wp-content/uploads/2023/01/Osservatorio.pdf), il Legislatore europeo ha espressamente sanzionato le pratiche che – all'interno delle interfacce delle piattaforme *online* – sono volte a distorcere o compromettere in misura rilevante, intenzionalmente o di fatto, la capacità dei destinatari del servizio di compiere scelte o decisioni autonome e informate, con il fine di convincere i destinatari del servizio ad adottare comportamenti indesiderati o decisioni indesiderate che abbiano conseguenze negative per loro (v. Considerando n. 67 del DSA). In particolare, l'art. 25, par. 1 del DSA dispone che i "*fornitori di piattaforme online non progettano, organizzano o gestiscono le loro interfacce online in modo tale da ingannare o manipolare i destinatari dei loro servizi o da materialmente falsare o compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate*" e, in caso di violazione di tale divieto, gli Stati Membri possono infliggere delle sanzioni a carico dei fornitori di servizi (art. 52 DSA) ferma restando l'applicazione della legislazione adottata dagli Stati Membri in attuazione della direttiva 2005/29/CE

sulle pratiche commerciali sleali e l'applicazione del regolamento (UE) 2016/679 (GDPR) (cfr. ancora Considerando 67 e art. 25 par. 2 DSA). Si ricorda in proposito anche che, ai sensi del par. 3 del medesimo art. 25 DSA, la Commissione "*può emanare orientamenti sull'applicazione del paragrafo 1 con riguardo a pratiche specifiche, in particolare: a) attribuire maggiore rilevanza visiva ad alcune scelte quando si richiede al destinatario del servizio di prendere una decisione; b) chiedere ripetutamente che un destinatario del servizio effettui una scelta laddove tale scelta sia già stata fatta, specialmente presentando pop-up che interferiscano con l'esperienza dell'utente; c) rendere la procedura di disdetta di un servizio più difficile della sottoscrizione dello stesso*".

Tornando ai risultati dell'indagine a tappeto in commento, ora le autorità della rete CPC inviteranno gli operatori interessati a mettere in regola i loro siti *web* e, se necessario, adotteranno ulteriori misure in conformità con le procedure nazionali. Inoltre, la Commissione contatterà anche gli operatori commerciali individuati nello studio sulle pratiche commerciali sleali condotto nel 2022 (il cui *report* finale è disponibile qui: https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418) per chiedere loro di rimediare ai problemi messi in luce dai controlli.

Infine, la Commissione ha indetto una consultazione pubblica finalizzata a raccogliere contributi su tre direttive relative alla tutela dei consumatori (e cioè: la direttiva 2005/29/CE sulle pratiche commerciali sleali; la direttiva 2011/83/UE sui diritti dei consumatori; nonché, la direttiva 93/13/CEE sulle clausole abusive nei contratti) al fine di determinare se esse garantiscono un adeguato livello di protezione dell'utente nel c.d. ambiente digitale. Attendiamo, dunque, con interesse i risultati di tale consultazione, non ancora pubblicati alla data del presente contributo.

RICCARDO ALFONSI

https://ec.europa.eu/commission/presscorner/detail/it/ip_23_418

11. Le conclusioni rassegnate il 16.3.2023 dall'Avvocato generale della Corte di Giustizia UE nella causa C-634/21 (OQ vs Land Hassen; Schufa) sull'articolo 22 GDPR

Lo scorso 16 marzo sono state depositate le conclusioni dell'Avvocato Generale Priit Pikamäe nella causa pendente presso la Corte di Giustizia dell'Unione Europea (CGUE) C-634/21 che origina da un rinvio pregiudiziale, proposto dal Tribunale amministrativo di Wiesbaden l'1.10.2021 e che concerne l'interpretazione degli artt. 6(1) e 22(1) del GDPR. Si tratta del primo procedimento pendente davanti alla CGUE in relazione all'art. 22 GDPR, disposizione che costituisce una delle norme del GDPR più discusse dalla dottrina europea.

Il giudice tedesco che ha operato il rinvio alla CGUE è chiamato a pronunciarsi rispetto alla decisione del garante per la protezione dei dati del Land Assia (dall'*Hessischer Beauftragter für Datenschutz und Informationsfreiheit*, "**HBDI**"). In questa decisione HBDI ha ritenuto il rifiuto da parte di una società privata di valutazione della solvibilità di terzi (SCHUFA Holding AG ("**SCHUFA**") di dare seguito alla richiesta avanzata da una persona fisica, la ricorrente OQ ("**ricorrente**"), conforme al diritto tedesco. Dopo che un istituto di credito aveva respinto la sua domanda sulla base della valutazione fornita da SCHUFA, la ricorrente aveva infatti chiesto di avere accesso ai dati che la riguardano, cancellare quelli inesatti, e di ricevere informazioni circa le modalità con cui SCHUFA aveva valutato il suo *credit scoring*. In risposta, SCHUFA si era limitata a comunicare, in termini generali, alla ricorrente il funzionamento basilare del suo calcolo del punteggio di *scoring*, senza però indicare le singole informazioni incluse nel calcolo e il loro peso. SCHUFA ha ritenuto di non essere obbligata a rivelare i metodi di calcolo, poiché questi sarebbero coperti da segreto industriale e commerciale.

Nell'ambito del giudizio proposto davanti al tribunale amministrativo competente contro il provvedimento dell'HBDI che ha respinto le doglianze della ricorrente, il giudice tedesco ha formulato due quesiti alla CGUE. Qui rileva il primo, in cui si domanda se l'articolo 22, paragrafo 1, del GDPR debba essere interpretato nel senso che il calcolo automatizzato di un tasso di probabilità relativo alla capacità di un interessato di saldare in futuro un debito costituisce già una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici che riguardano l'interessato o che incide in modo analogo significativamente sulla sua persona, qualora tale tasso, calcolato sulla base di dati personali relativi all'interessato, sia trasmesso dal titolare del trattamento a un terzo titolare del trattamento e quest'ultimo basi prevalentemente su tale tasso la sua decisione sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con l'interessato. Nelle proprie conclusioni,

l'Avvocato Generale Pikamäe, già Presidente della Corte Suprema estone e docente presso l'Università di Tartu, risponde positivamente a simile quesito.
Egli afferma innanzitutto che, malgrado la terminologia impiegata, l'applicazione dell'articolo 22, paragrafo 1, del GDPR non richiede che l'interessato invochi attivamente il diritto e che, alla luce dei paragrafi successivi e del considerando 71 del GDPR, la disposizione *de qua* prevede un divieto generale, teso a "a tutelare le persone fisiche dagli effetti potenzialmente discriminatori e iniqui dei trattamenti automatizzati dei dati". Tale conclusione circa la natura di divieto, come noto, è condivisa da diversi autori e anche dall'EDPB (*European Data Protection Board*) che ha approvato le Linee Guida elaborate in tema nel 2018 dal "Gruppo di Lavoro Articolo 29 per la protezione dei dati" (cfr. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en e *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* del 22 agosto 2018: https://ec.europa.eu/newsroom/article29/items/612053).
Prima di affermare la possibilità di applicare l'art. 22(1) GDPR al procedimento decisionale inerente alla richiesta di credito della ricorrente, l'Avvocato Generale Pikamäe si è soffermato sull'analisi dei vari presupposti. L'ambito operativo del divieto è infatti segnato dall'art. 22(1) GDPR, il quale richiama la "decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici che riguardano l'interessato o che incide in modo analogo significativamente sulla sua persona". Per ciò che concerne la "decisione", l'Avvocato Generale Pikamäe, rilevata l'assenza di una definizione, suggerisce che "il legislatore dell'Unione abbia optato per una nozione ampia, idonea a ricomprendere una molteplicità di atti che possono incidere sull'interessato in diversi modi". Per quanto riguarda, invece, la richiesta che la decisione in questione produca "effetti giuridici" che riguardano l'interessato o che "incida in modo analogo significativamente sulla sua persona", l'Avvocato Generale Pikamäe ritiene che con simili formule si faccia riferimento alla circostanza per cui gli effetti della decisione abbiano "ripercussioni gravi".
Considerato che tali presupposti ricorrono anche nella vicenda descritta *supra*, l'Avvocato Generale Pikamäe ritiene che al quesito sollevato dal Tribunale amministrativo di Wiesbaden si possa rispondere affermando che l'art. 22(1) GDPR sia da considerarsi applicabile in circostanze quali quelle di cui al procedimento principale. In modo opportuno, l'Avvocato Generale Pikamäe ha infatti escluso che l'essere la valutazione automatizzata di *credit scoring* formulata da un soggetto diverso dall'istituto di credito che ha negato l'erogazione del credito possa escludere l'applicazione dell'art. 22 GDPR. A tal proposito, egli afferma che l'aspetto essenziale è quello di stabilire se il processo decisionale sia concepito con modalità tali per cui il calcolo del punteggio di *scoring* da parte dell'agenzia di valutazione del credito predetermina la decisione dell'istituto finanziario di concedere o negare il credito. In particolare, se lo *scoring* deve essere compiuto senza alcun intervento umano che possa, se del caso, verificare il suo risultato e la correttezza della decisione da adottare nei confronti del soggetto che richiede il credito, sembra logico all'Avvocato Generale Pikamäe ritenere che costituisca esso stesso la «decisione» di cui all'articolo 22, paragrafo 1, del GDPR.
La decisione della CGUE sulla questione pregiudiziale sollevata dal giudice tedesco è prevista entro la fine del 2023.

DANIELE IMBRUGLIA

urly.it/3tdyn

12. Il provvedimento cautelare del Garante privacy italiano del 2.2.2023 sulla *chatbot* Replika

Con provvedimento del 2 febbraio 2023 n. 39, l'Autorità garante per la protezione dei dati personali ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati personali degli utenti stabiliti nel territorio italiano, nei confronti della società statunitense Luka Inc., sviluppatrice e gestrice della chatbot "Replika", in considerazione dei concreti rischi che l'impiego di tale app presenta nei confronti dei minori di età e dei soggetti più fragili dal punto di vista emotivo.
"Replika" è una applicazione di intelligenza artificiale di tipo conversazionale che genera un personaggio virtuale programmato per instaurare conversazioni, quasi del tutto realistiche, con gli utenti e per stringere con essi legami di amicizia o anche sentimentali. Tale applicazione è stata presentata dagli stessi sviluppatori come "capace di migliorare l'umore ed il benessere emotivo dell'utente, aiutandolo a comprendere i suoi pensieri e i suoi sentimenti, a tenere traccia del suo umore, ad apprendere capacità di *coping* - ossia, di controllo dello stress - a calmare l'ansia e a lavorare

verso obiettivi come il pensiero positivo, la gestione dello stress, la socializzazione e la ricerca dell'amore". Le *chatbot* sono infatti programmi per computer che utilizzano gli algoritmi di intelligenza artificiale per restituire un dialogo strutturato all'utente, simulando ed elaborando conversazioni umane (testuali o vocali), consentendo agli utenti di interagire con il sistema digitale come se stessero conversando con una persona reale. In base poi al grado di sviluppo del software possono simulare legami emotivi complessi, al punto da turbare, se non determinare disagi psicologici importanti agli utenti, specialmente quando sono coinvolti soggetti particolarmente vulnerabili.

Proprio avendo riguardo a tali soggetti, l'Autorità garante ha avviato un'istruttoria nei confronti della società statunitense che ha sviluppato la suddetta applicazione, dopo aver acquisito alcune informazioni, da diversi articoli di stampa, che avrebbero dato evidenza dei concreti rischi legati all'impiego della chatbot nei confronti dei minori d'età e delle persone in stato di fragilità emotiva.

Durante l'istruttoria sono emerse diverse criticità. Da un lato si è appurato che il titolare del trattamento (ora nella 'privacy policy', ora negli 'app store') dopo aver dato atto della classificazione dell'applicazione come idonea a persone maggiori di 17 anni, dichiara di precludere ai soggetti di età inferiore a 13 anni l'uso dell'applicazione, di consentirlo ai minori di 18 anni solo previa autorizzazione dei genitori o tutori, di non raccogliere, conseguentemente, i dati personali dei soggetti di età inferiore a 13 anni, di incoraggiare comunque i genitori e i tutori legali a monitorare l'utilizzo di Internet da parte dei propri figli e ad istruire i minori a non fornire mai i dati personali sul servizio senza la loro autorizzazione. Tuttavia, dall'altro lato, si è constatata l'assenza di procedure di verifica e di controllo dell'età dell'utente, dal momento che il sistema si limita a chiedere solamente il nome, l'email e il genere. Ciò pertanto consente anche ai "piccoli minori" (di età inferiore ai 14 anni) di accedere al servizio e conversare con la chatbot senza il consenso dei genitori, con il rischio di risultare esposti a 'risposte' e contenuti non adatti alla loro età. Inoltre, anche nei casi in cui l'utente espliciti la sua minore età, non sono previsti meccanismi di filtro o di blocco con riguardo alle 'risposte' della chatbot e ai contenuti che risultano inidonei al grado di sviluppo e di consapevolezza di certi utenti o comunque inopportuni. A tale ultimo riguardo il Garante ha verificato che in diverse recensioni pubblicate all'interno dei due principali 'app store', gli utenti hanno segnalato e lamentato la presenza, nelle risposte fornite dalla chatbot, di contenuti sessualmente inopportuni.

Il Garante inoltre ha rilevato come le caratteristiche intrinseche della suddetta chatbot, come descritte nello stesso sito web, intervenendo sull'umore delle persone "possono risultare idonee ad accrescere i rischi per i soggetti fragili coinvolti", quindi anche a prescindere dall'età dell'utente.

Alla luce di quanto sopra evidenziato, il Garante ha ritenuto l'informativa privacy contenuta nel sito web dello sviluppatore non conforme ai principi e agli obblighi previsti dal GDPR in tema di trasparenza del trattamento, non essendo menzionati gli elementi essenziali del trattamento con riferimento ai dati personali dei minori. Ciò non consente di individuare la base giuridica delle varie operazioni di trattamento effettuate dalla menzionata chatbot, tenendo conto che il consenso non può considerarsi idonea base giuridica quando riferito ai minori, i quali non hanno la capacità di concludere i contratti. Al riguardo si precisa come le disposizioni sul c.d. consenso digitale del minore (di cui agli artt. 8 GDPR e 2-*quinquies* Codice della privacy) non trovano applicazione nel caso di specie non ricorrendone i presupposti: il servizio offerto dalla app Replika, come del resto riconosciuto dagli stessi sviluppatori, non rientra infatti nell'ambito dell'offerta dei servizi diretta ai minori di età, in ragione del fatto che implica una rilevante messa a disposizione dei dati personali degli utenti; né tantomeno, per la medesima ragione, l'atto di disposizione del consenso al trattamento dei dati personali potrebbe rientrare fra i cosiddetti atti minuti della vita quotidiana, in relazione, e nei limiti dei quali, il nostro ordinamento "ammette" i minori a concludere un contratto.

In considerazione quindi dell'assenza di qualsivoglia meccanismo di verifica dell'età degli utenti, nonché delle violazioni rilevate, il Garante ha motivatamente ritenuto di disporre, con effetto immediato, la limitazione provvisoria del trattamento di tutti i dati personali degli utenti stabiliti nel territorio italiano, invitando la società statunitense Luka Inc. a comunicare entro 20 giorni al Garante le misure intraprese per garantire il rispetto dei principi sanciti dal GDPR. In caso di mancato riscontro la sanzione può arrivare fino al 4% del fatturato annuo globale o a 20 milioni di euro (come previsto dall'art. 83, par. 5, lett. e), del Regolamento (UE) 2016/679).

ILARIA GARACI

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852506

13. L'avvio di istruttoria AGCM del 21.3.2023 nei confronti di TikTok per omessa predisposizione di adeguati sistemi di monitoraggio dei contenuti pubblicati da terzi (il caso della "cicatrice francese")

Il 21 marzo 2023 l'Autorità Garante della Concorrenza e del Mercato (di seguito **AGCM** o l'**Autorità**) ha avviato un'istruttoria nei confronti della società irlandese TikTok Technology Limited (**TikTok**), attiva nel settore dei social media attraverso la piattaforma TikTok e responsabile dei rapporti con i consumatori europei, nonché nei confronti della società inglese e di quella italiana dell'omonimo gruppo.

L'AGCM ha contestato a TikTok la mancata predisposizione di adeguati sistemi di monitoraggio per vigilare i contenuti pubblicati dei terzi, secondo i parametri di diligenza richiesti dalla normativa di settore, nonché dalle Linee guida adottate dalla stessa TikTok, che contemplano la rimozione di contenuti pericolosi che istigano al suicidio, all'autolesionismo e ad una alimentazione scorretta. Secondo l'Autorità, tali controlli devono essere effettuati in maniera ancor più rigorosa in presenza di fruitori del servizio particolarmente vulnerabili quali i minori.

L'AGCM ha deciso di avviare l'istruttoria a seguito della presenza sulla piattaforma TikTok di numerosi video di ragazzi, perlopiù minorenni, che adottano comportamenti autolesionistici; da ultimo, è diventata virale la c.d. sfida della "cicatrice francese". Si tratta di un nuovo trend (nato in Francia, da cui il nome) che vede coinvolti soprattutto gli utenti più giovani e che consiste nel mostrare i segni di cicatrici sul viso, una sfida apparentemente innocua che però può portare a conseguenze dannose e permanenti.

La sfida della "cicatrice francese" non è certo il primo comportamento pericoloso a guadagnare popolarità su TikTok (ad esempio, in passato era in voga la c.d. "*Blackout Challenge*", che consisteva nel trattenere il respiro fino a svenire; la c.d. "*Skull Breaker Challenge*", che prevedeva di far cadere una persona facendole perdere l'equilibrio; o la c.d. "*Fire Challenge*", che comportava l'accensione di fiammiferi o accendini vicino al viso). Non a caso, già nel gennaio 2021 il Garante italiano per la protezione dei dati personali – dopo aver aperto una istruttoria nel dicembre 2020 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923)– aveva disposto il blocco dell'uso dei dati degli utenti per i quali non fosse stata accertata l'età anagrafica (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/952422). Il provvedimento di blocco era stato adottato a seguito della morte di una bambina siciliana di 10 anni, avvenuta dopo la riproduzione di una sfida condivisa tra gli utenti della piattaforma che prevedeva il tentativo di soffocamento dell'utente tramite una cintura attorno al collo. Per rispondere alle preoccupazioni del Garante Privacy, TikTok ha adottato misure per bloccare l'accesso agli utenti minori di 13 anni e lanciato una campagna informativa per sensibilizzare genitori e figli. Ma, a quanto pare, ciò non è stato sufficiente ad evitare la diffusione di altri comportamenti pericolosi fra i più giovani.

Come è noto, la piattaforma TikTok gode di ampia popolarità, in costante crescita, soprattutto presso i più giovani. La sua fruizione è semplice e immediata, sia per caricare e pubblicare video sia per visionarne i contenuti, che sono proposti tramite una profilazione delle abitudini di navigazione degli utenti, dei like, delle pagine seguite, sulla base di un processo di elaborazione algoritmica.

L'AGCM ha contestato anche lo sfruttamento di tecniche di intelligenza artificiale suscettibili di provocare un indebito condizionamento dell'utenza (art. 18, co.1, lett *l)* c. cons.). In particolare, viene messo in discussione l'utilizzo dell'algoritmo sotteso al funzionamento della piattaforma che, adoperando i dati degli utenti, personalizza la visualizzazione della pubblicità e ripropone contenuti simili a quelli già visualizzati e con cui si è interagito attraverso la funzione dei *like* (nella specie contenuti autolesionistici).

Occorrerà monitorare il caso per verificare se TikTok presenterà impegni, per tentare di chiudere il caso senza accertamento dell'infrazione e senza sanzione, ovvero se l'AGCM deciderà di condurre l'istruttoria fino in fondo.

GIORGIA DIOTALLEVI

https://www.agcm.it/media-e-comunicazione/dettaglio?id=6d0b4104-3c73-4d5c-bf03-e7ae0bdce304

14. Il provvedimento del Garante privacy italiano del 24.11.2022 contro Areti sull'esattezza dei dati personali

Il 24 novembre 2022 il Garante per la protezione dei dati personali (il **Garante**) ha sanzionato per 1 milione di euro Areti S.p.a., società distributrice di energia elettrica, per lo scorretto trattamento dei dati personali dei suoi utenti. Nello specifico, il Garante ha accertato la violazione dei principi di esattezza del dato e di limitazione della conservazione (art. 5, par. 1, lett. d) ed e), Reg. UE 2016/679 o "GDPR"), il principio di *accountability* (art. 5, par. 2 e art. 24, GDPR) e l'omesso idoneo riscontro alla richiesta di accesso ai dati del reclamante (artt. 12, par. 3, e 15, GDPR).

Tale pronuncia acquisisce importanza soprattutto per quanto statuito in relazione al principio di esattezza dei dati personali. Principio che presidia la qualità delle informazioni e imprescindibile soprattutto quando queste sono alla base di una valutazione sulle persone e che, in considerazione del sempre più ampio ricorso ad algoritmi predittivi e sistemi di intelligenza artificiale, è destinato ad avere importanza strategica nella società digitale. È, infatti, un principio centrale anche nella proposta regolamentazione europea dell'intelligenza artificiale (*AI Act*) dove si evidenza la necessità di avere dati "neutrali", non portatori di pregiudizi inconsci (c.d. *bias*).

La sanzione ha avuto origine dal reclamo di un utente che lamentava di essere considerato dalla società distributrice di energia elettrica quale debitore "moroso" nonostante avesse provveduto a saldare quanto dovuto.

Il Garante ha così accertato che, a causa di una serie di errori tecnici ed applicativi nei sistemi interni della società, la stessa, dal dicembre 2016 al gennaio 2022, ha attribuito al reclamante e ad altri 16mila utenti e clienti finali una condizione di morosità non corrispondente al vero.

Tale erronea qualificazione ha prodotto alcuni pregiudizi tra cui l'impossibilità di cambiare gestore perché, in base alla normativa di settore, l'attribuzione della qualifica di moroso consentiva ai nuovi fornitori di energia di negare l'attivazione presso gli stessi di nuove forniture di energia elettrica (nel provvedimento il Garante ha accertato il mancato perfezionamento, per esercizio del diritto di revoca del venditore entrante, di circa 47mila richieste di "*switching*"), oltre a pregiudizi di natura economica conseguenti dalla perdita del potenziale risparmio per il passaggio a nuovo operatore.

L'illiceità e dannosità del trattamento deriva proprio dal mancato rispetto del principio di esattezza dei dati personali. Affinché una valutazione non produca danni sulla persona è necessario che i dati perosnali alla base del trattamento siano sempre esatti e l'interessato abbia la possibilità di rettificarli o aggiornarli. I dati personali divenuti obsoleti devono essere cancellati, cosa non avvenuta correttamente tanto da spingere il Garante a contestare alla società anche l'inadeguatezza delle tempistiche di conservazione dei dati.

Il rispetto del principio di esattezza serve quindi a consentire il trattamento di dati personali della massima qualità possibile e si pone come imprescindibile tutela quando le valutazioni sulle persone sono poste in essere da trattamenti interamente automatizzati (che se produttivi di effetti giuridici o significativi sulla persona sono subordinati alla più rigida disciplina dell'art. 22 GDPR) come i sistemi di intelligenza artificiale.

Si tratta, quindi, di un provvedimento di estremo interesse perché evidenzia i rischi e individua i principi da rispettare nel caso, sempre più diffuso, di trattamenti di "*rating*" o "*scoring*", ossia in tutti quei casi in cui si attribuiscono agli interessati etichette, qualifiche o punteggi da cui far derivare conseguenze che incidono sulla "reputazione" della persona, col rischio di creare vere e proprie forme di discriminazioni sociali. Tali rischi aumentano se i trattamenti di *rating* vengono effettuati con sistemi interamente automatizzati o di intelligenza artificiale.

Il provvedimento si inserisce nel filone di attività svolte dal Garante dinanzi trattamenti reputazionali illeciti: a partire dall'algoritmo di rating di Mevaluate (prov. n. 488 del 24 novembre 2016, doc. web n. 5796783), caso arrivato fino alla Corte di Cassazione che, con ordinanza n. 14381 del 25 maggio 2021, ha ribadito l'importanza di un'adeguata trasparenza e informazione sulle caratteristiche dell'algoritmo (sul caso Mevaluate v. su questa rubrica, la notizia n. 2 del numero 3/2021: http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf), fino ai sistemi di sorveglianza biometrica, come nel parere sfavorevole del Garante sull'utilizzo del sistema di riconoscimento facciale "Sari Real Time" da parte del Ministero dell'interno (su cui v. in questa rubrica la notizia n. 3 del numero 2/2021: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf) o le più recenti indagini nei confronti di alcuni comuni italiani intenzionati ad adottare sistemi di "*social scoring*", ossia meccanismi di profilazione che producono una sorta di "cittadinanza a punti", in base alle loro azioni si possono attribuire dei punteggi ai cittadini dai quali possono derivare conseguenze giuridiche positive o negative (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9778361).

Il provvedimento evidenzia così, in maniera chiara e semplice, i pregiudizi di un'errata valutazione dell'interessato: il vedersi attribuiti una qualifica o

reputazione non veritiera e produttiva di pregiudizi che possono generare conseguenze ingiustificate o discriminazioni. Rischi destinati ad aumentare se tali trattamenti sono svolti da algoritmi o sistemi di intelligenza artificiale al di fuori di qualunque supervisione umana.
In conclusione, se da un lato questo provvedimento mette in luce una tutela "pratica" e "consumeristica" della protezione dei dati personali, perché a garanzia dell'utente, dall'altro rende evidente perché strutturare il trattamento dei dati personali in modo corretto è molto più di una tutela dell'utente, bensì una tutela della persona e dei suoi spazi di libertà.
Tutela sempre più necessaria in una società governata da sistemi automatizzati che gestiscono ogni aspetto della vita umana: dal suggerimento di contenuti di interesse, all'acquisto di beni e svolgimento di attività sulle piattaforme fino alla possibilità di esercitare diritti o accedere a servizi pubblici.

GUIDO D'IPPOLITO

www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9832979

15. La relazione di ENISA del gennaio 2023 sull'ingegnerizzazione della condivisione dei dati personali con particolare focus sui dati del settore sanitario

Il 27 gennaio 2023 l'ENISA (*European Agency for Cybersecurity*) ha pubblicato il report intitolato "*Engineering Personal Data Sharing - Emerging Use Cases and Technologies*", riguardante la progettazione di tecnologie e le tecniche specifiche per consentire la condivisione dei dati personali nel pieno rispetto della privacy e del GDPR, in particolare applicato al settore sanitario. Il lavoro è frutto della collaborazione con il gruppo di lavoro *ad hoc* dell'ENISA sull'ingegneria della protezione dei dati personali.
L'Agenzia rileva un aumento della quantità di dati generati, elaborati e successivamente condivisi negli ultimi venti anni, indicando come naturale la tendenza a "portare i dati fuori dai dispositivi o dalle organizzazioni" e a condividerli tra diverse parti per uno scopo specifico al fine di creare nuovo valore per le persone e per la nostra società o semplicemente per ridurre i costi operativi.
Dall'analisi emerge che, considerando solo l'area dei 27 paesi europei, il valore dei dati nel 2025 sarà di 829 miliardi di euro, rispetto ai 301 miliardi di euro (2,4% PIL dell'UE) del 2018.
Il legislatore europeo è attualmente interessato a sviluppare la potenzialità della condivisione settoriale e intersettoriale dei dati a vantaggio di privati e imprese, mirando a renderli disponibili, anche tramite la regolazione del loro riutilizzo e facilitando questo processo mediante la creazione di nuovi intermediari e di ambienti di condivisione in cui le parti coinvolte possono mettere in comune dati e strutture.
Ottenere e garantire una solida *governance*, nonché tutele efficaci per i diritti delle persone fisiche si rivela essere fondamentale nell'ecosistema di condivisione delle informazioni, in quanto la protezione dei dati personali costituisce la base su cui si fonda la fiducia sia degli individui che delle organizzazioni. Insieme alla regolamentazione, il report individua come centrale il ruolo dell'"ingegneria della protezione dei dati", strumento adatto a tradurre in concreto i principi della privacy by Design e by Default previsti dall'art. 25 GDPR.
L'ENISA si concentra soprattutto sui casi d'uso nel settore sanitario, sebbene le tecnologie e le tecniche presentate siano ugualmente applicabili anche ad altri ambiti, con l'obiettivo di mostrare come i principi di protezione dei dati possano essere rispettati attraverso l'uso appropriato di soluzioni tecnologiche basate su tecniche crittografiche avanzate. Il settore della salute si presta in modo ottimale a rappresentare il terreno fertile per la condivisione dei dati, rappresentando un'opportunità di sviluppo notevole: il coordinamento e la collaborazione tra gli enti sanitari pubblici e privati, infatti, potrebbe portare a notevoli vantaggi sotto vari profili. A livello istituzionale, la condivisione comporterebbe un generale miglioramento del sistema sanitario, in quanto a livello individuale avrebbe come risultato quello di fornire ai cittadini un'assistenza sanitaria personalizzata ed efficace. Inoltre, a livello collettivo si favorirebbe la conduzione di ricerche scientifiche (compresi gli studi clinici) inerenti la distribuzione nella popolazione di patologie e fattori di rischio e sull'efficacia delle terapie disponibili.
La condivisione, anche transfrontaliera, dei dati sanitari comporta, tuttavia, la necessità di soddisfare i requisiti essenziali del GDPR al fine di ottenere una condivisione che permetta, allo stesso tempo, all'interessato di mantenere un controllo sulle proprie informazioni. I principali obblighi richiesti sono di trasparenza nei confronti dell'utente, in modo che sia sempre consapevole di chi detiene e ha avuto accesso ai suoi dati; di sicurezza e di

minimizzazione. Il report, in particolare, sottolinea la necessità di soddisfare le seguenti proprietà: i dati per la diagnosi e il trattamento dei singoli pazienti devono essere identificabili; quelli per la ricerca medica (eventualmente trattati su larga scala) devono essere adeguatamente pseudonimizzati per garantire che il livello di probabilità di re-identificazione sia ridotto al minimo; deve essere infine presente la capacità di gestire più fonti di dati del paziente, compresi i dispositivi indossabili e le app.

Uno dei case study riportati nel report esplora la situazione di un dispositivo indossabile per il monitoraggio continuo del glucosio (CSM) che, al contempo, monitora anche la pressione sanguigna, i livelli di caffeina e i livelli di lattato 7. Il dispositivo carica i flussi di dati raccolti nel cloud per l'archiviazione e l'ulteriore elaborazione da parte dell'utente stesso e di soggetti terzi, come la sua famiglia e i medici. La complessità principale da superare è quella di permettere all'utente di selezionare specifici flussi di dati da condividere con soggetti specifici e l'ora e il tempo d'accesso, per esempio permettere a un soggetto terzo l'accesso ai dati corrispondenti agli ultimi tre mesi per specifici set di dati. In tal senso, sono descritte alcune soluzioni crittografiche per proteggere la privacy dei dati sanitari durante la loro condivisione tra utenti diversi. In particolare, si tratta di tre tecniche di crittografia asimmetrica: con chiave pubblica, l'Attribute Based Encryption (ABE) e la Proxy Re-encryption. La tecnologia con chiave pubblica prevede che ogni segmento di dati da condividere venga crittografato dall'utente con la chiave pubblica del destinatario interessato. Tale soluzione, tuttavia, risulta poco pratica quando i dati devono essere condivisi tra più entità. L' ABE comporta invece la crittografia dei dati con una chiave pubblica ABE, che consente l'esistenza di più chiavi di decifrazione legate a informazioni aggiuntive relative ai dati, chiamate attributi. La Proxy Re-encryption, infine, consente la condivisione di dati già criptati da una chiave pubblica a un'altra, senza che il proxy abbia accesso al set di dati non criptati.

Uno scenario tipico di condivisione di dati sanitari è quello della gestione delle cartelle cliniche elettroniche (EHR) da parte degli operatori sanitari. Sono cartelle che raccolgono la storia clinica del paziente e di solito vengono conservate in archivi centrali nazionali. Gli utenti possono autorizzare l'accesso ai propri dati ai medici curanti o alle istituzioni mediche. A seguito della pandemia, si è resa urgente la necessità di progetti di raccolta dati ai fini della progressione della ricerca scientifica e della prognosi. Di solito, essendo il sistema centralizzato, la gestione dei meccanismi di controllo degli accessi viene effettuata dal centro medico, affinché solo i fornitori di servizi sanitari autorizzati abbiano accesso alle informazioni personalizzate. Quando i dati devono essere trasmessi a ricercatori interni o esterni, occorre adottare misure di pseudonimizzazione, al fine di scongiurare l'identificazione del paziente.

ENISA, dunque, propone l'utilizzo della crittografia polimorfica e pseudonimizzazione (PEP), tecnologia che consente di crittografare i dati senza la necessità di stabilire in anticipo chi può decifrarli. Ciò significa che l'accesso ai dati può essere concesso successivamente, a diverse parti con chiavi differenti. Ad ogni individuo viene assegnato uno pseudonimo diverso per ogni richiesta di accesso, quindi ogni paziente ha un identificatore univoco. Questo identificativo viene trasformato in diversi pseudonimi a seconda del destinatario e del contesto della condivisione dei dati. Gli pseudonimi utilizzati per lo stesso paziente non possono essere collegati, preservando così la riservatezza dei dati del paziente. La PEP è già stata testata con successo in uno studio sul morbo di Parkinson e come proposta per il sistema olandese di Electronic Identification (eID).

In conclusione, la condivisione dei dati è un'opportunità di sviluppo notevole per il settore sanitario e per la società in generale, ma deve essere regolamentata adeguatamente per garantire la protezione dei dati personali e la fiducia degli individui e delle organizzazioni. In merito, "l'ingegneria della protezione dei dati" si rivela essere una grande alleata per rispettare i principi di privacy *by design* e *by default* previsti dall'art. 25 GDPR.

CARMINE ANDREA TROVATO

https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

16. Il *working paper* dell'ISDA del gennaio 2023 sull'insolvenza nei mercati degli assets digitali

Nel gennaio 2023 l'International Swaps and Derivatives Association ("**ISDA**") ha pubblicato un *working paper* intitolato "*Navigating Bankruptcy in Digital Asset Markets: Netting and Collateral Enforceability*" vertente sui contratti derivati inerenti ai *digital assets*.

Il documento tra origine dai recenti fallimenti di FTX - nota piattaforma di *trading online* -, "TerraUSD" - una *stablecoin* -, "Three Arrows

Capital" – *hedge fund* specializzato in criptovalute - , "Celsius" - una società attiva nel segmento *crypto lender* – e alla richiesta ai sensi del Chapter 11 di "BlockFi" – altra impresa di *crypto lender*.

I suddetti eventi hanno scosso il mercato e incrinato la fiducia degli investitori (*rectius*, risparmiatori) imponendo alle Autorità di supervisione del mercato di approntare rapidamente un quadro regolatorio adeguato.

Tale disciplina deve anche tenere conto delle peculiarità del fenomeno considerato. Per tale motivo, è difficile rispondere univocamente ad alcuni interrogativi. Ad esempio, come si individua il proprietario di un *digital asset*? E ancora, come si gestisce il rischio di credito di controparte in caso di insolvenza del gestore della piattaforma di *trading* o della *stablecoin*?

Il documento dell'ISDA si propone di rispondere a tale ultimo interrogativo analizzando due istituti: il "*close-out netting*" e i collaterali.

Preliminarmente, va detto che gli attori del mercato dovrebbero avere una chiara comprensione dei diritti e obblighi nascenti da rapporti contrattuali con oggetto *digital assets*.

Occorre, quindi, tentare di definire la natura giuridica degli *assets* digitali, la quale risente delle loro particolari caratteristiche giuridiche, tecnologiche ed economiche, nonché i connessi diritti e doveri.

Ebbene, il *working paper* si concentra sugli *assets* che utilizzano la *Distributed Ledger Technology* (c.d. DLT) in cui il bene non è controllato da un'entità centralizzata, ma la titolarità risulta distribuita tra i vari nodi della rete. A ciò si aggiunga che alcuni *asset* digitali esistono solo nella rete (ad esempio, i Bitcoin), poiché non configurano una rappresentazione digitale di un bene esistente nella realtà, altri rappresentano un fascio di situazioni giuridiche che esistono sia *online*, sia *offline*. Altri ancora esistono *online*, ma sono collegati con altri beni esistenti in natura, un sottostante.

Da quanto detto, emerge la difficoltà di coniugare tale fenomeno con gli attuali *legal frameworks*, che peraltro verosimilmente non conoscono la proprietà diffusa di un bene. Di conseguenza, il *paper* utilizza il termine "*holder*" in modo generico riferendosi a colui che ha il potere di controllare l'*asset* digitale e non come sinonimo di "*possessed*".

In merito alla gestione del rischio di controparte, il *close-out netting* è un istituto ampiamente diffuso nei contratti derivati per cui in caso di *termination* del contratto, ad esempio per insolvenza di una parte, tutte le obbligazioni originanti dal rapporto giuridico sono risolte, le prestazioni ad esse collegate sono valutate e tramutate nel pagamento di una somma (*lump sum*) dal debitore al creditore. Si tratta di un meccanismo che consente: i) la risoluzione anticipata di un accordo; ii) la valutazione delle prestazioni ancora dovute; iii) il pagamento di una somma in sostituzione delle varie prestazioni potenzialmente da eseguire; ma soprattutto, iv) di evitare che la *defaulting party* possa continuare a assumere diritti e obblighi seppur non sia più in grado di adempiervi regolarmente.

Il funzionamento di tale meccanismo, previsto dal modello contrattuale dell'*ISDA Master Agreement*, non cambia laddove il contratto abbia ad oggetto *digital assets*. È possibile, tuttavia, che alcuni ordinamenti giuridici non conoscano tale istituto. Esso, infatti, è sicuramente applicabile alle transazioni regolate dalla legge inglese e americana, ma non a quelle rette dal diritto degli stati europei che hanno attuato la dir. 2002/47/CE, c.d. *Financial Collateral Directive*. A ciò si aggiunga che la normativa secondaria emanata dalle Autorità di supervisione bancaria può determinare l'inoperatività del sistema di *close-out netting*.

Per tali motivi, il *paper* dichiara che l'ISDA sta lavorando per far includere il *close-out netting* in tutte le transazioni con oggetto un *digital asset*.

I collaterali, invece, sono beni dati in garanzia da un contraente ("*collateral provider*") all'altro ("*collateral taker*") al fine di mitigare l'esposizione al rischio di credito di controparte. In un contratto ciascuna parte può sia rilasciare che ricevere collaterali.

I benefici associati al rilascio di una garanzia sono diversi. Innanzitutto, i tempi per l'escussione sono generalmente brevi per gli *assets* liquidi. Addirittura, se i *collateral* sono *asset* digitali, l'incasso può avvenire quasi istantaneamente (c.d. "*atomic settlement*"). In secondo luogo, il collaterale esce dal controllo del garante.

In caso di *default* della parte che ha rilasciato la garanzia, l'altra può i) acquisire la proprietà del bene soddisfacendosi sino alla concorrenza dell'importo dovuto in base al contratto non adempiuto e restituendo l'ammontare della garanzia in eccesso (c.d. "*title transfer agreement*"); ii) acquisire un "*secondary proprietary interest*" sul collaterale e, di conseguenza, soddisfarsi sul bene (c.d. "*security interest*").

Per completezza, comunque, va detto che al trasferimento della proprietà del collaterale può seguire l'appropriazione del bene o l'esecuzione forzata, ossia la sua vendita con soddisfacimento sul ricavato.

La costituzione di una garanzia impone di interrogarsi su come determinare la proprietà di un *digital asset*. Il paper in commento, rinviando all'"*ISDA Legal Guidelines for Smart Derivatives Contracts – Collateral*", rileva che non esiste una risposta univoca in considerazione delle differenze tra i vari ordinamenti giuridici e che ogni considerazione al riguardo è influenzata da fattori tecnologici.

È necessario, inoltre, indagare come si perfeziona la garanzia avente ad oggetto i *digital assets*. Al riguardo, il *working paper* qui analizzato precisa che è difficile determinarlo a priori, a causa delle differenze tra gli ordinamenti giuridici, soprattutto sui concetti di "*control*" e "*possession*". Ad ogni modo, laddove un individuo possa dimostrare di avere il controllo su un *digital asset*, ad esempio perché quest'ultimo è stato trasferito in un suo *account* o *wallet*, è ragionevole supporre che la garanzia si sia perfezionata.

Assai condivisibilmente, il *paper* in commento, rinviando all' *ISDA Whitepaper* "*Contractual Standards for Digital Asset Derivatives*", evidenzia pure che le peculiarità degli *asset* digitali e degli ordinamenti giuridici coinvolti si riflettono, tra l'altro, nella formulazione dei contratti che li riguardano e nei conflitti di legge nascenti dai suddetti contratti.

Per concludere, il *working paper* dell'ISDA rileva che la rapida evoluzione del mercato e alcuni recenti accadimenti rendono sempre più importante sviluppare un quadro normativo armonizzato e chiaro riguardo ai derivanti inerenti ai *digital assets*.

EMANUELE STABILE

https://www.isda.org/2023/01/26/navigating-bankruptcy-in-digital-asset-markets-netting-and-collateral-enforceability/

17. La determina dell'Agenzia per la cybersicurezza nazionale del 3.1.2023 sulla tassonomia degli incidenti informatici da notificare

Il 3 gennaio 2023 è stata pubblicata sulla Gazzetta Ufficiale la determina (da ora anche la "**Determina**") dell'Agenzia per la cybersicurezza nazionale (da ora anche l'"**Agenzia**") recante la definizione degli incidenti ICT che devono essere notificati all'Agenzia.

La Determina è stata emanata in attuazione dell'art. 1, comma 3 bis D. L. 105/2019 (da ora il "**Decreto**"), convertito in L. n. 133/2019, recante "*disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*".

La Determina si propone proprio di definire la tassonomia degli incidenti che possono avere un impatto negativo sulla rete, sui sistemi informativi e sui servizi informatici diversi dai "beni ICT" che i soggetti di cui all'art. 1, comma 2 bis del Decreto (c.d. "soggetti inclusi nel perimetro") sono tenuti a notificare.

L'art. 1 della Determina contiene le seguenti definizioni:

- "soggetto incluso nel perimetro", i soggetti di cui all'art. 1, co. 2 bis Decreto, ossia "*amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo*";
- "*bene ICT*", ossia "*un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'art. 1, comma 2, lettera b)*" del Decreto;
- "*incidente"* indica *"ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*";
- "*impatto sul bene ICT",* ossia la *"limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali*".

L'art. 2 della Determina definisce l'oggetto del provvedimento in esame, sostanzialmente coincidente con quanto sopra detto.

L'art. 3, infine, rinvia all'Allegato A alla Determina che si presenta diviso in due parti per la definizione della tassonomia degli incidenti. Nella prima sono elencati gli incidenti da notificare. Nella seconda, invece, sono descritti gli eventi da cui originano gli incidenti che dovranno essere segnalati.

EMANUELE STABILE

https://www.acn.gov.it/notizie/contenuti/si-rafforza-il-perimetro-nazionale-di-sicurezza-cibernetica

18. Il provvedimento del 21.2.2023 dello US Copyright Office su opera d'arte composita di testi creati da un uomo e immagini generate da un sistema di IA generativa (Midjourney) e la *Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence* del 16.3.2023

Il 21 febbraio 2023, lo United States Copyright Office (**USCO** o **Ufficio**) ha cancellato parzialmente la registrazione rilasciata all'artista Kristina Kashtanova, concessa lo scorso 15 settembre 2022, per la sua *graphic novel* "Zarya of the Dawn", a causa di "informazioni non accurate e incomplete".

Il fumetto conteneva infatti, oltre a elementi testuali dell'autrice, anche opere generate da Midjourney, un sistema di intelligenza artificiale che crea immagini in base a istruzioni di testo; l'artista non lo aveva comunicato allo USCO nella sua domanda di registrazione.

Prima di giungere a tale decisione, nell'ottobre 2022 l'Ufficio ha richiesto all'artista ulteriori informazioni sul processo creativo dell'opera esprimendo le sue preoccupazioni sul fatto che l'opera d'arte generata tramite Midjourney fosse in grado di soddisfare il requisito della paternità umana dell'opera [così come previsto da copiosa casistica (*ex multis Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 58 (1884)*; *Naruto v. Slater, 888 F.3d 418, 426 (9th Cir. 2018))* e dalle linee guida dello stesso Ufficio "*Compendium of U.S. Copyright Office Practices § 306*" (3d ed. 2021)].

Kashtanova ha risposto sostenendo che, nonostante l'uso del servizio di generazione di immagini di Midjourney come parte del processo creativo, ogni singolo elemento dell'opera è stato realizzato grazie al suo contributo e riflette la sua paternità. Il processo creativo di Kashtanova era consistito nel generare una serie di immagini tramite Midjourney che erano state poi selezionate in maniera accurata e organizzate da lei per creare l'insieme costituito dalla storia raccontata nel fumetto.

A prescindere dalle considerazioni dell'artista, secondo l'USCO, sebbene Kashtanova sostenesse di aver deciso direttamente il contenuto e la struttura di ciascuna immagine, il processo descritto rende evidente che il sistema di IA non l'ha semplicemente assistita (al pari di software specializzati nell'elaborazione di opere appartenenti all'arte figurative, e.g. Adobe Photoshop) ma ha creato le immagini seguendo un processo che non è lo stesso di un artista, scrittore o fotografo umano; pertanto, le immagini generate da Midjourney non sono frutto di una creazione umana.

Nella sua decisione, l'USCO ha fatto riferimento alla sentenza della Corte Suprema degli Stati Uniti nella causa *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991)* in cui si spiega che il termine "originale" nel contesto della tutela del *copyright* consiste di due componenti: creazione indipendente e creatività sufficiente. In primo luogo, l'opera deve essere stata creata in modo indipendente dall'autore. In secondo luogo, l'opera deve possedere una creatività sufficiente. È necessario solo un "minimo di creatività". Vale la pena notare che il Copyright Compendium dell'USCO sopra citato afferma esplicitamente che solo le opere create dall'uomo sono registrabili.

Midjourney produce immagini in modo imprevedibile, pertanto gli utenti del software non sono gli autori delle immagini generate dalla tecnologia. Come ha spiegato la Corte Suprema degli Stati Uniti d'America, nel caso sopra menzionato *Burrow-Giles Lithographic Co. v. Sarony*, l'autore di un'opera tutelata dal *copyright* è la persona che ha effettivamente realizzato l'immagine, la "mente inventiva" dietro l'opera stessa. Un utente che fornisce suggerimenti testuali a Midjourney non può essere considerato l'autore.

L'USCO ha precisato che il testo della *graphic novel* (le didascalie a commento delle immagini) così come la selezione, il coordinamento e la disposizione delle immagini dell'opera sono tutelati dalla normativa sul *copyright* ma che le singole immagini create da Midjourney non possono esserlo.

Il certificato originale rilasciato all'artista è stato cancellato e ne è stato emesso uno nuovo, insieme a un aggiornamento del registro pubblico, per "chiarire che la registrazione cancellata è stata sostituita con la nuova registrazione più limitata".

La decisione in commento è stata confermata recentemente dalle Linee Guida dell'USCO per la registrazione di opere create dall'IA, pubblicate in data 16 marzo 2023 ("*Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence"*: https://www.copyright.gov/ai/ai_policy_guidance.pdf).

Secondo l'Ufficio, è ormai assodato che il diritto d'autore può proteggere solo il materiale che è il prodotto della creatività umana. Il termine "autore", utilizzato sia dalla Costituzione

Americana sia dalla normativa sul Copyright, esclude autori non umani.
I regolamenti per la registrazione delle opere pubblicati dell'USCO riflettono le indicazioni della legge e della giurisprudenza in materia.
Ai sensi delle Linee Guida, l'Ufficio valuterà ai fini della registrazione, caso per caso, se i contributi dei sistemi di IA sono il risultato di una "riproduzione meccanica" o invece di una "concezione mentale originale" dell'autore. La risposta dipenderà dalle circostanze, in particolare dal funzionamento dello strumento di IA e dal modo in cui è stato utilizzato per creare l'opera finale. Secondo l'Ufficio, ad oggi, i sistemi di intelligenza artificiale generativa attualmente disponibili non consentono agli utenti di esercitare un controllo creativo sul modo in cui tali sistemi interpretano i suggerimenti e generano materiale. L'USCO equipara la situazione attuale a quella in cui un cliente incarica un'artista di creare un'immagine dandogli indicazioni approssimative e generali sul risultato finale. In tali casi, l'autore sarebbe l'artista che ha ricevuto le istruzioni e ha determinato in maniera del tutto autonoma il modo migliore per esprimerle. Il committente fornisce l'idea che non è tutelabile mentre è l'artista che la esprime in un oggetto tangibile.
L'Ufficio precisa come i richiedenti abbiano il dovere di rivelare l'inclusione di contenuti generati dai sistemi di IA in un'opera presentata per la registrazione e di fornire una breve spiegazione dei contributi dell'autore umano all'opera (a differenza di quanto avvenuto per la registrazione della *graphic novel* "Zarya of the Dawn").
La presentazione della domanda di registrazione presso l'USCO è soggetta a sanzioni pecuniarie ai sensi del 17 U.S.C. §506(e) "per chiunque faccia consapevolmente una falsa rappresentazione di un fatto materiale".
La decisione dell'USCO è importante perché ribadisce che le opere generate tramite sistemi di intelligenza artificiale non sono tutelabili ai sensi della normativa statunitense sul Copyright qualora il materiale sia realizzato senza che l'utente possa determinarne l'esito (non predittivo) e non possa modificarne la sua forma espressiva.

FRANCESCO GROSSI

https://copyright.gov/docs/zarya-of-the-dawn.pdf

https://www.copyright.gov/ai/

https://www.copyright.gov/ai/ai_policy_guidance.pdf

19. Gli *obiter dicta* dell'ordinanza della Corte di Cassazione I sez. n. 1107 del 16.01.2023 su diritto d'autore e computer generated content (caso Rai Festival di Sanremo).

Lo scorso 16 gennaio la Corte di Cassazione ha avuto modo di pronunciarsi sul legittimo utilizzo di un'immagine digitale raffigurante un fiore, utilizzata dalla Rai come scenografia in occasione del Festival di Sanremo del 2016.
Un' architetta genovese, conosciuta con il nome d'arte 'Lindelokse', aveva dato vita ad un'opera intitolata "*The Scent of the Night*" rappresentante un elemento floreale con una tecnica c.d. frattale realizzata con l'utilizzo di un software. Per frattale si intende un oggetto geometrico dotato di omotetia interna: si ripete nella sua forma, allo stesso modo, su scale diverse un'immagine in modo tale che, ingrandendo una qualunque sua parte, si ottiene una figura simile all'originale.
La particolare forma dell'opera, che ricorda un fiore che sboccia, si è facilmente prestata alla scenografia del notorio festival della canzone italiana, in cui, proprio per la città che lo ospita, le composizioni floreali giocano un ruolo centrale. Nel caso in questione, però, la Rai non aveva acquistato i diritti dall'autrice che si è rivolta, nel 2018, all'autorità giudiziaria per tutelare i suoi interessi, chiedendo il risarcimento del danno, la rimozione del programma da RaiPlay e la pubblicazione della sentenza.
Sia in primo che in secondo grado la Rai è risultata soccombente sulla scorta di due motivi: l'accertata paternità dell'opera in capo alla ricorrente e il carattere creativo dell'opera, tutelabile dunque ai sensi della disciplina sul diritto d'autore.
La Rai ha allora proposto ricorso per Cassazione e l'occasione è stata propizia per i giudici di legittimità per accennare alla questione della creatività della c.d. arte digitale o computer art.
Venendo ad analizzare le censure sollevate dalla ricorrente, con il primo motivo di ricorso la Rai ha assunto che la Corte d'Appello abbia errato nel postulare il carattere creativo dell'immagine, lamentando, ex art. 360 c.p.c. n.4, la nullità della sentenza per motivazione apparente. Sul punto la Cassazione ha invece ritenuto la motivazione esistente e non meramente apparente, ribadendo la presenza del requisito di creatività dell'opera sulla scorta della classica interpretazione data del concetto di "creatività", da intendere non in senso assoluto, ma come originale espressione della personalità del suo autore.

Nel caso di specie, ha concluso la Cassazione, l'opera non è una semplice riproduzione di un fiore ma una sua rielaborazione; la stessa RAI l'ha implicitamente riconosciuto, valorizzandola in modo accentuato come simbolo della manifestazione tanto che gli utenti hanno reagito positivamente con acquisizione di un buon grado di notorietà.

Con il secondo motivo di ricorso, in subordine, la RAI ha contestato il fatto che la Corte di appello abbia erroneamente qualificato come opera dell'ingegno un'immagine generata da un software e non attribuibile ad un'idea creativa della sua supposta autrice.

Quanto sopra è stato sostenuto dalla ricorrente in virtù del fatto che l'opera è stata realizzata da un software, che ne ha elaborato forma, colori e dettagli tramite algoritmi matematici e l'autrice avrebbe, si asserisce, solamente scelto un algoritmo da applicare e approvato a posteriori il risultato generato dal computer.

La Cassazione ha ritenuto inammissibile quest'ultimo motivo perché volto a introdurre per la prima volta in sede di legittimità una questione nuova non trattata nel giudizio di merito. Sorvolando sui motivi procedurali, La Corte si pronuncia però incidentalmente anche sull'inesplorato tema dell'arte digitale, per tale intendendo quella pratica artistica che utilizza la tecnologia digitale come parte del processo creativo o di presentazione espositiva.

Infatti, i giudici hanno sostenuto che "*non è certamente sufficiente a tal fine l'ammissione della controparte di aver utilizzato un software per generare l'immagine, circostanza questa che, come ammette la stessa ricorrente, è pur sempre compatibile con l'elaborazione di un'opera dell'ingegno con un tasso di creatività che andrebbe solo scrutinato con maggior rigore, se, com'è avvenuto nel caso concreto, la RAI non ha chiesto ai giudici di merito il rigetto della domanda per quella ragione. E infatti si sarebbe reso necessario un accertamento di fatto per verificare se e in qual misura l'utilizzo dello strumento avesse assorbito l'elaborazione creativa dell'artista che se ne era avvalsa. Il motivo deve pertanto essere dichiarato inammissibile, senza la necessità di affrontare in questa sede i temi, per ora inesplorati nella giurisprudenza di questa Corte, della cosiddetta arte digitale (detta anche digital art o computer art) quale opera o pratica artistica che utilizza la tecnologia digitale come parte del processo creativo o di presentazione espositiva*".

Seppur la Suprema Corte, non ha fatto riferimento in questa ordinanza a sistemi di intelligenza artificiale c.d. generativi, l'approccio che, *incidenter tantum*, essa ha in questo modo affacciato, aggiunge forse un piccolo, seppur importante, tassello alla delicata questione della tutelabilità delle opere ottenute da intelligenza artificiale generativa.

Ci troviamo in un momento storico in cui ChatGPT di OpenAI è solo la punta dell'iceberg di un processo che sta coinvolgendo le aziende ormai da anni, in quanto con un minore investimento in termini di tempo e risorse si può ottenete un output ad hoc. Questo vale tanto per i più svariati prodotti dell'industria in genere, quanto per il mondo dell'arte. Si vedano ad esempio, a livello amatoriale i prompt Text-to-Image generati dai sistemi di AI Midjourney e DALL-E; ovvero a livello più accreditato, le opere di Davide Quayola o di Refik Anadol. Per quest'ultimo si fa riferimento in particolare alla sua recente mostra "Unsupervised" presentata al MoMA, in cui un modello di apprendimento automatico esplora la collezione del museo e la rielabora dando vita a nuove immagini, ottenute dalla interpretazione e trasformazione fantasiosa di ciò che la circonda. Il sottotitolo della mostra curiosamente è: "Cosa sognerebbe una macchina dopo aver visto la collezione del Museum of Modern Art?".

Normalmente due domande accompagnano le opere realizzate con l'ausilio di applicazioni software e a maggior ragione quelle generate da sistemi di intelligenza artificiale: se siano tutelabili ai sensi del diritto d'autore e a chi andrebbe attribuita la paternità dell'opera.

La Cassazione con dei brevi cenni alla questione ha affrontato la prima delle domande suesposte e sembra aver aperto la strada alla possibilità che, nel momento in cui sia identificabile un autonomo e sufficientemente creativo contributo umano nel processo che ha visto il concorso, anche consistente, di una applicazione software, l'opera può comunque dirsi "creativa". La Suprema Corte, come detto, non ha fatto riferimento in questa ordinanza a sistemi di intelligenza artificiale c.d. generativi, né ci sono elementi per ritenere che il software utilizzato per l'immagine del fiore, nel caso in questione, fosse un software di intelligenza artificiale.

Tuttavia, sembra di potersi leggere tra le righe di questo *obiter dictum* che la Corte di Cassazione reputi generalmente rilevante andare ad analizzare caso per caso se l'applicazione *software* utilizzata per realizzare un'opera abbia rappresentato un momento o uno strumento all'interno di un processo creativo frutto dell'espressione del suo autore umano.

EMANUELA BURGIO

https://web.uniroma1.it/deap/sites/default/files/allegati/Cass_ord_1107_2023.pdf

20. L'ordinanza cautelare del Tribunale di Venezia del 24.10.2022 in materia di riproduzione digitale di opere pubbliche in pubblico dominio. Il caso "puzzle dell'Uomo Vitruviano – Ravensburger" tra codice dei beni culturali e direttiva europea sul copyright nel mercato unico digitale

Il 24 febbraio 2023, è stata pubblicata su due quotidiani nazionali e su due quotidiani locali e nelle relative edizioni online, nei termini da essa stessa prescritti, un'ordinanza cautelare emessa dal Tribunale di Venezia in data 24.10.2022 su un ricorso d'urgenza ex art. 700 c.p.c. introdotto dal Ministero della cultura e dalle Gallerie dell'Accademia di Venezia riguardante l'utilizzo dell'opera di Leonardo Da Vinci, "Uomo Vitruviano", per la creazione e la vendita di puzzle da parte della società Ravensburger.

Le aziende tedesche di fama mondiale (Ravensburger AG, Ravensburger Verlag GMBH e la loro sede italiana rappresentata da Ravensburger S.r.l.) sono state, infatti, citate in giudizio per aver utilizzato l'immagine dell'opera per realizzare e vendere puzzle, senza aver ottenuto l'autorizzazione e aver pagato il canone annuale, oltre ad una royalty sulle vendite, all'istituto che ha in custodia il bene, le Gallerie dell'Accademia di Venezia. L'attività di impresa sarebbe posta in violazione del "*Regolamento per la riproduzione dei beni culturali in consegna alle Gallerie dell'Accademia di Venezia*", elaborato in conformità agli artt. 107-109 del Codice dei beni culturali (D.Lgs. 22.01.2004, n. 42), in particolare all'art. 108 dello stesso. La casa produttrice e quella distributrice del prodotto di *merchandising* avrebbero, quindi, utilizzato, senza essere state a ciò autorizzate, il nome e l'immagine dell'opera di Leonardo. L'opera, la cui riproduzione è in contestazione, non è protetta dal diritto d'autore, ma è in pubblico dominio, non tanto in quanto sia scaduto il termine di protezione legale (che, ai sensi della legge sul diritto d'autore n. 633/1941, è pari a settanta anni dopo la morte dell'autore, fatti salvi i diritti morali), ma in quanto la creazione del disegno da parte di Leonardo risale al 1490 e la prima legislazione che diede riconoscimento al diritto sulla proprietà intellettuale in Italia è stata la legge 19 fiorile anno IX del 9 maggio 1801 della Repubblica Cisalpina. Si può quindi ritenere che il disegno di Leonardo non sia mai stato soggetto alla relativa tutela in materia di diritto d'autore. Il disegno però rientra nella definizione di "bene culturale" ed è, dunque, soggetto anche alla disciplina del codice dei beni culturali. Agli articoli 106 e seguenti del Codice dei beni culturali, sono disciplinate le disposizioni sull'uso e le riproduzioni del patrimonio culturale. Lo Stato, le Regioni e gli altri enti pubblici territoriali possono concedere l'uso "individuale" dei beni culturali che abbiano in consegna, per finalità compatibili con la loro destinazione culturale a singoli richiedenti (art. 106 Codice dei beni culturali). Tale fattispecie è relativa all'uso fisico e rivale del bene culturale.

Per quanto invece, riguarda, le disposizioni circa la riproduzione delle immagini dei beni culturali esse stabiliscono che sono libere e nessun canone è dovuto, se effettuate senza scopo di lucro, per finalità di studio, ricerca, libera manifestazione del pensiero o espressione creativa, promozione della conoscenza del patrimonio culturale. È riconosciuta, altresì, la facoltà di divulgazione, con qualsiasi mezzo, delle immagini di beni culturali, legittimamente acquisite, in modo da non poter essere ulteriormente riprodotte a scopo di lucro.

In caso di utilizzo a fini commerciali è richiesto il rilascio di un'autorizzazione e il pagamento di un canone, la cui definizione è rimessa alla discrezionalità di ciascun istituto culturale che ha in custodia il bene, in base alla valutazione di determinati fattori quali: il carattere delle attività; i mezzi e le modalità con i quali sono effettuate le riproduzioni; l'uso e la destinazione delle stesse e dei benefici economici che ne derivano al richiedente (artt. 107 e 108 Codice dei beni culturali).

Nell'ordinanza in esame, il Tribunale di Venezia, prima di occuparsi dell'interpretazione delle suddette disposizioni di legge che limitano le riproduzioni delle immagini dei beni culturali e il loro libero riuso al solo fine non commerciale, si sofferma su diverse questioni attinenti la giurisdizione, la legittimazione passiva dei convenuti, la competenza territoriale e l'applicabilità delle norme del codice dei beni culturali a soggetti stranieri.

Con riferimento alla questione della giurisdizione, il Tribunale sancisce la giurisdizione italiana richiamandosi al regolamento (UE) n. 1215/2012, in virtù del quale, in materia di illeciti civili dolosi o colposi, una persona domiciliata in uno Stato membro può essere convenuta in un altro Stato membro "davanti all'autorità giurisdizionale del luogo in cui l'evento dannoso è avvenuto o può avvenire" (art. 7, punto 2 regolamento (UE) n. 1215/2012), e all'interpretazione fornita dalla Corte

di giustizia europea in base alla quale la nozione di "luogo in cui l'evento dannoso è avvenuto" può coincidere con il luogo in cui si concretizza il danno (CGUE C-12/15).
In tal senso, è rimessa alla facoltà dell'attore la scelta dello Stato ove instaurare il procedimento, se quello della residenza del convenuto, dove è sorto il danno, o in quello in cui si è verificata la condotta.
Secondo il Tribunale, nel caso di specie, "si è […] determinata una separazione geografica tra il luogo del fatto generatore del danno (l'uso dell'immagine dell'opera a fini di lucro, avvenuto Germania) e il luogo dove il pregiudizio non patrimoniale lamentato si è concretamente prodotto (ovvero l'Italia), così consentendo alle reclamanti di scegliere tra i due fori, posti in posizione di alternatività e di pari ordinazione".
Per quanto riguarda la competenza territoriale, il Tribunale dichiara la propria competenza ex art. 20 c.p.c., ancorandola al luogo "in cui certamente e principalmente si è verificato il danno risarcibile" e in cui "si realizzano le ricadute negative della lesione".
Non essendo, infatti, possibile secondo i giudici collocare l'illecito in modo chiaro sul piano spaziale ed essendo necessario individuare un luogo certo del pregiudizio oggetto del risarcimento, dove cioè possa dirsi sorta l'obbligazione dedotta in giudizio a norma dell'art. 20 c.p.c., la competenza territoriale viene affermata quale giudice del luogo del domicilio del danneggiato. A Venezia, infatti, si trovano il bene culturale e la sede dell'ente che lo ha in custodia, al quale dev'essere chiesta l'autorizzazione per la sua riproduzione e che, nel caso di specie, non ha potuto effettuare il controllo sulla compatibilità dell'utilizzo effettuato da Ravesburger "con il [...] profilo culturale e valoriale oltre che dei corrispettivi dovuti".
Le società resistenti tedesche lamentavano, altresì, la carenza della loro legittimazione passiva, dichiarandosi estranee alla condotta illecita. In particolare, Ravensburger AG rassegnava in tal senso di non aver ricoperto alcun ruolo operativo e Ravensburger Verlag Gmbh di aver effettuato la produzione esclusivamente all'estero. Tali doglianze non sono state accolte.
Riguardo l'esistenza del *fumus boni iuris*, il Tribunale, in primo luogo, verificava l'applicabilità del Codice dei beni culturali alle parti in causa, giustificandola in ragione del forte collegamento della fattispecie con il territorio italiano, luogo in cui si sono verificate le conseguenze dell'illecito, ove è custodito il bene culturale e si trova l'istituto custode.
Il Codice dei beni culturali viene poi definito una "norma di applicazione necessaria" ex artt. 17 della L. 218/1995 e 16 del regolamento (CE) n. 864/2007 sulla legge applicabile alle obbligazioni extracontrattuali (c.d. regolamento "Roma II"), in quanto assolutamente cruciale per la salvaguardia dell'interesse pubblico.
Il Tribunale prosegue la disanima, riferendosi inoltre all'art. 4, paragrafo 1, del citato regolamento Roma II, secondo cui la legge applicabile alle obbligazioni extracontrattuali che derivano da un fatto illecito "è quella del paese in cui il danno si verifica, indipendentemente dal paese nel quale è avvenuto il fatto che ha dato origine al danno e a prescindere dal paese o dai paesi in cui si verificano le conseguenze indirette di tale fatto".
Assodata l'applicabilità alle parti della disciplina delle norme del Codice dei beni culturali e del codice civile italiano, i giudici deducono che la condotta delle società reclamate rientri nella disciplina ex artt. 2043 e 2059 c.c., in relazione alla quale il danno è costituito dallo "svilimento dell'immagine e della denominazione del bene culturale", in quanto utilizzati senza permesso, e dunque senza alcun controllo, nonché dalla perdita economica subita dall'istituto che non ha riscosso il canone.
Quanto al *periculum in mora*, i giudici ravvisano il pericolo di danno proprio nell'utilizzo, senza alcun controllo dell'ente custode, della riproduzione dell'opera a fini commerciali. L'irreparabilità del danno emerge in relazione alla gravità della lesione ai danni dell'immagine e del norme del bene culturale, danneggiato irreparabilmente solo per il fatto di essere stato utilizzato senza la verifica dell'ente custode. A parere del Tribunale, inoltre, gli effetti lesivi sono da considerarsi aggravati proprio dal perdurare dell'illecito, circostanza che rende il pregiudizio imminente.
A fronte di tali premesse, il Tribunale di Venezia ha inibito ai convenuti l'utilizzo a fini commerciali dell'immagine dell'opera "Uomo Vitruviano" di Leonardo da Vinci e della sua denominazione, in qualsiasi forma e in qualunque prodotto e/o strumento, anche informatico sui propri siti internet e su tutti gli altri siti e *social network* di loro competenza; ha condannato i convenuti al pagamento di una penale di € 1.500,00 in favore del Ministero della Cultura e delle Gallerie dell'Accademia di Venezia per ogni giorno di ritardo nell'esecuzione del provvedimento cautelare a decorrere dal settimo giorno successivo alla comunicazione del provvedimento e per il caso di eventuale ripresa dell'utilizzo abusivo dopo la sospensione dell'attività illecita per ordine del

Tribunale; ed ha, infine, disposto la pubblicazione dell'ordinanza in estratti e/o sintesi del suo contenuto da parte dei reclamanti e a spese dei convenuti a caratteri doppi del normale, per due volte, anche non consecutive, su due quotidiani a diffusione nazionale - il Corriere della Sera e la Repubblica - e su due quotidiani a diffusione locale – Il Gazzettino e La Nuova Venezia -, anche nelle loro versioni on-line, con termine non superiore a giorni 10 dalla comunicazione per l'inserzione su due quotidiani nazionali e su due quotidiani locali.

La pronuncia rafforza la portata dell'applicabilità del Codice dei beni culturali, sebbene lo stesso presenti dei profili di incompatibilità con l'art. 14 della direttiva (UE) 2019/790 sul diritto d'autore e i diritti connessi nel mercato unico digitale (c.d. direttiva CDSM dal suo acronimo inglese *Copyright in the Digital Single Market*) che stabilisce che le riproduzioni non originali di opere delle arti visive in pubblico dominio devono rimanere in pubblico dominio: «art. 14 *Opere delle arti visive di dominio pubblico* - Gli Stati membri provvedono a che, alla scadenza della durata di protezione di un'opera delle arte visive, il materiale derivante da un atto di riproduzione di tale opera non sia soggetto al diritto d'autore o a diritti connessi, a meno che il materiale risultante da tale atto di riproduzione sia originale nel senso che costituisce una creazione intellettuale propria dell'autore».

In tal senso, l'art. 32-*quater* della legge italiana sul diritto d'autore (legge 22 aprile 1941, n. 633) introdotto dal D.lgs. 177/2021 del 5.11.2021 in attuazione dell'art. 14 della direttiva CDSM, presenta numerosi profili critici nella parte in cui limita l'efficacia del principio all'applicazione del codice dei beni culturali ("*Restano ferme le disposizioni in materia di riproduzione dei beni culturali di cui al decreto legislativo 22 gennaio 2004, n. 42*"), di fatto impedendo l'esplicarsi degli intenti del legislatore europeo (ben delineati nei Considerando 3 e 53 della direttiva CDSM e nei chiarimenti forniti dalla stessa Commissione europea in forma di FAQ: https://digital-strategy.ec.europa.eu/en/faqs/copyright-reform-questions-and-answers), e creando una distinzione tra opere delle arti visive in pubblico dominio e i beni culturali pubblici in pubblico dominio (sull'attuazione in Italia della direttiva CDSM in generale v. in questa rubrica la notizia n. 1 nel numero 1/2022 : http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf).

Anche nel caso in cui la legislazione europea sia introdotta con una direttiva che non ha di per sé effetti o applicabilità diretta nell'ordinamento giuridico nazionale degli Stati membri, essa deve sempre rappresentare un indispensabile parametro guida per i tribunali nazionali, che sono chiamati a interpretare il diritto nazionale alla luce della legislazione europea (ossia, un obbligo di interpretazione conforme). Inoltre, esiste un divieto generale per gli Stati membri di far prevalere una norma nazionale su una norma comunitaria contraria, senza distinguere tra diritto nazionale anteriore e posteriore.

In conclusione, l'attuale impianto normativo italiano, stratificando la protezione al di fuori dei confini del diritto d'autore, di fatto ostacola la libera riproduzione delle immagini del patrimonio culturale italiano nel mercato unico, riducendo la portata del pubblico dominio europeo. In tal senso, sarebbe auspicabile una pronuncia della Corte di Giustizia europea che chiarisca se la disciplina italiana possa dirsi compatibile con la chiara volontà del legislatore europeo di tutelare il pubblico dominio.

DEBORAH DE ANGELIS

https://web.uniroma1.it/deap/sites/default/files/allegati/%20Trib_Venezia_ord_17.11.2022_Ravensburger.pdf

21. Ultimi sviluppi del caso DABUS in Brasile e nel Regno Unito (a proposito della possibilità che un sistema di IA possa qualificarsi come inventore ai fini di una domanda di brevetto per invenzione industriale).

La questione se un sistema di intelligenza artificiale possa essere designato quale inventore in una domanda di brevetto è approdata anche in Brasile, all'Istituto Nazionale di Proprietà Industriale (*Instituto Nacional da Propriedade Industrial* "**INPI**"), con la richiesta n. BR 112021008931-4, in cui il Dr. Stephen Thaler è il richiedente e 'DABUS' (acronimo per *Device for the Autonomous Bootstrapping of Unified Sentience*) è il sistema di IA - creato dallo stesso Dr. Thaler - che avrebbe a sua volta creato due dispositivi brevettabili che sono stati l'oggetto delle suddette domande di brevetto.

La vicenda si inserisce nell'ambito della campagna internazionale di depositi di brevetto e ricorsi ("*Artificial Inventor Project*"), avviata da Thaler a partire dal 2018, per sostenere la tesi che un sistema di IA debba poter essere designato come inventore in una domanda di brevetto per invenzione industriale (v. notizia n. 6 nel numero 4/2021 di

questa rubrica: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf).
L'INPI ha inizialmente formulato una richiesta di chiarimenti al richiedente nei seguenti termini: "alla luce di quanto previsto dall'art. 6 della Legge brasiliana sulla proprietà industriale n. 9279/96 (LPI), si deduce che l'inventore di una domanda di brevetto debba essere in grado di essere titolare di diritti, possedendo capacità giuridica. Si prega di chiarire e di giustificare la nomina dell'intelligenza artificiale DABUS come unico inventore della domanda di brevetto alla luce delle disposizioni della LPI".
Le argomentazioni che Thaler ha portato a supporto della sua richiesta prendono in esame il predetto art. 6 LPI, precisando che il suddetto articolo non stabilisce che l'inventore debba avere capacità giuridica; fra l'altro, nel sistema giuridico brasiliano non esiste una definizione del termine "inventore" o una chiara delimitazione dei requisiti necessari per la sua identificazione.
Il richiedente Thaler ha inoltre sostenuto che la nomina di DABUS come unico inventore è corretta, essendo questi l'unico responsabile dell'invenzione, e, essendo lo stesso Thaler proprietario del sistema di IA, Thaler sarebbe anche il titolare dei suoi frutti, ai sensi delle disposizioni dell'art. 1.232 del Codice Civile brasiliano.
Thaler, infine, sostiene che la ricerca e lo sviluppo in ambito IA, avrebbero un significativo rallentamento dal fatto che sistemi di IA come DABUS non siano riconosciuti come inventore.
Considerata la complessità della questione legata alla possibilità di indicare un sistema di IA quale inventore, l'INPI ha ritenuto opportuno coinvolgere la Procura Federale richiedendone un parere in merito (parere n. 00024/2022/CGPI/PFE-INPI/PGF/AGU, datato 8 agosto 2022).
In sintesi, la Procura arriva alla conclusione che non è possibile indicare o nominare un sistema di IA come inventore di una domanda di brevetto in Brasile, al pari di quanto già deciso nella maggior parte dei Paesi in cui è stato affrontato il tema. La possibilità che figure non umane (o *software*) siano autori di opere artistiche o invenzioni, viene ignorata dalla normativa brasiliana in materia e per arrivare a tale conclusione oltre a fare riferimento anche all'art. 4-*ter* della Convenzione di Parigi, prende anche in esame alcune controversie passate afferenti al diritto d'autore, come il famoso caso del *selfie* del macaco Naruto (Naruto v. Slater, 888 F.3d 418, 426, 9th Cir. 2018). Sempre a sostegno della tesi che solamente una persona umana può essere definita "inventore", la Procura Federale richiama l'art. 1 del Codice Civile brasiliano ("ogni persona è capace di diritti e doveri nell'ordinamento civile").
Anche la tesi portata avanti da Thaler sulla titolarità dei frutti prodotti dal bene di sua proprietà viene respinta dalla Procura Federale dato che la normativa sulla proprietà intellettuale si riferisce a beni immateriali/beni non tangibili, mentre il Codice Civile si riferisce a beni tangibili e per tale motivo deve essere esclusa tale analogia.
Nella conclusione del suo parere, la Procura Federale sottolinea come sia fondamentale tenere conto del fatto che l'attuale normativa brasiliana non disciplina in maniera esaustiva la creazione di invenzioni da parte di sistemi di IA e, di conseguenza, vi è la necessità di adottare una legislazione *ad hoc*, anche sottoscrivendo trattati internazionali per standardizzare i principi di tutela nei vari Paesi. La Procura evidenzia anche che l'assenza di una disciplina specifica potrebbe scoraggiare investimenti nel settore dato che non vi è la garanzia di un riconoscimento dei diritti.
In seguito a tale parere, il 6 settembre 2022 l'INPI ha annunciato il rigetto della domanda di brevetto, a causa dell'impossibilità di indicare o nominare un sistema di IA come inventore (decisione pubblicata nella Gazzetta della Proprietà Industriale (RPI) n. 2696 del 6 settembre 2022).
Thaler ha impugnato la decisione e avrà la possibilità di adire la Corte Federale brasiliana.
L'INPI, quindi, in coerenza con l'interpretazione adottata nella maggior parte dei Paesi ove è stata presentata la domanda di registrazione da Thaler, non riconosce un sistema di IA come inventore (di recente anche Corea del Sud, Taiwan e Nuova Zelanda hanno rigettato simili domande).
Thaler, comunque, continua la sua battaglia: in seguito alla sentenza della *Court of Appeal* inglese che ha confermato le precedenti pronunce dell'*Intellectual Property Office* (UKIPO) e della High Court (v. notizia n. 6 nel numero 4/2021 di questa rubrica: http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf), ha presentato ricorso alla *Supreme Court* con le seguenti questioni da chiarire:
(a) Se l'articolo 13, paragrafo 2, lettera a), del Patents Act 1977 richieda che una persona sia indicata come inventore in tutti i casi, anche quando il richiedente ritiene che l'invenzione sia stata creata da un sistema di IA in assenza di un inventore umano;
(b) Se la legge del 1977 preveda la concessione di un brevetto senza un inventore umano; e
(c) se nel caso di un'invenzione realizzata da un sistema di IA, il proprietario, il creatore e

l'utilizzatore di tale sistema di IA hanno diritto alla concessione di un brevetto per tale invenzione?
L'udienza si è tenuta il 2 marzo 2023, e, al momento in cui viene scritto questo contributo, si attende la sentenza.

http://revistas.inpi.gov.br/rpi/
https://www.gov.br/inpi/pt-br/central-de-conteudo/noticias/inteligencia-artificial-nao-pode-ser-indicada-como-inventora-em-pedido-de-patente/ParecerCGPIPROCsobreInteligenciaartificial.pdf
https://www.supremecourt.uk/cases/uksc-2021-0201.html